NATIONAL CYBERWATCH CENTER

REPORT

COLLABORATIVE CURRICULUM TASKFORCE

STUDY OF THE CYBERSECURITY WORKFORCE FRAMEWORK MAPPING TO ACADEMIC COURSES

NOVEMBER 15, 2014

PREPARED BY:

DR. MARGARET LEARY

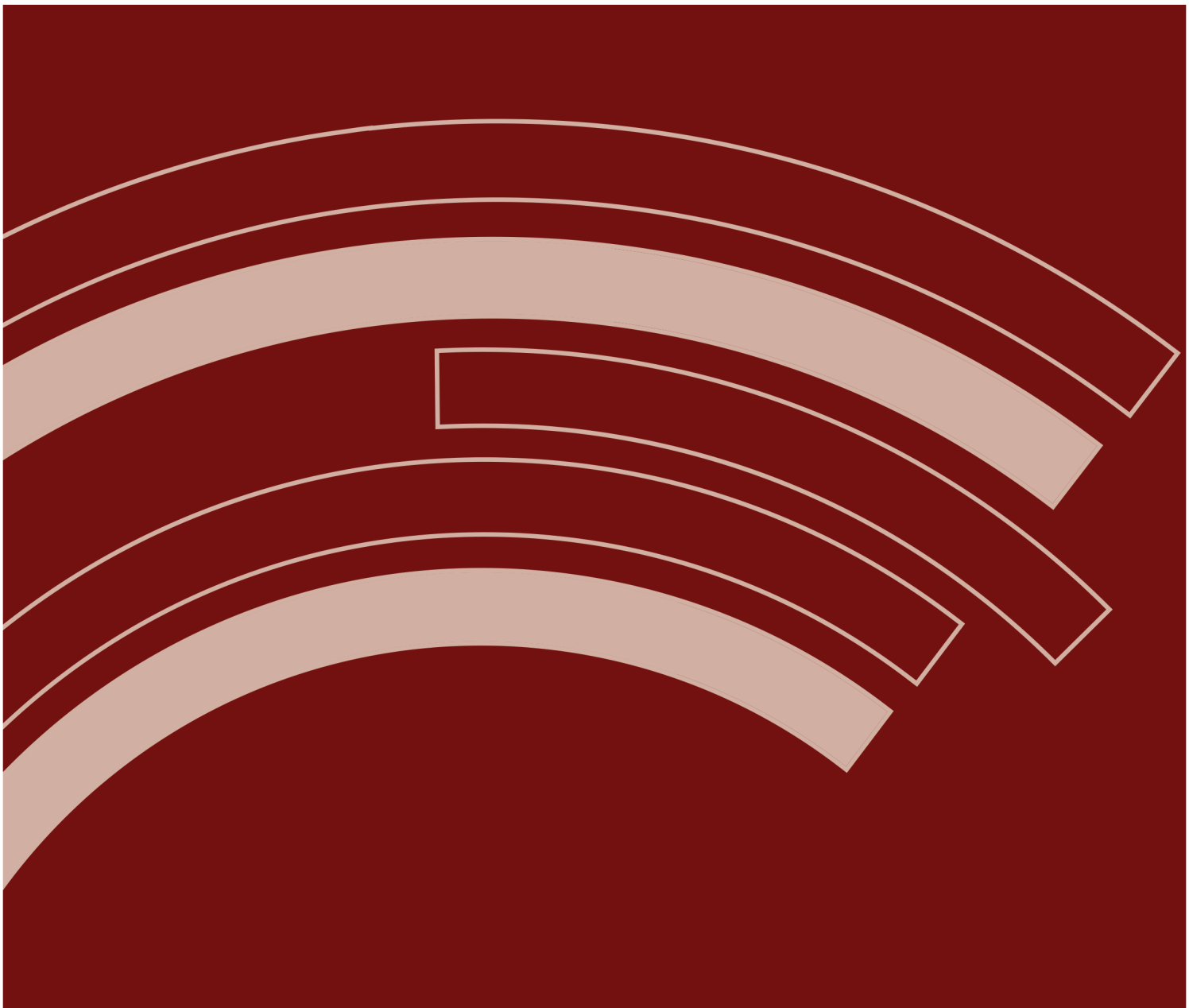

Table of Contents

I.

I. Executive Summary

This report provides the results of a mapping effort performed by the National CyberWatch Center's Curriculum Task Force of cybersecurity curricula to the National Cybersecurity Workforce Framework 1.0 Knowledge, Skills, and Abilities (KSAs). The goal of this study was to build a taxonomy of courses and identify how these courses aligned with the KSAs specified within the framework, identifying "gaps" in academic courses to the Framework and the possibility of developing a lexicon for use when developing new cybersecurity courses.

This work was performed of a period of 5 months by a taskforce of 12 faculty members from 2- and 4-year institutional cybersecurity faculty and 18 student coders performing the mapping. Each coder was provided instructions and a template. Curriculum Taskforce members validated the results of the mapping and performed a comprehensive analysis on data. A database was developed that will enable academic institutions to populate their data and produce reports. This will also extend the ability of the Curriculum Taskforce to collect and analyze mapping data.

Summary results of this study evidenced no consistency in course naming or content sufficient to build a lexicon of terms. Too, while more than 97% of the KSAs were mapped across the courses examined, only a small set of KSAs were implemented with regularity. Recommendations are made in the report for continued research.

II. Purpose

The National Initiative for Cybersecurity Education (NICE) is an interagency effort coordinated by the National Institute for Standards and Technology (NIST) to improve the nation's cybersecurity education, with the goal of improving cybersecurity workforce. Cybersecurity workforce tasks and associated knowledge, skills, and abilities (KSAs) have been identified within the National Cybersecurity Workforce Framework and are regarded as a starting point for agencies desiring a common framework and lexicon for developing a cadre of cybersecurity workers. This guide identifies and classifies the requirements of cybersecurity workers into seven categories: Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze, Securely Provision, and Oversight and Development. Within each category, Specialty Areas provide recommendations on typical job tasks' knowledge, skills and abilities (KSAs) recommended to enable the cybersecurity specialist to perform a specific role.

In response to the critical need to build a cybersecurity workforce, educational institutions have increased cybersecurity programs offered across the nation. Programs can be found at both the 2-year and 4-year levels, within public, as well as with private, educational institutions. Many of these programs, those that are Centers of Academic Excellence (CAE) and CAE2Y (CAEs at the community college level), have implemented prescribed academic programs. Initially, these academic requirements were driven by NSA, emphasizing CNSS standards. These standards are no longer a requirement for designation and updated criteria has been jointly defined by the NSA and Department of Homeland Security (DHS).

The purpose of this study was to perform a survey of NSA/DHS CAE and CAE2Y institutions to develop a taxonomy of cybersecurity program objectives mapped to Framework. The objective was to attempt to address the following questions:

- To what extent do existing cybersecurity courses address the Framework KSAs?
- Can cybersecurity program course objectives be normalized across institutions such that a common catalog, or lexicon, of cybersecurity concepts can be developed that map to the Framework KSAs?
- To what extent do other standards, such as the Association of Computing Machinery (ACM) Curricula Recommendations (see http://www.acm.org/education/curricula-recommendations and http://ai.stanford.edu/users/sahami/CS2013/), address the Framework KSAs? This will include the model courses in the upcoming 2013 curriculum recommendations (CS 2013).
- To what extent do the courses address the new OPM guidelines, based on the Framework, for the classification of Federal cybersecurity positions as defined in pages A-106 through A-112 in http://www.opm.gov/policy-data-oversight/data-analysis-documentation/data-policy-guidance/reporting-guidance/part-a-human-resources.pdf?

Outcomes proposed for this research included the following:

- ***A catalog of course objectives that institutions can leverage when developing a syllabus***. These course objectives include Framework identifiers such that the objective can be linked to the KSAs in the specialization areas to which they relate.
- ***An analysis of "gaps" between sampled curriculum and the Framework.*** Initially, it was proposed to also identify gaps between the Framework and OPM job descriptions/classifications, however information on OPM job descriptions/classifications was unattainable so could not be analyzed within this report.
- ***Development of a survey instrument that can be used by institutions to identify Framework KSAs within their cybersecurity courses.*** A database has been developed to facilitate this effort and continue to support data collection and analysis efforts. This process can also be used to facilitate articulation agreements between institutions.

III. Methodology

A content analysis approach was modified to accommodate the project goals, with a national team of cybersecurity faculty from across 4- and 2-year colleges selected to serve on a Curriculum Task Force. These faculty members provided process recommendations and oversaw the content mapping of course objectives/syllabi provided by institutions. Faculty participating in this effort included the following:

- **Dr. Ali Bicak** – Marymount University
- **Prof. William Bill Butler** – Capitol Technology University
- **Dr. Wm. Arthur Conklin** – University of Houston
- **Dr. Deanne Cranford-Wesley** – Forsyth Technical Community College
- **Dr. John Knight** – Ivy Tech Community College – Northeast

- **Shamsi Moussavi** – MassBay Community College
- **Dr. William Hoag** – Champlain University
- **Dr. Margaret Leary** – Northern Virginia Community College, Project Chair
- **Dr. Tom Pigg** – Jackson State Community College
- **Dr. John Sener** – Sener Learning
- **Pat Tamburelli** – County College of Morris
- **Bruce Waugh** – Craven Community College

The methodology for the project consisted of three phases: 1) data collection, 2) data mapping, and 3) analysis, as addressed below.

Phase 1: Data Collection

A request for support was sent in October 2013 by Lynn Hathaway at NSA to all 166 CAE/CAE2Y institutions. In addition, CAE2Ys were directly queried by the Project Chair through the National Cyberwatch Center database. Taskforce members were also asked to reach out to their contacts to solicit input. Recipients were asked to identify courses included in their security programs and to provide course descriptions and/or course objectives/student learning outcomes for each. In exchange for identifying these courses, completed mappings would be provided to the institutions in order to incent institutions to respond.

The response rate to multiple solicitation requests was relatively low, but after several rounds of solicitations, 36 schools provided materials. In some cases, only course descriptions were given and the protocol for the study was based on learning objectives as they give a more complete perspective of the knowledge, skills, and abilities a student might have as a result of taking the course. Some institutions had graduate programs in security, but no undergraduate. It was decided, for this phase of the project, to limit the scope of the study to undergraduate courses. Undergraduate and graduate students were engaged to survey low-reporting schools to find syllabi/course objectives publicly posted in order to obtain a sufficient sample size for analysis. A list of schools which either submitted course information (Appendix B), or were directly examined for course information, are listed in Appendix A. Of the 166 institutions that were queried, 36 institutions were selected from across 19 different states, submitting approximately 250 courses. This represented a response rate of only 20%. Of the responses and subsequent surveys, 32 schools were selected for analysis. Of the schools selected for analysis, 252 courses were reviewed for mapping.

Phase 2: Data Mapping

A mapping input form (Appendix C) was developed, extrapolating the KSAs from the interactive Framework report, and was provided to faculty performing data mapping, or supervising students performing the mapping efforts. Coding Instructions (Appendix D) were provided and reviewed by participants in a conference call. The undergraduate syllabi assembled for analysis were distributed to taskforce members and learning objectives were mapped to the Framework KSAs. As expected, institutions had a varying number of relevant courses, with each course possessing a number of learning

objectives. In total, there were 2340 learning objective statements to match to KSAs. Student workers were provided stipends to perform the mapping. Students were trained to recognize key words in learning objective statements and search for those words in the KSA list. They then made a judgment as to whether the learning objective matched enough elements of KSA to be considered as contributing to the knowledge, skill, or ability described. In the Framework, KSAs are grouped by Category and many KSAs belong to a multiple categories. Thus, a list of KSA's was used for mapping.

Phase 3: Analysis

The eventual goal of the project is to have the data available within a database that can be used for further analysis, help guide schools in developing learning objectives, and be expanded by schools. A second goal was to analyze learning objectives associated with specific KSA's to determine if there were commonalities in the language being used.

Database. It was agreed on by Taskforce members that the following objectives would be established for the database:

1. Provide a mapping of course objectives/learning objective statements to the Framework.
2. Enable the Taskforce to identify gaps that might present opportunities to institutions to develop courses to Framework content.
3. Provide institutions with a mechanism allowing them to map their courses to the Framework.

The database was designed and built around the following reports anticipated to be of use to institutions with, or developing, cybersecurity courses:

- List of courses, and their institutions, that satisfy a specific KSA;
- List of courses, and their institutions, that map to any of the KSAs for a given domain;
- List of courses, and their institutions, that map to any of the KSAs for a given specialty;
- List of KSAs to which no course is mapped;
- List of all KSAs that one or more course have mapped to, showing the names of all courses (& institution) for every KSA;
- List of learning objectives mapped to a KSA;
- Common KSA's : KSAs that map to learning objectives in over half of all schools; and
- Categories, % of KSA's mapped, by 2-year and by 4-year institution.

This database will be hosted at the National Cyberwatch Center and will be made available to all institutions who would like to add or update their course information. In order to get a quick view on what the results looked like, all of the mapping data was combined into an Excel spreadsheet. A pivot table was developed using the mapping data from the schools. This provided a perspective on which KSA's were most commonly associated with course learning objectives and which KSAs were weakly associated (or not at all associated) with course learning objectives. It also became possible to group the data by KSA and begin to review the language used in learning objectives for a single KSA.

IV. Constraints

Several constraints were encountered that warrant discussion as some negatively impacted the ability to meet specific project objectives, or impacted the sufficiency of the data reported in this report.

- Framework 2.0 had not been released at the time that this study started. Framework 1.0 version was used.
- NSA was not able to directly share CAE/CAE2Y contact information. It was felt that this inability to reach out directly to each defined point of contact was partially responsible for the lower rates of return to the initial participation requests.
- The format for course outcomes are not consistently defined. Some institutions provided syllabi, others objectives and still others learning outcomes. In some cases, only broadly stated topics were defined, perhaps consisting of only 3 or 4 per course, whereas elsewhere outcomes for each course were multiple pages in length.
- The request made to institutions was very broad and interpreted differently by each institution. Some schools provided only cybersecurity courses, while other institutions provided "foundational" courses. As an example, Capitol Technology University provided only Information Assurance courses and did not provide the 18 hours of coursework in computer science required in the 120 credit degree program. This made it difficult to obtain an accurate comparison across all institutions. Some schools had over 60 courses to map, which included courses with considerably outdated technologies (i.e. Star, DOS).
- Even with coding suggestions, the differences between the wording in the KUs, KSAs, and courses was found to be a barrier to deriving accurate mappings. Some KSAs were found to be too granular to be captured by analysis within a more broadly stated course description or learning objective. Other KSAs were too broadly stated to be mapped to course objectives that were very process-oriented.

V. Findings

The preliminary results from the pivot table analysis provide some information on how well the learning objectives of 32 institutions learning objectives in security and related courses match up with the KSAs in the Framework. Overall findings identified during the research included the following:

- 32 total schools were analyzed. Of these, 18 were community colleges and technical schools (15 CAE2Y) and 14 were four-year institutions (11 CAEs).
- 252 courses containing 2340 learning objectives.
- 5582 mappings of learning objectives to KSAs (many learning objectives mapped to more than one KSA).
- There was a significant lack of consistency between course titles and the material associated with the course. For instance, in one case, a Microsoft Windows Course that would be expected to contain basic System Administration information (installation of Microsoft Server, setup and

management of access controls, printing, and other basic services) was, instead, focused on infrastructure topics such as DHCP, DNS, IPSEC, and routing.

- Some courses mapped a single course to Security+ content, whereas others mapped multiple courses to this same content.
- It was noted that there was confusion on the part of the institutions regarding Framework KSAs and CAE/CAE2Y KUs. This was evidenced by the fact that several institutions contacted the Chair to request copies of their mappings to facilitate their application for CAE/CAE2Y designation. While this confusion did not negatively impact this survey, it does illustrate that DHS/NSA should better clarify the importance of integrating Framework elements into a course of study.

KSAs addressed in cybersecurity curricula. A complete table of KSAs and their occurrences by course is contained in the spreadsheet provided in Appendix E. An analysis of this data revealed the following:

- A total of 387 KSAs, of 395 total (98% of all KSAs), were addressed by at least one course.
- A total of 209 (53%) KSAs were addressed in 10 or more courses.
- The gradation of KSA occurrences by course is remarkably consistent with no discernible hard breaks beyond the top six most commonly occurring KSAs.

To determine which KSA's are most prevalent, the schools with course learning objectives that mapped to a particular KSA were counted. The KSAs with 40 or more occurrences, in order of frequency of occurrence, are listed below:

Rank	KSA #	Description	Category	# Occurrences
1)	986	Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control)	Identity Management	59
2)	70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)	Information Systems/Network Security	53
3)	92	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Infrastructure Design	52
4)	139	Knowledge of common networking protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP]) and services (e.g., web, mail, Domain Name System [DNS]) and how they interact to provide network communications	Infrastructure Design	49
5)	1114	Knowledge of encryption methodologies	Cryptography	49
6)	985	Skill in configuring and utilizing network protection components (e.g., firewalls, Virtual Private Networks [VPNs], network Intrusion Detection Systems [IDSs])	Configuration Management	47
7)	77	Knowledge of current industry methods for	Information	45

Rank	KSA #	Description	Category	# Occurrences
		evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures, utilizing standards-based concepts and capabilities	Systems/Network Security	
8)	123	Knowledge of system and application security threats and vulnerabilities	Vulnerabilities Assessment	44
9)	3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Vulnerabilities Assessment	43
10)	177	Skill in designing countermeasures to identified security risks	Vulnerabilities Assessment	43
11)	108	Knowledge of risk management processes, including steps and methods for assessing risk	Risk Management	42
12)	25	Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES).	Cryptography	41
13)	341	Knowledge of UNIX and Windows systems that provide radius authentication, Domain Name Server, mail, web service, FTP server, DHCP, firewall, and simple network management protocol	Operating Systems	41
14)	364	Skill in identifying, modifying, and manipulating applicable system components (Window and/or Unix/Linux) (e.g., passwords, user accounts, files)	Operating Systems	41
15)	4	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data	Vulnerabilities Assessment	40
16)	49	Knowledge of host/network access controls (e.g., access control list)	Information Systems/Network Security	40
17)	81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design	40
18)	150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security	40
19)	1069	Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks)	Computer Network Defense	40

Table 1. Commonly Occurring KSAs

Another method of presenting this data can be performed by examining the percentage of schools mapping to a KSA. If 70% of the schools had courses that mapped to a KSA, it was considered strongly represented. Ten KSA's emerged as the most prevalent within this view (see Table 2, below). Similarly,

if fewer than 30% of the colleges reporting had course learning objectives that mapped to a particular KSA, it was considered to be a weak association. Two hundred-nineteen (219), or 55%, of the KSAs fell into this category. That leaves 159 KSAs that have some reasonable representation in the mappings. This information may also inform the next iteration on the Framework for wording of KSA's. The 30%, 70% are fairly arbitrary and different categorization values could be used in further analysis. If the categories are set at 50%, then 78 KSA's have more than half the schools with learning objectives that map to them, while 310 KSAs are not represented.

KSA	Description	Category
3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Vulnerabilities Assessment
4	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data	Vulnerabilities Assessment
25	Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES).	Cryptography
49	Knowledge of host/network access controls (e.g., access control list)	Information Systems/Network Security
70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)	Information Systems/Network Security
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security
341	Knowledge of UNIX and Windows systems that provide radius authentication, Domain Name Server, mail, web service, FTP server, DHCP, firewall, and simple network management protocol	Operating Systems
986	Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control)	Identity Management
1114	Knowledge of encryption methodologies	Cryptography

Table 2. Strongly Associated KSAs

As noted in the constraints, the broad brush addressing vulnerability scanning and analysis of that data, as evidenced in the associated KSA #3 verbiage, can cause the rationalization, and even over-rationalization, of many different course objective statements when mapping. This limits the usefulness of this mapping exercise to developing a common cybersecurity education lexicon.

Weakly Associated KSAs. KSAs with Low (under 5) matches to learning objectives are detailed below.

KSA #	KSA Description	Category	# of Occurrences
7	Knowledge of “knowledge base” capabilities for identifying the solutions to less common and more complex system problems	Knowledge Management	5
18	Knowledge of circuit analysis	Computers and Electronics	2
20	Knowledge of complex data structures	Object Technology	2
21	Knowledge of computer algorithms	Mathematical Reasoning	5
46	Knowledge of fault tolerance	Information Assurance	2
52	Knowledge of human-computer interaction principles	Human Factors	5
65	Knowledge of information theory	Mathematical Reasoning	1
74	Knowledge of low level computer languages (e.g., assembly languages)	Computer Languages	1
78	Knowledge of microprocessors	Computers and Electronics	2
89	Knowledge of new technological developments in server administration	Technology Awareness	5
94	Knowledge of parallel and distributed computing concepts	Information Technology Architecture	3
99	Knowledge of principles and methods for integrating server components	Systems Integration	3
101	Knowledge of process engineering concepts	Logical Systems Design	2
102	Knowledge of programming language structures and logic	Computer Languages	4
115	Knowledge of content development	Computer Network Defense	3
116	Knowledge of software debugging principles	Software Development	5
119	Knowledge of software engineering	Software Engineering	3
120	Knowledge of sources, characteristics, and uses of the organization’s data assets	Data Management	4
132	Knowledge of technology integration processes	Systems Integration	5
134	Knowledge of the capabilities and functionality associated with various content creation technologies (e.g., wikis, social networking, blogs)	Technology Awareness	4

KSA #	KSA Description	Category	# of Occurrences
136	Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint)	Technology Awareness	2
144	Knowledge of the systems engineering process	Systems Life Cycle	3
152	Skill in allocating storage capacity in the design of data management systems	Database Administration	3
155	Skill in applying and incorporating information technologies into proposed solutions	Technology Awareness	2
158	Skill in applying organization-specific systems analysis principles and techniques	Systems Testing and Evaluation	5
162	Skill in conducting capabilities and requirements analysis	Requirements Analysis	2
163	Skill in conducting information searches	Computer Skills	3
164	Skill in conducting knowledge mapping (map of knowledge repositories)	Knowledge Management	
165	Skill in conducting open source research for troubleshooting novel client-level problems	Knowledge Management	2
168	Skill in conducting software debugging	Software Development	3
170	Skill in configuring and optimizing software	Software Engineering	5
172	Skill in creating and utilizing mathematical or statistical models	Modeling and Simulation	1
176	Skill in designing a data analysis structure (i.e., the types of data your test must generate and how to analyze those data)	Systems Testing and Evaluation	2
178	Skill in designing databases	Database Administration	2
180	Skill in designing the integration of hardware and software solutions	Systems Integration	3
182	Skill in determining an appropriate level of test rigor for a given system	Systems Testing and Evaluation	5
185	Skill in developing applications that can log errors, exceptions, and application faults and logging	Software Development	4
186	Skill in developing data dictionaries	Data Management	2
187	Skill in developing data models	Modeling and Simulation	4
188	Skill in developing data repositories	Data Management	1
190	Skill in developing operations-based testing scenarios	Systems Testing and Evaluation	4
195	Skill in diagnosing failed servers	Network Management	4

KSA #	KSA Description	Category	# of Occurrences
198	Skill in establishing a routing schema	Infrastructure Design	3
203	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system	Information Technology Performance Assessment	4
211	Skill in monitoring and optimizing server performance	Information Technology Performance Assessment	4
213	Skill in optimizing database performance	Database Administration	1
220	Skill in systems integration testing	Systems Testing and Evaluation	3
222	Skill in the basic operation of computers	Computer Skills	1
223	Skill in the measuring and reporting of intellectual capital	Knowledge Management	2
224	Skill in the use of design modeling (e.g., unified modeling language)	Modeling and Simulation	1
227	Skill in tuning sensors	Computer Network Defense	1
230	Skill in using knowledge management technologies	Knowledge Management	1
234	Skill in using sub-netting tools	Infrastructure Design	4
235	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system	Computers and Electronics	3
238	Skill in writing code that is compatible with legacy code (e.g., Common Business-Oriented Language [COBOL], FORTRAN IV)in a modern programming language (e.g., Java, C++)	Computer Languages	3
239	Skill in writing test plans	Systems Testing and Evaluation	4
244	Ability to determine the validity of technology trend data	Technology Awareness	0
246	Knowledge and experience in the Instructional System Design (ISD) methodology	Multimedia Technologies	0
269	Knowledge of CNE/CNA/CNO methodologies	Computer Network Defense	2
270	Knowledge of common adversary tactics, techniques, and procedures (TTPs) in assigned area of responsibility (e.g., historical country-specific TTPs, emerging capabilities)	Computer Network Defense	3

KSA #	KSA Description	Category	# of Occurrences
282	Knowledge of emerging computer-based technology that has potential for exploitation by adversaries	Technology Awareness	3
285	Knowledge of evasion strategies and techniques (e.g., noise, stealth, situational awareness, bandwidth throttling)	Computer Network Defense	4
296	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise	External Awareness	4
297	Knowledge of industry indicators useful for identifying technology trends	Technology Awareness	3
314	Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain	Teaching Others	1
320	Knowledge of external organizations and academic institutions dealing with cybersecurity issues	External Awareness	5
336	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure [NII])	Telecommunications	5
337	Knowledge of the nexus between Cyber Counter-Intelligence and other Intelligence operations (i.e., How/ Where/ When Cyber Counter-Intelligence fits in, etc.)	External Awareness	2
339	Knowledge of the structure and intent of military operation plans, concept operation plans, orders, and standing rules of engagement	Organizational Awareness	2
345	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies	Web Technology	4
350	Skill in analyzing memory dumps to extract information	Reasoning	2
353	Skill in collecting data from a variety of Computer Network Defense resources (e.g., signals intelligence, open source intelligence, Computer Network Defense tools)	Computer Network Defense	5
355	Skill in creating plans in support of remote endpoint operations	Requirements Analysis	2
361	Skill in gathering and analyzing all-source information in support of indications and warnings	Reasoning	0
363	Skill in identifying gaps in technical capabilities	Teaching Others	3
367	Skill in multi-disciplined intelligence report writing	Writing	3

KSA #	KSA Description	Category	# of Occurrences
368	Skill in navigating mapping tools	Computer Skills	1
383	Skill in using scientific rules and methods to solve problems	Reasoning	2
389	Skill in physically disassembling personal computers (PCs)	Computers and Electronics	1
897	Skill in performing damage assessments	Information Assurance	5
899	Skill in gathering information from cyber social networks (e.g., MySpace, Facebook etc.)	Information Management	5
904	Knowledge of interpreted and compiled computer languages	Computer Languages	1
905	Knowledge of secure coding techniques	Computer Languages	1
907	Skill in data mining techniques	Data Management	4
909	Skill in processing collected data for follow-on analysis	Computer Skills	1
910	Knowledge of database theory	Data Management	4
911	Ability to interpret and translate customer requirements into operational cyber actions	Requirements Analysis	0
912	Knowledge of collection management processes, capabilities, and limitations	Configuration Management	3
913	Knowledge of how passive and active collections supplement each other	Information Management	1
914	Skill in identifying gaps in cyber collection capabilities	Strategic Thinking	2
916	Skill in de-conflicting cyber operations and activities	Political Savvy	2
920	Knowledge of threat list countries' cyber capabilities, intent, opportunities, and presence	External Awareness	2
921	Ability to identify possible threat actor uses of a new technology	Technology Awareness	5
950	Skill in evaluating test plans for applicability and completeness	Systems Testing and Evaluation	5
954	Knowledge of Export Control regulations and responsible agencies for the purpose of reducing supply chain risk	Contracting/Procurement	3
973	Skill in using code analysis tools to eradicate bugs	Software Development	0
974	Ability to tailor code analysis for application-specific concerns	Software Testing and Evaluation	2
976	Knowledge of software quality assurance process	Software Engineering	4
1004	Knowledge of critical information technology (IT) procurement requirements	Contracting/Procurement	1

KSA #	KSA Description	Category	# of Occurrences
1007	Skills in data reduction	Data Management	2
1012	Knowledge of Capabilities and Maturity Model Integration (CMMI) at all five levels	Internal Controls	2
1022	Knowledge of the nature and function of the relevant information structure	Enterprise Architecture	2
1042	Ability to apply network programming towards client/server model	Requirements Analysis	5
1047	Skill in writing kernel level applications	Software Development	3
1054	Knowledge of hardware reverse engineering techniques	Vulnerabilities Assessment	4
1062	Knowledge of software reverse engineering techniques	Vulnerabilities Assessment	5
1064	Knowledge of Extensible Markup Language (XML) schemas	Infrastructure Design	1
1088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump)	Computer Languages	2
1094	Knowledge of debugging procedures and tools	Software Development	1
1095	Knowledge of how different file types can be used for anomalous behavior	Vulnerabilities Assessment	4
1098	Skill in analyzing anomalous code as malicious or benign	Computer Network Defense	3
1100	Skill in identifying obfuscation techniques	Computer Network Defense	3
1101	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures	Computer Network Defense	3

Table 3. Weakly Associated KSAs

It is somewhat surprising that complex data structures and computer algorithms is not represented better in the learning objectives. One possible rationale is that, in most cases, only the security courses were mapped, not programming or Computer Science courses. Too, it may represent a trend to more network security-centric coursework.

These views may provide suggestions for common courses/learning objectives in cybersecurity education. The data allows analysis of the wording of learning objectives from a diverse set of colleges that map to a particular KSA. This may provide suggestions for common language to be used in learning objectives as the data allows analysis of the wording of learning objectives from a diverse set of colleges that map to a particular KSA. An example where specific course objective statements were categorized as mapping to KSA #3 follows:

KSA 3: Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
Probe a system for vulnerabilities
Conduct a vulnerability analysis.
Hacking overview hacking phases
Apply tools and techniques for vulnerability assessment
Identify security issues when they are confronted, or recognize them before they happen
Threats, Vulnerabilities, and Countermeasures related to physically protecting the enterprise's sensitive information assets Threats and Vulnerabilities
Active Reconnaissance Footprinting: Gathering Information about the Target Vulnerability Identification Using Nitko, Nessus
Vulnerability Assessment and Mitigating Attacks Vulnerability Assessment Assessment Techniques Assessment Tools Vulnerability Scanning vs. Penetration Testing Vulnerability Scanning? Penetration Testing Mitigating and Deterring Attack Database Vulnerabilities and Threats Vulnerabilities of IEEE 802.11 Security Vulnerabilities, Threats, Counter Measures National Threats, Vulnerabilities, Counter Measures, C1.0
Evaluate vulnerability of an information system and establish a plan for risk management
Demonstrate knowledge of security models and modes of operation;
Carry out vulnerability assessments using common tools, Use monitoring tools on systems and networks and detect security related anomalies
Explain the importance of vulnerability analysis, importance of network and technical vulnerabilities
Identify and discuss issues (such as security, privacy, redundancy, etc.) related to networked environments
Identify and discuss issues (such as security, privacy, redundancy, etc.) related to networked environments
Analyze and assess a computer system and/or network for vulnerabilities
This course is intended to provide the student with the knowledge and tools to protect systems and networks from threats and vulnerabilities thus providing the highest level of information system assurance.
Describe basic security vulnerabilities. Describe security technologies, products, solutions, and design. Design and manage a security policy. Explain industry security terminology and acronyms. Implement AAA using Cisco routers and PIX Security Appliances. Implement Secure Network Design.

KSA 3: Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
Explain techniques to harden hosts, server, and embedded operating systems against Windows and Linux vulnerabilities.
Performance of vulnerability analysis
Create a secure networking environment Identify different security topologies Describe firewalls and physical security concepts Demonstrate the daily tasks involved with managing and troubleshooting security technologies Create a security policy
Identify and evaluate different types of threats, malware, spyware, viruses, vulnerabilities, and today's attacks such as social engineering, rootkit, and botnets, Get hands-on experience using popular security tools, auditing, vulnerability scanning, and pen testing.
Identify and discuss issues (such as security, privacy, redundancy, etc.) related to networked environments
Identify and discuss issues (such as security, privacy, redundancy, etc.) related to networked environments
Threats and Vulnerabilities
Threats and Vulnerabilities
Students will learn the methodologies and tools used to probe networks for vulnerabilities and propose solutions.
Learn and understand basic security concepts and terminology associated with computer and information security.
Assess system vulnerability and exposure to develop an overall organizational security posture
Identify common threats and attacks employed against web accessible applications
Apply standard hacking methodologies and processes to vulnerability identification.
Vulnerabilities assessments
Identify malware through behavioral analysis
Determine various types of vulnerabilities and determine its risk level. Prepare a risk assessment report generated from raw penetration test data. Live systems, ports, vulnerabilities, services, operating system. Conduct a CrossSite Scripting attack against a vulnerable target. Conduct a bruteforce attack on a password file using various cracking tools. Discuss the vulnerabilities in using LANMAN, NTLMv1 & NTLMv2 and Kerberos. Discuss how salting works and the methods available to crack passwords that implement it.
Common system vulnerabilities and countermeasures; privacy and security policies and risk analysis.
Describe common characteristics of vulnerabilities and exploits
Explain various vulnerabilities and exploits
Perform ethical hacking techniques to do a vulnerability analysis and penetration testing. Identify the vulnerabilities of common protocols used in an organization.
Develop recommendations for hardening techniques for Windows operating systems. (3) Describe the vulnerabilities of a password.
Create appropriate security policy for an organization. Develop a security emergency plan. Communicate effectively.

KSA 3: Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
Identify security threats and system vulnerabilities.
Technology Safeguards: IDS, Scanning, Wireless Tools, Sniffers,
Summarize operating system vulnerabilities to learn how to prevent or mitigate certain types of attacks.
Identify security threats and vulnerabilities

Table 4. Example of KSA #3 Statement Mapping

Institutional coverage of Framework Specializations. KSAs selected in the available data are those mapped to a corresponding Competency Area. Determining the correlation between coverage and Competency Area is problematic because there is a such a large range of KSAs associated with each Competency Area, ranging from one (e.g., Capacity Management) to 30 (Computer Network Defense). Within a given Competency Area, coverage of KSA's also varies widely, for instance:

Specialty Area	KSAs w/high occurrence	KSAs w/low occurrence
Computer Network Defense	#1069: Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks) (40) #59: Knowledge of Intrusion Detection System (IDS) tools and applications (35)	#227: Skill in tuning sensors (1) #1098: Skill in analyzing anomalous code as malicious or benign (3) #1099: Skill in identifying obfuscation techniques (3) #1101: Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures (3)
Identity Management	#986: Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control) (59(+)	#209: Skill in maintaining delivery services (4)
Information Systems/Network Security	#70: Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption) (53)	#1119: Knowledge of signature implementation impact (9)

Table 5. Coverage of Framework Specializations

Preliminary analysis indicates that some Specialty Areas are better covered than others. For instance, the KSAs associated with Cryptography are covered by between 23 and 41 courses; however, there are only four KSAs associated with this Specialty Area. By contrast, the Capacity Management's single KSA is covered by only nine courses. This suggests that a more complete data analysis might be indicated, but also better parameters defining what constitutes "coverage" should also be defined.

VI. Conclusions

This study attempted to address several questions:

- ***To what extent do existing cybersecurity courses address the Framework KSAs?*** The extensive nature of the KSAs ensures that no single academic institution would be able to address all of the KSAs defined by NICE in its Framework. Now that Framework 2.0 has been formalized, and an alignment to the NSA Knowledge Units in the CAE criteria is being examined, it is expected that academic and workforce development programs will be increasingly focused on specific roles and specializations, as defined in the Framework. To this end, the National CyberWatch Center will be identifying model curriculum and content for institutions to leverage.

- ***Can cybersecurity program course objectives be normalized across institutions such that a common catalog, or lexicon, of cybersecurity concepts can be developed that map to the Framework KSAs?*** This survey of a small sampling of cybersecurity curricula reveals that while course names and course descriptions can be similar, it can be very difficult to ascertain the exact content and elements taught simply on the basis of title or description. To address this, a common lexicon should be developed to provide a semantic framework for academic institutions. This will require a mix of cybersecurity educators and industry Subject Matter Experts in order to ensure that the academic topics are transferrable to recognizable industry skills. Another recommendation is that syllabi should be developed Syllabi should reflect student learning outcomes. The National CyberWatch Curriculum Taskforce recommends that educational institutions include student learning outcomes on syllabi that includes a detailed descriptions of the skills that the student must be able to perform upon successful completion of the course. These skills should align with the CAE KUs and Framework KSAs, if it is desired to meet workforce training needs. Additionally, syllabi should address how these elements will be assessed. Resources should be provided to institutions to enable them to consistently assess knowledge and skill attainment across institutions.

- ***To what extent do other standards, such as the Association of Computing Machinery (ACM) Curricula Recommendations (see http://www.acm.org/education/curricula-recommendations and http://ai.stanford.edu/users/sahami/CS2013/), address the Framework KSAs?*** This will include the model courses in the upcoming 2013 curriculum recommendations (CS 2013). A review of the ACM standards demonstrates that it is focused on undergraduate computer

science programs, largely programming, however do also address a broad set of KUs and KSAs. Model course syllabi have been developed for the following:

- Algorithms and Complexity (AL)
- Architecture and Organization (AR)
- Computational Science (CN)
- Discrete Structures (DS)
- Graphics and Visualization (GV)
- Human-Computer Interaction (HCI)
- Information Assurance and Security (IAS)
- Information Management (IM)
- Intelligent Systems (IS)
- Networking and Communication (NC)
- Operating Systems (OS)
- Platform-Based Development (PBD)
- Parallel and Distributed Computing (PD)
- Programming Languages (PL)
- Software Development Fundamentals (SDF)
- Software Engineering (SE)
- Systems Fundamentals (SF)

Time and funding did not permit these courses to be mapped to the KSAs, however it is anticipated that, while comprehensive, the differences in language used for learning outcomes will differ from language used within the Framework KSAs to the same extent found within this study. A review of the ACM document indicates that the focus on programming will result in significant gaps with hard skills in areas of systems management than what is expected in the Framework KSAs. As another example, where the Framework specifies "Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems", the acquisition of these types of "hard skills" are not specified in the curriculum criteria. Learning outcomes, by and large, address "describing", "identifying", "explaining", "summarizing", "diagramming", etc. The model courses, however, do provide a reference point for developing a common lexicon and should be considered by the Curriculum Taskforce in that effort.

§ ***To what extent do the courses address the new OPM guidelines, based on the Framework, for the classification of Federal cybersecurity positions?*** As guidelines relevant to this research were not provided, this analysis could not be performed at this time – however should be considered for future research.

§ ***How well do the CAE/IA standards map to the Cybersecurity Workforce Framework?*** The Curriculum Taskforce participated in an exercise performed by Dr. Diana Burley, Research Director, National CyberWatch Center. The resultant Mapping Report of the Centers of Academic Excellence (CAE) Knowledge Units (KUs) to the National Initiative for Cybersecurity

Education (NICE) Knowledge, Skills, and Abilities (KSAs), found that a significant number of KSAs were not mapped to the KUs (pg. 3). Some of this is likely due to the lack of a common lexicon, such as that defined in other disciplines (i.e. Computer Science) and addressed earlier in this report. Regardless, the numerous standards-mapping "requirements" (CAE KUs, Framework KSAs, ABET, etc.) imposed on colleges and universities can easily become onerous and must be tied to some Return on Investment (ROI) in terms of resources necessary to maintain conformance to these standards. At present, there is no grant funding to provide incentive to map curriculum to the Framework KSAs, nor is there institutional designation.

VII. Recommendations for Further Research

Additional time is needed to perform a more comprehensive analysis on collected data. In particular, the National CyberWatch Center will continue data collection, mapping and analysis efforts to determine the following:

- Is there a hierarchy for KSAs within curriculum as demonstrated in the data (based on 1st year, 2nd year…etc.)?
- Are there KSAs that are not addressed in undergraduate programs, or in 2-year programs that should be addressed? Are there KSAs that are not reasonable for credit programs to address, that might be more clearly skills or knowledge that is best learned on the job or within very specific role-based training programs, or within workforce development (non-credit) programs? Do these lend themselves to units smaller than courses (e.g. modules, internships)?
- Is there an identifiable core subset of KSAs or specialty areas that should receive greater attention relative to the others? If so, how would these be identified?
- Are there emphases on category or specialty areas by school? This may be answerable as more data is populated into the database.
- There were several elements in course objectives that coders were not able to map to existing KSAs. This content should be examined for relevancy.
- The value of this data to institutions should be better captured perhaps in the areas of 1) articulation 2) highlighting or differentiating programs 3) performing an internal gap analysis, and 4) identifying what would constitute a core program requirement versus elective or optional content.

Appendix A – Participating Schools

- Bossier Parish Community College
- Capella University
- Capitol College
- Champlain College
- College of Southern Maryland
- Florida State College at Jacksonville
- Francis Tuttle
- George Mason University
- Hagerstown Community College
- Highline Community College
- Howard Community College
- Jackson State Community College
- Manhattan Area Technical College
- Marymount University
- Mass Bay Community College
- Mercy College
- Montgomery College
- New Jersey City University
- Norwich University
- Oklahoma City Community College
- Prince George's Community College
- Rochester Institute of Technology
- Rose State College
- Snead State Community College
- Southern PolyTech
- St. Leo University
- University of Advancing Technology
- University of Maryland University College
- University of Tennessee at Chattanooga
- University of the District of Columbia
- Valencia College
- Whatcom Community College

Appendix B – Courses Mapped

Institution Submitting Coursework (* indicates those used in mapping)	Courses Mapped
Bossier Parish Community College (10)	CIT 101 CIT 115 CIT 170 CIT 172 CIT 220 CIT 224 CIT 225 CIT 272 CIT 279 CIT 280
Capella University (8)	IT 4070 IT 4072 IT 4071 IT 4073 IT 4074 IT 4075 IT 4076 IT 4803
Capitol Technical University (9)	IAE 201 IAE 301 IAE 315 IAE 321 IAE 325 IAE 402 IAE405 IAE406 IAE410
Champlain College (14)	CIT 130 CIT 140 FOR 240 FOR 270 FOR 320 NET 225 NET 255 NET215 NET320 SEC 250

	SEC 335 SEC 350 SEC 440 SEC345
College of Southern Maryland (4)	ITS2090 ITS2500 ITS2530 ITS2535
Florida State College – Jacksonville (17)	CAP 2023 CAP 2140 CAP 2141 CET 1114 CET 1630 CET 1936 CET1173 CET1513 CET2172 CET2179 CET2588 CET2600 CET2629 CET2662 CET2687 CET2752 CET2759
Francis Tuttle (6)	CS2713 CS2743 CS2783 ECS 2224 ECS1214 ECS2514
George Mason University (6)	IT 223 IT 353 IT 357 IT 366 IT 462 IT 466
Hagerstown Community College (13)	CYB 101 CYB 201 CYB 225 CYB 240 CYB 245 IST 108 IST/CSC 109

	IST154 IST155 IST156 IST160 IST255 IST261
Highline Community College (11)	CIS 115 CIS 160 CIS 161 CIS 166 CIS 210 CIS 215 CIS 216 CIS 217 CIS 230 CIS 235 CIS 236
Howard Community College (13)	CFOR 101 CFOR 200 CFOR 210 CFOR 909 CFOR 910 CMSY 162 CMSY 163 CMSY 164 CMSY 219 CMSY 255 CMSY 256 CMSY 262 CMSY 263
Jackson State Community College (5)	CIS 156 CIS 259 CIS250 CIS251 CIS257
Manhattan Area Technical College (3)	CRT 100 CRT 282 CRT 289
Marymount University (7)	IT305 IT310 IT315 IT335 IT355 IT370

	IT390
MassBay (1)	CS 116
Mercy College (4)	CISC 335 CISC 359 IASP 420 IASP 440
Montgomery College (7)	MG 288 NW 173 NW 245 NW 246 NW 261 NW 263 NW 275
New Jersey City University (2)	SECU 222 SECU 422
Norwich University (6)	CJ341 IS 240 IS 340 IS342 IS407 IS455
Northern Virginia Community College	
Oklahoma City Community College (5)	CS116 CS2713 CS2723 CS2743 CS2783
Our Lady of the Lake University	
Prince George Community College (13)	BMT 2860 BMT 2880 FOS 2600 FOS 2610 INT 1010 INT 1620 INT 1680 INT 1700 INT 2300 INT 2680 INT 2690 INT2721

	INT2760
Rice University	
Richland College of the Dallas County Community College District	
Rochester Institute of Technology (18)	CSCI 141 CSCI 243 CSCI 250 CSEC 101 CSEC 210 CSEC 464 CSEC 465 CSEC 466 CSEC461 CSEC462 GCCISCSEC362 GCCISCSEC363 GCCISCSEC467 GCCISCSEC472 ISTE 230 NSSA 221 NSSA 241 NSSA 242
Rose State College (9)	CIT 2323 CIT 2533 CIT 2543 CIT 2553 CIT 2573 CIT 2603 CIT2513 CIT2523 CIT2563
San Antonio College	
Sinclair Community College	
Snead State Community College (2)	CIS 161 CIS 280
Southern Methodist University	
Southern Polytechnical State University (6)	IT 4533 IT 4823 IT 4833 IT 4843 IT 4853 IT 4903
St. Leo University (3)	COM 470 COM 475

	COM416
St. Philip's College	
Syracuse	
Texas A&M, San Antonio	
Texas A&M, Corpus Cristi	
Texas A&M University	
University of Tennessee at Chattanooga (6)	CPSC 4600 CPSC 4550 CPSC 4670 CPSC 4680 CPSC4610 CPSC4620
University of Texas – Austin	
University of Texas – El Paso	
University of Texas – San Antonio	
University of Texas – Dallas	
Towson University	
Tuskegee University	
University of Advancing Technology (18)	CFR210 CFR227 CFR255 CFR410 NTS201 NTS225 NTS310 NTS330 NTS350 NTS370 NTS415 NTS435 NTS442 NTS445 NTS465 NTW102 NTW213 NTW216
University of the District of Columbia (8)	CSCI315 CSCI351 CSCI352 CSCI353 CSCI412 CSCI441 CSCI453 CSCI455
University of Maryland University College(11)	CMIT265

	CMIT320 CMIT321 CMIT369 CMIT391 CMSC 412 CSIA 303 CSIA 412 CSIA 413 CSIA 485 CSIA301
United States Naval Academy	
University of Maryland, Baltimore County	
University of Maryland, College Park	
University of Dallas	
University of Houston	
University of North Texas	
University of Wilmington	
Valencia College(9)	CET 2830C CET 2880C CET 2890C CET 2894C CET 2830C CET 2892C CET 2660C CET 2881C CET 2994C
Whatcom Community College (5)	CIS 110 CIS 214 CIS 215 CIS 216 CIS 225

Appendix C – Mapping Survey Instrument

Institution

Course Number

Course Name

KSA	KSA Description	**Course Objective (copy in the column below from course description beside the KSA to which it maps)**
3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	Vulnerabilities Assessment
4	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data	Vulnerabilities Assessment
5	Ability to match the appropriate knowledge repository technology for a given application or environment	Knowledge Management
7	Knowledge of "knowledge base" capabilities for identifying the solutions to less common and more complex system problems	Knowledge Management
8	Knowledge of access authentication methods	Identity Management
9	Knowledge of applicable business processes and operations of customer organizations	Requirements Analysis
10	Knowledge of application vulnerabilities	Vulnerabilities Assessment
12	Knowledge of communication methods, principles, and concepts (e.g., cryptography, dual hubs, time multiplexers) that support the network infrastructure	Infrastructure Design
15	Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware	Hardware
16	Knowledge of capabilities and requirements analysis	Requirements Analysis
17	Knowledge of certified ethical hacking principles and techniques	Vulnerabilities Assessment
18	Knowledge of circuit analysis	Computers and Electronics
19	Knowledge of Computer Network Defense tools, including open source tools, and their capabilities	Computer Network Defense
20	Knowledge of complex data structures	Object Technology
21	Knowledge of computer algorithms	Mathematical Reasoning
22	Knowledge of computer networking fundamentals	Infrastructure Design
23	Knowledge of computer programming principles such as object-oriented design	Object Technology
24	Knowledge of concepts and practices of processing digital forensic data	Data Management
25	Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES).	Cryptography
27	Knowledge of cryptology	Cryptography
28	Knowledge of data administration and data standardization policies and standards	Data Management
29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics

31	Knowledge of data mining and data warehousing principles	Data Management
32	Knowledge of database management systems, query languages, table relationships, and views	Database Management Systems
33	Knowledge of database procedures used for documenting and querying reported incidents	Incident Management
34	Knowledge of database systems	Database Management Systems
35	Knowledge of digital rights management	Encryption
37	Knowledge of disaster recovery and continuity of operations plans.	Incident Management
38	Knowledge of organization's enterprise information security architecture system	Information Assurance
40	Knowledge of organization's evaluation and validation requirements	Systems Testing and Evaluation
41	Knowledge of organization's Local Area Network (LAN)/Wide Area Network (WAN) pathways	Infrastructure Design
42	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware	Hardware Engineering
43	Knowledge of embedded systems	Embedded Computers
44	Knowledge of enterprise messaging systems and associated software	Enterprise Architecture
46	Knowledge of fault tolerance	Information Assurance
49	Knowledge of host/network access controls (e.g., access control list)	Information Systems/Network Security
50	Knowledge of how network services and protocols interact to provide network communications	Infrastructure Design
51	Knowledge of how system components are installed, integrated, and optimized	Systems Integration
52	Knowledge of human-computer interaction principles	Human Factors
53	Knowledge of the Security Assessment and Authorization (SA&A) process	Information Assurance
55	Knowledge of Information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data	Information Assurance
56	Knowledge of information assurance (IA) principles and methods that apply to software development	Information Assurance
58	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins	Information Systems/Network Security
59	Knowledge of Intrusion Detection System (IDS) tools and applications	Computer Network Defense
60	Knowledge of incident categories, incident responses, and timelines for responses	Incident Management
61	Knowledge of incident response and handling methodologies	Incident Management
62	Knowledge of industry-standard and organizationally accepted analysis principles and methods	Logical Systems Design
63	Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
64	Knowledge of information security systems engineering principles	Information Systems/ Network Security
65	Knowledge of information theory	Mathematical Reasoning
66	Knowledge of intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies	Computer Network Defense
68	Knowledge of information technology (IT) architectural concepts and frameworks	Information Technology Architecture

69	Knowledge of Risk Management Framework (RMF) requirements	Information Systems Security Certification
70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)	Information Systems/Network Security
72	Knowledge of local area network (LAN) and wide area network (WAN) principles and concepts, including bandwidth management	Infrastructure Design
74	Knowledge of low level computer languages (e.g., assembly languages)	Computer Languages
75	Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics	Mathematical Reasoning
76	Knowledge of measures or indicators of system performance and availability	Information Technology Performance Assessment
77	Knowledege of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures, utilizing standards-based concepts and capabilities	Information Systems/Network Security
78	Knowledge of microprocessors	Computers and Electronics
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI])	Identity Management
81	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design
82	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs	Infrastructure Design
83	Knowledge of network hardware devices and functions	Hardware
87	Knowledge of network traffic analysis methods	Information Systems/Network Security
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
89	Knowledge of new technological developments in server administration	Technology Awareness
90	Knowledge of operating systems	Operating Systems
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])	Infrastructure Design
93	Knowledge of packet-level analysis	Vulnerabilities Assessment
94	Knowledge of parallel and distributed computing concepts	Information Technology Architecture
95	Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit)	Vulnerabilities Assessment
96	Knowledge of performance tuning tools and techniques	Information Technology Performance Assessment
98	Knowledge of policy-based and risk adaptive access controls	Identity Management
99	Knowledge of principles and methods for integrating server components	Systems Integration
100	Knowledge of Privacy Impact Assessments (PIA)	Personnel Safety and Security
101	Knowledge of process engineering concepts	Logical Systems Design
102	Knowledge of programming language structures and logic	Computer Languages
104	Knowledge of query languages such as Strcutured Query Language (SQL)	Database Management Systems
105	Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection.	Legal, Government and Jurisprudence
106	Knowledge of remote access technology concepts	Information Technology Architecture
107	Knowledge of resource management principles and techniques	Project Management

108	Knowledge of risk management processes, including steps and methods for assessing risk	Risk Management
109	Knowledge of secure configuration management techniques	Configuration Management
110	Knowledge of security management	Information Assurance
111	Knowledge of security system design tools, methods, and techniques	Information Systems/Network Security
112	Knowledge of server administration and systems engineering theories, concepts, and methods	Systems Life Cycle
113	Knowledge of server and client operating systems	Operating Systems
114	Knowledge of server diagnostic tools and fault identification techniques	Computer Forensics
115	Knowledge of content development	Computer Network Defense
116	Knowledge of software debugging principles	Software Development
117	Knowledge of software design tools, methods, and techniques	Software Development
118	Knowledge of software development models (e.g., waterfall model, spiral model)	Software Engineering
119	Knowledge of software engineering	Software Engineering
120	Knowledge of sources, characteristics, and uses of the organization's data assets	Data Management
121	Knowledge of structured analysis principles and methods	Logical Systems Design
122	Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems.	Operating Systems
123	Knowledge of system and application security threats and vulnerabilities	Vulnerabilities Assessment
124	Knowledge of system design tools, methods, and techniques, including automated system analysis and design tools	Logical Systems Design
126	Knowledge of system software and organizaional design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design	Requirements Analysis
127	Knowledge of systems administration concepts	Operating Systems
128	Knowledge of systems diagnostic tools and fault identification techniques	Systems Testing and Evaluation
129	Knowledge of systems lifecycle management principles, including software security and usability	Systems Life Cycle
130	Knowledge of systems testing and evaluation methods	Systems Testing and Evaluation
132	Knowledge of technoloy integration processes	Systems Integration
133	Knowledge of telecommunications concepts	Telecommunications
134	Knowledge of the capabilities and functionality associated with various content creation technologies (e.g., wikis, social networking, blogs)	Technology Awareness
135	Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines)	Data Management
136	Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint)	Technology Awareness
137	Knowledge of the characteristics of physical and virtual data storage media	Data Management
138	Knowledge of the computer network defense (CND) service provider reporting structure and processes within one's own organization	Information Systems/Network Security
139	Knowledge of common networking protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP]) and services (e.g., web, mail, Domain Name System [DNS]) and how they interact to provide network communications	Infrastructure Design
141	Knowledge of the enterprise information technology (IT) architecture	Information Technology Architecture

142	Knowledge of the operations and processes for diagnosing common or recurring system problems	Systems Life Cycle
143	Knowledge of the organization's enterprise information technology (IT) goals and objectives	Enterprise Architecture
144	Knowledge of the systems engineering process	Systems Life Cycle
145	Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly.	Systems Life Cycle
146	Knowledge of the types of Intrusion Detection System (IDS) hardware and software	Computer Network Defense
148	Knowledge of VPN security.	Encryption
149	Knowledge of web services, including service oriented architecture, Simple Object Access Protocol (SOAP), and web service description language	Web Technology
150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security
152	Skill in allocating storage capacity in the design of data management systems	Database Administration
153	Skill in handling malware	Computer Network Defense
154	Skill in analyzing network traffic capacity and performance characteristics	Capacity Management
155	Skill in applying and incorporating information technologies into proposed solutions	Technology Awareness
156	Skill in applying confidentiality, integrity, and availability principles	Information Assurance
157	Skill in applying host/network access controls (e.g., access control list)	Identity Management
158	Skill in applying organization-specific systems analysis principles and techniques	Systems Testing and Evaluation
160	Skill in assessing the robustness of security systems and designs	Vulnerabilities Assessment
162	Skill in conducting capabilities and requirements analysis	Requirements Analysis
163	Skill in conducting information searches	Computer Skills
164	Skill in conducting knowledge mapping (map of knowledge repositories)	Knowledge Management
165	Skill in conducting open source research for toubleshooting novel client-level problems	Knowledge Management
166	Skill in conducting queries and developing algorithms to analyze data structures	Database Management Systems
167	Skill in conducting server planning, management, and maintenance	Network Management
168	Skill in conducting software debugging	Software Development
169	Skill in conducting test events	Systems Testing and Evaluation
170	Skill in configuring and optimizing software	Software Engineering
171	Skill in correcting physical and technical problems which impact server performance	Network Management
172	Skill in creating and utilizing mathematical or statistical models	Modeling and Simulation
173	Skill in creating policies that relfect system security objectives	Information Systems Security Certification
174	Skill in creating programs that validate and process multiple inputs, including command line arguments, environmental variables, and input streams	Software Testing and Evaluation
175	Skill in developing and deploying signatures	Information Systems/Network Security
176	Skill in designing a data analysis structure (i.e., the types of data your test must generate and how to analyze those data)	Systems Testing and Evaluation
177	Skill in designing countermeasures to identified security risks	Vulnerabilities Assessment
178	Skill in designing databases	Database Administration

179	Skill in designing security controls based on information assurance (IA) principles and tenets	Information Assurance
180	Skill in designing the integration of hardware and software solutions	Systems Integration
181	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort)	Computer Network Defense
182	Skill in determining an appropriate level of test rigor for a given system	Systems Testing and Evaluation
183	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes	Information Assurance
185	Skill in developing applications that can log errors, exceptions, and application faults and logging	Software Development
186	Skill in developing data dictionaries	Data Management
187	Skill in developing data models	Modeling and Simulation
188	Skill in developing data repositories	Data Management
190	Skill in developing operations-based testing scenarios	Systems Testing and Evaluation
191	Skill in developing and applying security system access controls	Identity Management
193	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans	Information Assurance
194	Skill in diagnosing connectivity problems	Network Management
195	Skill in diagnosing failed servers	Network Management
197	Skill in discerning the protection needs (i.e., security controls) of information systems and networks	Information Systems/Network Security
198	Skill in establishing a routing schema	Infrastructure Design
199	Skill in evaluating the adequacy of security designs	Vulnerabilities Assessment
201	Skill in generating queries and reports	Database Management Systems
202	Skill in identifying and anticipating server performance, availability, capacity, or configuration problems	Information Technology Performance Assessment
203	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system	Information Technology Performance Assessment
204	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation	Systems Life Cycle
205	Skill in implementing, maintaining, and improving established security practices	Information Systems/Network Security
206	Skill in installing computer and server upgrades	Systems Life Cycle
207	Skill in installing, configuring, and troubleshooting local area network (LAN) and wide area network (WAN)	
208	Skill in maintaining databases	Database Management Systems
209	Skill in maintaining directory services	Identity Management
210	Skill in mimicking threat behaviors	Computer Network Defense
211	Skill in monitoring and optimizing server performance	Information Technology Performance Assessment
212	Skill in network mapping and recreating network topologies	Infrastructure Design
213	Skill in optimizing database performance	Database Administration
214	Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump)	Vulnerabilities Assessment
216	Skill in recovering failed servers	Incident Management
217	Skill in preserving evidence integrity according to standard operating procedures or national standards	Computer Forensics
219	Skill in system administration for Unix/Linux operating systems	Operating Systems
220	Skill in systems integration testing	Systems Testing and Evaluation
221	Skill in testing and configuring network workstations and peripherals	Network Management

222	Skill in the basic operation of computers	Computer Skills
223	Skill in the measuring and reporting of intellectual capital	Knowledge Management
224	Skill in the use of design modeling (e.g., unified modeling language)	Modeling and Simulation
225	Skill in the use of penetration testing tools and techniques	Vulnerabilities Assessment
226	Skill in the use of social engineering techniques	Human Factors
227	Skill in tuning sensors	Computer Network Defense
229	Skill in using incident handling methodologies	Incident Management
230	Skill in using knowledge management technologies	Knowledge Management
231	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol)	Network Management
233	Skill in using protocol analyzers	Vulnerabilities Assessment
234	Skill in using sub-netting tools	Infrastructure Design
235	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system	Computers and Electronics
237	Skill in using Virtual Private Network (VPN) devices and encryption	Encryption
238	Skill in writing code that is compatible with legacy code (e.g., Common Business-Oriented Language [COBOL], FORTRAN IV)in a modern programming language (e.g., Java, C++)	Computer Languages
239	Skill in writing test plans	Systems Testing and Evaluation
244	Ability to determine the validity of technology trend data	Technology Awareness
246	Knowledge and experience in the Instructional System Design (ISD) methodology	Multimedia Technologies
252	Knowledge of and experience in Insider Threat investigations, reporting, investigative tools and laws/regulations	Computer Network Defense
261	Knowledge of basic concepts, terminology, and operations of a wide range of communications media (computer and telephony networks, satellite, fiber, wireless)	Telecommunications
264	Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., central processing units [CPUs], network interface cards [NICs], data storage)	Computers and Electronics
269	Knowledge of CNE/CNA/CNO methodologies	Computer Network Defense
270	Knowledge of common adversary tactics, techniques, and procedures (TTPs) in assigned area of responsibility (e.g., historical country-specific TTPs, emerging capabilities)	Computer Network Defense
271	Knowledge of common network tools (e.g., ping, traceroute, nslookup)	Infrastructure Design
274	Knowledge of concepts, principles, methods, and tools related to processing and exploitation	Computer Network Defense
277	Knowledge of defense in-depth principles and network security architecture	Computer Network Defense
278	Knowledge of different types of network communication (e.g., Local Area Network [LAN], Wide Area Network [WAN], Metropolitan Area Network [MAN], Wireless Local Area Networm [WLAN], Wireless Wide Area Network [WWAN])	Telecommunications
281	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, electronic organizers, hard drives, memory cards, modems, network components, printers, removable storage devices, scanners, telephones, copiers, credit card skimmers, facsimile machines, global positioning systems [GPSs])	Hardware
282	Knowledge of emerging computer-based technology that has potential for exploitation by adversaries	Technology Awareness
284	Knowledge of encryption algorithms and tools for WLANs (e.g., SSL, PGP)	Cryptography

285	Knowledge of evasion strategies and techniques (e.g., noise, stealth, situational awareness, bandwidth throttling)	Computer Network Defense
286	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip)	Operating Systems
287	Knowledge of file system Implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extentsion [EXT])	Operating Systems
290	Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody)	Forensics
294	Knowledge of hacking methodologies in Windows or Unix/Linux environment	Surveillance
296	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise	External Awareness
297	Knowledge of industry indicators useful for identifying technology trends	Technology Awareness
299	Knowledge of information security program management and project management principles and techniques	Project Management
300	Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportability criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions	Organizational Awareness
302	Knowledge of investigative implications of hardware, operating systems, and network technologies	Computer Forensics
305	Knowledge of laws that affect cyber security (e.g., Wiretap Act, Pen/Trap and Trace Statue, Stored Electronic Communication Act)	Forensics
310	Knowledge of legal governance related to admissibility (e.g., Federal Rules of Evidence)	Criminal Law
313	Knowledge of logging services for network devices	Information Systems/Network Security
314	Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain	Teaching Others
316	Knowledge of processes for collecting, packaging, transporting and storing electronic evidence to avoid alteration, loss, physical damage or destruction of data.	Criminal Law
320	Knowledge of external organizations and academic institutions dealing with cybersecurity issues	External Awareness
321	Knowledge of products and nomenclature of major vendors (e.g., security suites)(Trend Micro, Symantec, McAfee, Outpost, Panda, Kaspersky, etc.) and how differences affect exploitation/vulnerabilities	Technology Awareness
322	Knowledge of router and routing processes, connections, protocols, and configuration (including their effects on operations)	Infrastructure Design
325	Knowledge of secure acquisitions (e.g., relevant Contracting Officer's Technical Representative [COTR] duties, secure procurement, supply chain risk management)	Contracting/Procurement
326	Knowledge of security hardware and software options, including the network artifacts they induce and their effects on exploitation	Information Systems/Network Security
327	Knowledge of security implications of software configurations	Information Assurance
329	Knowledge of surveillance detection and countermeasures	Surveillance
332	Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience	Teaching Others
336	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure [NII])	Telecommunications

337	Knowledge of the nexus between Cyber Counter-Intelligence and other Intelligence operations (i.e., How/ Where/ When Cyber Counter-Intelligence fits in, etc.)	External Awareness
338	Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing intelligence	Reasoning
339	Knowledge of the structure and intent of military operation plans, concept operation plans, orders, and standing rules of engagement	Organizational Awareness
340	Knowledge of types and collection of persistent data	Computer Forensics
341	Knowledge of UNIX and Windows systems that provide radius authentication, Domain Name Server, mail, web service, FTP server, DHCP, firewall, and simple network management protocol	Operating Systems
342	Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep)	Computer Languages
344	Knowledge of virtualization technologies and virtual machine development and maintenance	Operating Systems
345	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies	Web Technology
346	Knowledge of which system files (e.g. log files, registry files, configuration files) contain relevant information and where to find those system files	Computer Forensics
347	Knowledge of Windows command line (e.g., ipconfig, netstat, dir, nbtstat)	Operating Systems
348	Knowledge of wireless network collection tactics, techniques, and procedures to include decryption tools, techniques, and procedures	Cryptography
349	Skill in analyzing data from a variety of Computer Network Defense resources (e.g., signals intelligence, open source intelligence, Computer Network Defense tools)	Reasoning
350	Skill in analyzing memory dumps to extract information	Reasoning
352	Skill in applying white hack hacking/security auditing techniques, procedures and tools	Vulnerabilities Assessment
353	Skill in collecting data from a variety of Computer Network Defense resources (e.g., signals intelligence, open source intelligence, Computer Network Defense tools)	Computer Network Defense
355	Skill in creating plans in support of remote endpoint operations	Requirements Analysis
356	Skill in determining installed patches on various operating systems and identifying patch signatures	Operating Systems
357	Skill in determining the effects of various router configurations on traffic patterns and network performance in both LAN and WAN environments	Configuration Management
358	Skill in determining tactics, techniques, and procedures	Strategic Thinking
359	Skill in developing and executing technical training programs and curricula	Computer Forensics
360	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics)	Computer Forensics
361	Skill in gathering and analyzing all-source information in support of indications and warnings	Reasoning
363	Skill in identifying gaps in technical capabilities	Teaching Others
364	Skill in identifying, modifying, and manipulating applicable system components (Window and/or Unix/Linux) (e.g., passwords, user accounts, files)	Operating Systems
366	Skill in law enforcement report writing	Technical Documentation
367	Skill in multi-disciplined intelligence report writing	Writing

368	Skill in navigating mapping tools	Computer Skills
369	Skill in collecting, processing, packaging, transporting and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Forensics
371	Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, VBS) on Windows and UNIX systems (e.g., those that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data)	Operating Systems
374	Skill in setting up a forensic workstation	Forensics
375	Skill in survey, collection, and analysis of wireless LAN metadata	Network Management
376	Skill in talking to others to convey information effectively	Oral Communication
377	Skill in tracking and analyzing technical and legal trends that will impact cyber activities	Legal, Government and Jurisprudence
379	Skill in using common digital forensics tools and techniques	Computer Forensics
381	Skill in using forensic tool suites (e.g. EnCase, Sleuthkit, Forensic Tool Kit [FTK])	Computer Forensics
383	Skill in using scientific rules and methods to solve problems	Reasoning
385	Skill in using traceroute analysis tools	Network Management
386	Skill in using virtual machines	Operating Systems
387	Skill in verifying the integrity of encrypted files	Encryption
389	Skill in physically disassembling personal computers (PCs)	Computers and Electronics
886	Skill in wireless network target analysis, templating, and geolocation	Vulnerabilities Assessment
888	Knowledge of types of digital forensics data and how to recognize them	Computer Forensics
889	Knowledge of deployable forensics	Computer Forensics
890	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems)	Computer Forensics
891	Skill in configuring and utilizing hardware-based computer protection components (e.g., hardware firewalls, servers, routers)	Configuration Management
892	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware)	Configuration Management
893	Skill in securing network communications	Information Assurance
895	Skill in recognizing and categorizing types of vulnerabilities and associated attacks	Information Assurance
896	Skill in protecting a network against malware	Computer Network Defense
897	Skill in performing damage assessments	Information Assurance
899	Skill in gathering information from cyber social networks (e.g., MySpace, Facebook etc.)	Information Management
900	Knowledge of web filtering technologies	Web Technology
901	Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, Voice over Internet Protocol [VoIP], Instant Messenger [IM], web forums, direct video broadcasts)	Network Management
902	Knowledge of the range of existing networks (e.g., Private Branching Exchange [PBX], Local Area Networks [LANs], Wide Area Networks [WANs], Wireless Fiedlity [WI-FI])	Network Management
903	Knowledge of Wireless Fidelity (WI-FI)	Network Management
904	Knowledge of interpreted and compiled computer languages	Computer Languages
905	Knowledge of secure coding techniques	Computer Languages
907	Skill in data mining techniques	Data Management
908	Ability to decrypt digital data collections	Computer Forensics
909	Skill in processing collected data for follow-on analysis	Computer Skills

910	Knowledge of database theory	Data Management
911	Ability to interpret and translate customer requirements into operational cyber actions	Requirements Analysis
912	Knowledge of collection management processes, capabilities, and limitations	Configuration Management
913	Knowledge of how passive and active collections supplement each other	Information Management
914	Skill in identifying gaps in cyber collection capabilities	Strategic Thinking
915	Knowledge of front-end collection systems, including network traffic collection, filtering, and selection.	Information Systems/Network Security
916	Skill in deconflicting cyber operations and activities	Political Savvy
917	Knowledge of social dynamics of computer attackers in a global context	External Awareness
918	Ability to prepare and deliver education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures	Teaching Others
920	Knowledge of threat list countries' cyber capabilities, intent, opportunities, and presence	External Awareness
921	Ability to identify possible threat actor uses of a new technology	Technology Awareness
922	Skill in using network analysis tools to identify vulnerabilities	Vulnerabilities Assessment
923	Knowledge of security event correlation tools	Information Systems/Network Security
942	Knowledge of the organization's core business/mission processes	Organizational Awareness
950	Skill in evaluating test plans for applicability and completeness	Systems Testing and Evaluation
952	Knowledge of emerging security issues, risks, and vulnerabilities	Technology Awareness
954	Knowledge of Export Control regulations and responsible agencies for the purpose of reducing supply chain risk	Contracting/Procurement
965	Knowledge of organization's risk tolerance and/or risk management approach	Risk Management
966	Knowledge of enterprise incident response program, roles, and responsibilities	Incident Management
967	Knowledge of current and emerging threats/threat vectors	Information Systems/Network Security
968	Knowledge of software-related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization)	Information Systems/Network Security
973	Skill in using code analysis tools to eradicate bugs	Software Development
974	Ability to tailor code analysis for application-specific concerns	Software Testing and Evaluation
975	Skill in integrating black box security testing tools into quality assurance process of software releases	Quality Assurance
976	Knowledge of software quality assurance process	Software Engineering
978	Knowledge of root cause analysis for incidents	Incident Management
979	Knowledge of supply chain risk management processes and practices	Risk Management
980	Skill in performing root cause analysis for incidents	Incident Management
981	Knowledge of International Traffic in Arms Regulation (ITARs) and relevance to cybersecurity	Criminal Law
982	Knowledge of electronic evidence law	Criminal Law
984	Knowledge of computer network defense (CND) policies, procedures, and regulations	Computer Network Defense
985	Skill in configuring and utilizing network protection components (e.g., firewalls, Virtual Private Networks [VPNs], network Intrusion Detection Systems [IDSs])	Configuration Management

986	Knowledge of organizational information technology (IT) user security policies (e..g, account creation, password rules, access control)	Identity Management
989	Knowledge of Voice over Internet Protocol (VoIP)	Telecommunications
990	Knowledge of common attack vectors on the network layer	Computer Network Defense
991	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution)	Computer Network Defense
992	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], third generation [nation state sponsored]	Computer Network Defense
993	Knowledge of the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DODAF], Federal Enterprise Architecture Framework [FEAF])	Enterprise Architecture
1002	Skill in conducting audits or reviews of technical systems	Information Technology Performance Assessment
1004	Knowledge of critical information technology (IT) procrement requirements	Contracting/Procurement
1005	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes)	Contracting/Procurement
1007	Skills in data reduction	Data Management
1008	Knowledge of how to troubleshoot basic systems and identify operating systems-related issues	Operating Systems
1011	Knowledge of processes for reporting network security related incidents	Security
1012	Knowledge of Capabilities and Maturity Model Integration (CMMI) at all five levels	Internal Controls
1020	Skill in secure test plan deisn (i.e., unit, integration, system, acceptance)	Systems Testing and Evaluation
1021	Knowledge of threat assessment	Risk Management
1022	Knowledge of the nature and function of the relevant information structure	Enterprise Architecture
1029	Knowledge of malware analysis concepts and methodology	Computer Network Defense
1033	Knowledge of basic system administration, network, and operating system hardening techniques	Information Systems/Network Security
1034	Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards	Security
1036	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S Code), Presidential Directives, executive branch guidelines, and/or administrative/crimial legal guidelines and procedures relevant to work performed	Criminal Law
1037	Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures	Risk Management
1038	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability)	Infrastructure Design
1039	Skill in evaluating the trustworthiness of the supplier and/or product	Contracting/Procurement

1040	Knowledge of relevant laws, policies, procedures ,or governance as they relate to work that may impact critical infrastructure	Criminal Law
1042	Abililty to apply network programming towards client/server model	Requirements Analysis
1044	Skill in identifying forensic footprints	Computer Forensics
1047	Skill in writing kernel level applications	Software Development
1052	Knowledge of Global Systems for Mobile Communications (GSM) architecture	Telecommunications
1054	Knowledge of hardware reverse engineering techniques	Vulnerabilities Assessment
1055	Knowledge of middleware	Software Development
1056	Knowledge of operations security	Public Safety and Security
1059	Knowledge of networking protocols	Infrastructure Design
1061	Knowledge of the lifecycle process	Systems Life Cycle
1062	Knowledge of software reverse engineering techniques	Vulnerabilities Assessment
1063	Knowledge of Unix/Linux operating system structure and internals (e.g., process management, directory structure, installed applications)	Operating Systems
1064	Knowledge of Extensible Markup Language (XML) schemas	Infrastructure Design
1066	Skill in utlilizing exploitation tools (e.g., Foundstone, fuzzers, packet sniffers, debug) to identify system/software vulnerabilities (penetration and testing)	Vulnerabilities Assessment
1067	Skill in utlilizing network analysis tools to identify software communications vulnerabilities	Vulnerabilities Assessment
1069	Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks)	Computer Network Defense
1069	Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)	Computer Network Defense
1070	Ability to determine impact of technology trend data on laws, regulations, and/or policies	Legal, Government and Jurisprudence
1071	Knowledge of secure software deployment methodologies, tools, and practices	Software Engineering
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools	Network Management
1074	Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fiedelity [Wi-Fi]. paging, cellular, satellite dishes), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly	Telecommunications
1086	Knowledge of data carving tools and techniques (e.g., Foremost)	Computer Forensics
1087	Skill in deep analysis of captured malicious code (e.g., malware forensics)	Computer Network Defense
1088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump)	Computer Languages
1089	Knowledge of reverse engineering concepts	Vulnerabilities Assessment
1091	Skill in one way hash functions (e.g., Secure Hash Algorithm [SHA], Message Direct Algorithm [MD5])	Data Management

1092	Knowledge of anti-forensics tactics, techniques, and procedures (TTPs)	Computer Forensics
1093	Knowledge of common forensic tool configuration and support applications (e.g., VMWare, Wireshark)	Computer Forensics
1094	Knowledge of debugging procedures and tools	Software Development
1095	Knowledge of how different file types can be used for anomalous behavior	Vulnerabilities Assessment
1096	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro)	Computer Network Defense
1097	Knowledge of virtual machine aware malware, debugger aware malware, and packing	Computer Network Defense
1098	Skill in analyzing anomalous code as malcious or benign	Computer Network Defense
1099	Skill in analyzing volatile data	Computer Forensics
1100	Skill in identifying obfusification techniques	Computer Network Defense
1101	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures	Computer Network Defense
1114	Knowledge of encryption methodologies	Cryptography
1115	Skill in reading Hexadecimal data	Computer Languages
1116	Skill in identifying common encoding techniques (e.g., Exclusive Disjunction [XOR], American Standard Code for Information Interchange [ASCII], Unicode, Base64, Uuencode, Uniform Resource Locator [URL] encode)	Computer Languages
1117	Skill in utilizing virtual networks for testing	Operating Systems
1118	Skill in reading and interpreting signatures (e.g., Snort)	Information Systems/Network Security
1119	Knowledge of signature implementation impact	Information Systems/Network Security
1120	Ability to interpret and incorporate data from multiple tool sources	Data Management
1121	Knowledge of Windows/Unix ports and services	Operating Systems

Appendix D- Coding Instructions

1. Provide the student with the Course Description for each course he or she is assigned from the Google Docs folder at https://drive.google.com/?usp=folder&authuser=0#folders/0B2RgepdOeklKNE92Z29TbE5BaUE
2. Use a different KSA Mapping Template.xlsx spreadsheet for each course.
3. For each course, enter the Institution, Course Number and Course Name in the cells at the top of the spreadsheet.
4. In Column D, copy the entire course objective statement and paste it in the row with the KSA that best maps to the statement.
5. If the Course Objective does not map to a KSA, copy the course objective in at the bottom against a row without a KSA.
6. When finished, save the file with the name of the institution and course number (i.e. NVCCITN260)
7. This effort is for **undergraduate courses** only. Do not map Cisco CCNA courses.
8. The information will be in many different forms - you will have syllabi, course descriptions, and possibly, other documents. Look for the sections that describe the student learning objectives or course objectives within the document.
9. Learning objectives may map (will map) to more than KSA. Please map to as many as are relevant.

Appendix E- Pivot Table

B.S / A. (All)
Catego (All)
Course (All)

Count ‹ Column Labels

Row La	Bossier Parish Community College	Capella University	Capitol College	Champlain College	College of Southern Maryland	Florida State College at Jacksonville	Frances Tuttle	George Mason University	Hagerstown Community College	Highline Community College	Howard Community College	Jackson State Community College	Manhattan Area Technical College	Marymount University	Mass Bay Community College	Mercy College	Montgomery College	New Jersey City University	Norwich University	Oklahoma City Community College	Prince George's Community College	Rochester Institute of Technology	Rose State College	Snead State Community College	Southern PolyTech	St. Leo University	University of Advancing Technology	University of Maryland University College	University of Tennessee at Chattanooga	University of the District of Columbia	ValenciaCollege	ValenciaCollege	Whatcom Community College	Grand Total
3	3	4	3	2	1	4		1	1	1	3		1				1	2	1	1	2	2	1		1	2	2	2				2	43
4	2	3	2	2	1	6		2		1	3	1	1	1	1		1	2		1	2		1		2	2	1	1				2	41
5			1								3	1						2			1					1							9
7		1	1	1								2																					5
8	2	3	2	2			1	2			5		2		1	2	2		1		3	3	2			1		1		2			1	38
9			1			5					3	1								1	1		1			1	1						15
10	2	2	1					1			3		1				1	2			1	1	2		3	1	1						22
12	2	3	1	1	2		1	3	1		4	2		2							2	1	1		2	1	1		3	2		1	36
15			2	1		8		1	4	1	1	1	1			1	1				1	1					1			2		1	28
16						9										1																	10
17		1	2	1	1			1	2		1			1			1				1				1	2	1	1	1				18
18						2																											2
19	1			1	1			1	2		1	1	1	1								4					1		1	2			18
20																						1	1										2
21																						2							1	2			5
22	2			1	1	6			3		5	1	1	1									1						1	4			27
23			1				1							1							1	2					1						7
24	1		2	2					1		2	2	1	1							2			1			1			2			18
25	1		2	2	1	8	1	2	1		3	2	1	1			1	2	1		3	1	1		1		1		2	2		1	41
27	1		3	3	2		1	2			4	2	1	1	1			2	1		3		2		1	1		1	2	2	2	1	39
28				2	1						3	1									2					1		1	1				12
29	1	1	1	1		6				1	2	2		1	1		2		1	1	4		1						1		1	1	1	30
31			1								2	1	1	1							1												7
32			1			2				1		1		1					1		1	1	1						1				11
33	3	1			1		1					2		1							1			1		2			2			15
34			1			2				1		1		1					1		1	1							1		1		11
35			2			6						1	1									1	1			1			1	4			18
37	3	2	1		1	4				1	2	2	1				2	2	1	1	4	1	2			2			1	2	1		36
38		2	1	1				1			3	1	1				1				1	1	1	1		1	1	2				1	20
40			1																		2		1			2							6
41	1			1		2		1		1	1	1		1		1	1				1		1		1				2				16
42	2		1			4															1	1			1			1					11
43			1			6															1												8
44		1	2								1										1							1	2				8
46				1							1																						2
49	4	1	3	1	2		1	2	2		3	2	1	1	1		2			1	2		3	1	1			2	2	1		2	41
50	1	3	1	2		2	1	1	2		4	1	1	1		1	1			1	2		1				1	2	4				33
51			1	2							4												1										8
52						2					2															1								5
53		1	1					1									1							1								1	6
55	2	2	3	2	1						2	2	1					2	1		2	1	1		2	1							25
56	1		2											1				2			1		1						2				10
58		1	1	2	1			3	1		2	1	1				1							1	1	1			1	2		1	21
59	2	1	2			4	2	1	1	1	4	1	1	1						1	2	3	2			1		1	2		1	1	35
60	3	1	1	3	1	5	1				4	2								1	2	3	3		1		3		1		1		1	37
61	3	1	1	4	1		1				4	2									2	3	4		1		3		1		1		1	33
62			2	1							1										2		2			1	1						10
63	4		2	3		10	1	2			4	1	2		1		1	2			2	1	2		1							1	40
64	1	1	2		1			1			1	1					1			1	1			1						1		1	14
65								1																									1
66	1	1				4		1			3	1	1	1			1				1	2	3					1					21
68											2	1									2	1						2					8
69	2	1	2		1		1	1			1	2	1				1	2		2	3			1								1	22
70	2	1	3	4	2	4	1	2	1		4	2	3	1			3				3	1	3	1		2	3	1		2	2		2	53
72			1	1		4		1	2		1	2		1		1	1				1	1	1		1					2			21
74																						1											1
75			1			4																						1					6
76			1	1		4					1										1		1										9
77	2	1	1	3	1	4		2			2	3	2				1	2			3		2	1	1	1	6	2	2	2		1	45
78						2																											2
79	1		2	1		4		2		1	4	1				1	2				3		2					1	1	2	1		29
81	1	2	2	2		10	1	1	2		2	1		2			2			1	3	1	1						2	4			40

82		2	2		1	6	1	2	1		3	1	2	1		2	1						1	1	1	1			2			1	32
83			2			8		1	1		2	1	2	1							1						1						20
87	1	1	1	2	1	2	1	2			4	1	1				1				1		2	1			1		1		1	1	26
88	1	1		2		6		1	3				1	1			1							1	1		1	1				1	22
89			1	1					1							1												1				5
90	1	1	2	3		6	2		1	1	2			1				2			1				1			1	1	4			30
92	1	1		3		16	1	1	4	1	3	1	1	2		1	1			1	3	1	1				1	1	2	4	1		52
93			1	1				2			4		1				2				1		1			1	1						15
94												1									1								1				3
95	2	1	4	1	3			2	2		2			1			2				3	1	2		2	1	1				1		31
96			1	1		4					1																					7
98	1	1	4	2	2	2	1				3	1	2	1	1		1	2			2	1	3		2	2			2	2			38
99			2								1																					3
100		1	2														1							1	1						1	7
101			1									1																				2
102																						2					2					4
104			1									1		1					1		2	1						1				8
105	1	1		1				1		1	1	1	1	1							3			1	2	1	1	1		2			20
106			2							1	4	1				1	2				1							1		1		1	15
107			1			1			1		1	1		1					1						1							8
108	4	1	3	2	2		3		1		5	1	1				2	2	1	1	4	1	2		2	2		1	1				42
109	1	1									3	1	1	1							1					1							10
110	1	1		1					1		3	1	1	1			1			1	1		1	1		1			1		1	1	19
111	3	1	1	1	2			1	1		4	2	1				1	2			1	1	2	1	1	1	3		1	2		1	34
112			1			4						1				1					1								1		1	10
113	1	1	2	1		4	2			1	2			1							1				1		1		1	4			23
114	1	1	1							1		1		1			1				1								1				9
115								1				1																	1				3
116			2											1																2			5
117			1	1										1												1				2			6
118			1											1					1										1	2			6
119			1																											2			3
120											2	1		1																			4
121			2			2																	2			1							7
122	3	1	1	3	1	2			1	3	2	2				1	1				3				1		1	1	2	4			33
123	3	4	3	4	1		1	1	1		4		2		1	1	2				2	1	3	2	3	2	1		2			1	45
124	1		1	1							1							2			1		2			1						10
126			1	2	1	6					2					1			1		2		2		1	1			2			22
127		1	1	1								1				1					2							2	2			11
128			1			8															1		1									11
129	2	1	3								2	1	1				1	2			1		2	1		1			2			1	21
130	2		1			4					3		1	1				2			2		1										17
132			1								2							2															5
133	1	1	1	1		4					2	1		1							2		1						1			16
134		1	1									1							1														4
135			1							1	1	1		1															1				6
136		1	1																														2
137		1				10					3	1		1							1		1										18
138		1	1		1			1				1		1			1							1			1	1			1	1	11
139	3	2	2	3		12	2	1	2		2	1		2			3			1	3	1	1				1	3	4			49
141				1							2	1						2			2	1						1				10
142			1			6																	1										8
143						2					1	1				1										1		1					7
144			1															2															3
145			1			10					2							2					1			1							17
146	1	1	2				1	1		1	2	1	1	1			1			1	2	2	2					1		1	1		23
148		1	3	4	1					1	2		1				2				2	1	1	1		1			1			1	23
149			1	1												1	1				2								1				7
150	2	1	3	2	1			2	1		5	1	1	2	1	1	3				1	1	2	2	2	2	1		1	2		1	41
152			1									1																	1				3
153			2	1				1			2	1	1	1							1								1			1	12
154				1		4		1				1					1						1										9
155																					1								1				2
156	2		1	2		6		1	3		1	1	2				1	2			2		1				2						27
157	2		3		1		1	1	1	1	4	2	2		1		1			1	2		2		1			2		1		1	30
158			2																		1		1			1							5
160		1	1	1				1			2		1				1						3	1	1	2						1	16
162			1													1																	2
163			1						2																								3
164												1																					1
165			1									1																					2
166			1									1		1					1		1	1	1			1		1					9
167	1		2			8		1				1													1								14
168			2			1																											3
169			1								2			1							1		1										6
170			1						1		2										1												5
171	1	1	1	2				1				1																					7
172																													1				1
173		1	1	3	1		2		1		4		2		1		1	2	1		1		1	1	1	1	1		1			1	28
174			2			1								1							1					1							6
175		1	1		1	4		1	1			1	1				1							1			1					1	15

176			1																		1													2
177	3	3	4	2	1	6		1			4		1				2	2	1		2	1	1	1	2	3	1		1				1	43
178														1															1					2
179	1	1	1	2		6					3	1	1				1	2			1		1	1	1	1			2				1	27
180			2								1																							3
181	1	1						1			2	1	1	1							1	1	2				1		1					14
182			1								1			1							1		1											5
183	2	1	1	2									1				1	2			1		1	1			1						1	15
185	2																				2													4
186			1									1																						2
187			1											1							1								1					4
188												1																						1
190			1																		1		1				1							4
191	3	2	3	1	1	2	1		1		3	2	2		1		1			1	2		1	1	1				2		1		1	33
193	1	1					1	1		1	3	1	1				1			1	3		1			1	2	1	1					21
194						6		1				1																		2				10
195	1		1					1				1																						4
197	1	1	1	1	1			1			2	1	2		1		1	2		1	1	1		1	1		1		2	2			1	26
198		1																				1					1							3
199		1	1	1	1			1			2		1				1						1	1		2							1	14
201	1		1			2						1		1					1		1						1		1					10
202	1		2	2								1									1		1											8
203			1	1								1											1											4
204			1	1		2						1						2			1		1		1									10
205		1	2	1	1	2	1	1			2	2	1				1						3	1	2	1	1	1					1	25
206			2	1		4																											1	8
207				1				1	2	1		1		1		1					2		1							2				13
208			1							1		2									1								1		1			7
209												2					2																	4
210											2	1		1								1			1				1					7
211			1	1					1																			1						4
212			1	1		8	1		1	1		1		1							2						1			2			1	21
213																													1					1
214	1		2	3	1	4		2			3		1				1				1		1		2	1	3				2	1		29
216		1	1		1							2															1		1					7
217	1	1	1	1				2			2	1	1	1			1			1	3		2		1				1	2				22
219	3	1	1	2	1		1			3	1	1				1	1				4				1			1	2	4				28
220			1																		1		1											3
221						8					1	2									1		1							2				15
222			1																															1
223												1																	1					2
224																													1					1
225	1	1	2	1	3	4		2	2		3		1				2				2	3	2		2	1	1	1						34
226	2	1				4	1				1		2								1													12
227												1																						1
229	1	1	2	1	1		1				2	2											2			1	3		1					18
230												1																						1
231	1			1		6	1				1	1					1				1	1	1				3			2	1			21
233		1	1	1				1			1		1				1									1	1							9
234				1							1			1													1							4
235			1			2																												3
237	1		2	3	1		1				4		2				1				3	1	1			1			1		2			24
238			1			1						1																						3
239			1											1							1		1											4
252	1	1							1			2		1							1		1		2	1			3	2				16
261	2	3	3	1		11					1	2		1							3		1		1				1	2				32
264		1	1			19	1				1	1	1								3	1						1	1					31
269												1		1																				2
270												1									1								1					3
271	1			1	1							1		1							1	1			1					2	1			11
274			2		1						1	2		1								4					2			2				15
277		1	3		1				1		4	2	1				1				2	1	3	1			2		1	2			2	28
278	2	2	4	2		8			1	1	1	1	1	1			1				2	1	1		1			1	1	2				34
281	1		2			4	1			1	1	2					1	2			4			1				1	1					22
282				1																		1					1							3
284	2		3	1	2	4		2			2	2		1			1				2	1			1	1	1		2	2			1	31
285											1											2		1										4
286		1	1											1											1				1	2				7
287		1	1	2		6	1				1			1						1	1	1	1		1		1		1	4	1			25
290	1		1	1			1	1		2	3	2	1	1			1			1	2		1		1				2	2	1			25
294		2	1	1	1			1	1	1	1	1	1	1			1				3		1			1	1							19
296			2	1						1																								4
297			1									1																1						3
299	1	1	1	1							1	1	1	1			1		1					1	1	1			1	2	1	1	1	19
300	1	1	3		1					1				1		1			1		2		2	1	3	1	1		1					21
302		2	3	1								2		1			1				2	1	1	2	2				1	2			1	22
305		2	2	1			1				1	1					2		1		3	2	2	1	1				2				1	23
310		1	2	1				1					1	1							3		2	1	1	1								15
313	2	1	1	1	1							1		1			1				2			2						4	1		1	19
314										1																								1
316		1		1			1	1			2		1	1					1	1	5		2		1									18

320		1									1						1							1									1	5
321		1	1					1					2				1					1	1	1		1	1						1	12
322		1				6				2						1	2				2	2	1				1							18
325		1										2									1					2			1					7
326		1	2	1	1							1					1	2			1			2			1			2			1	16
327	1	1	1	3									2				1	2			2			1						2			1	17
329	3		1					1										2	1		2													10
332			2			2				1																		1						6
336		2	1																		1								1					5
337																		2																2
338	1		1																		1				1		1		1					6
339			1																									1						2
340	1	1	1			2					1	1		1			1								1		1	1	1	2				15
341	4	1	1	2	1	6	1	2	1	1		1		1			1				3	1	2	1	1	2	1	1	1	4			1	41
342	1								2	3	3			1							1							1		4		1		17
344	1	1	1	1						1	1			1						1						1			1					10
345			1																		2				1									4
346	1	1	1	1		6					2	1		1			1				1		1				1		1	2			1	22
347	1	1	1			6			2		3										3		1		1		1		1					21
348	1		5		1			2				2									3		2	1	2	1	1		1				1	23
349						4						1	1											1										7
350			2																															2
352		3	1	2	1	6		2	1	1	2		1				1			1	3	2	3	1	1	1							1	34
353	1								1			1												1			1							5
355												1				1																		2
356		1	2	1			1		1	1	2	1	1						1						1			1	1	2				17
357			1									1		1							2		1	1										7
358						4				2											1													7
359		1	1							1		1					1				3		1						1					10
360		1	2	1		4				1	2	2		1			1				2		1				1		1	2				22
363			1							1		1																						3
364	1	1	1	1	1	13	1			2	2	2					1				4				1	1	1	2	1	4		1		41
366		1									1										2								1			1	1	7
367											1																1		1					3
368									1																									1
369	1	1	1	2			1	1		2	2	1		1			1		1	1	2				1				1	2				22
371		1	1						2	2	1	1		1							3				1		2		1	4				20
374			1							1	1	1		1			1			1	2						1		1					11
375			1									1									1		2	1	1		1		1					9
376		2	1						4																			1	3					11
377		1	1							1				1							1			1	1	1	1	1						10
379	1	1	1	2						2	4	2		1			1				2	1			1		2		1	2			1	25
381	1	1	1	1						3	1	1		1			1				2	1	1		1		2		1		1			20
383			1																			1												2
385	1											1									1		1	1						2				7
386	1	1	1							1	1			1															1					7
387	2		2					1			1		2			1							1			1			1	2				14
389		1																																1
886		1	2					1				1					1				2		1		1	1		1						12
888	1	1	1	2								2	1	1			1				2		1		1				1	2				17
889		1	1								1	1		1			1				1		1						1					9
890		1	2				1				1	1		1			1			1	1	1					1		1					13
891	1		3	2	1		2				2	1	2	1			3		1		4		2			2		1	1		2		1	32
892	1		1	2	1	6	1					1	2	1			1				4	3	2			2	1	1	1		2			33
893		1	1	1								1	2					2			1								1					10
895	1		5	1		4		1	1		3		3	2		1	2		1		2	1	1		1	1	1				1			33
896			2	1		4					2	1	2								1	1											1	15
897			2		1						2																							5
899	1	1									1	1									1													5
900			1	1																1	3										1			7
901	1	2	3	1		4	1					2					2			1	2	1							1	2	1			24
902	2	1	1	1		4				1		1		1			1				1		1							2				17
903	2		1	1								1	1			1					1	1			1					2				12
904																											1							1
905												1																						1
907											1	1	1								1													4
908	2	1	1	1			1					2		1			1				1				1				1					13
909																									1									1
910												1		1							1								1					4
912												1		1							1													3
913												1																						1
914			1									1																						2
915		1	1	1	1	8		1				1	1				1				1		1	1							1		1	21
916																					1						1							2
917			3	2		6	1														3	1			1		1							18
918	1	2	1	1	2	3		2		2		2	1		1		1				1		1	1	1	1		1					1	26
920									1																1									2
921			2									1													2									5
922	1	1	2	1	2			1			3	2	1				1		1			1	3				3							23
923	1	1	1	1	1			1				1					1							1						2			1	12
942			3			2						2								1	1					1								10

950			1											1							1		2											5
952	3	1	2	2	1	12		2			1		1				1		1			1	1	1	2	1	1		1				1	36
954		1			1																								1						3
965	3	1	1	1	1	4	1				1	1					1	2			2		1		1	1									22
966	2	1		3	1						3	2									3	3	4		1		1		1			1			26
967	1	1	2		1			1	2			1	2		1	1							1	2	2	1	1		2			1	23
968		1	3	1	1		1	1			2	1	1				1	2			2			1			1			2	1		2	24
974						1															1														2
975		1	1					1			1						1						1	1									1	8
976														1					1									2						4
978	1	1	1		1							2		1							1		3				2		1					14
979	1	1	1		1						3	1					1	2			2		1			1								15
980	1	1			1							2								1	1		3				1		1					12
981		2						1									1				2		1	1									1	9
982		1	1	1				1			2		1	1					1		2		1		1									13
984	1			1	1	4						1		1	1						2				1		1		2					16
985	1		1	2	1	8	2		1	1	2	1	2				4		1	2	4	1	3			2			1	2	3	2		47
986	1	1	3	4	3	12	2	2			2	3	2	1	1	1	3			1	4		4	1	2	2			1	2	1		1	60
989		1	1	2			1						1	1					1		1		1						1		1			12
990			1	1			1	1			3	1	2	2		1			1		1	1								2				18
991	1		3				1					1		2			2				2									2	2			16
992			1									1	1	1		1					1				2					2				10
993													1								2		2				2		1					8
1002	1	1	1			4		1		1						1			1		1	1					1			2				16
1004																1																		1
1005		1		1				1								1	1				1			1									1	8
1007												1		1																				2
1008		1	1	2		7						1													1				1	2				16
1011	1	3		1	1		1	1			2	2	1	1			1						1	1	1		2		2	2			1	25
1012				1																									2					3
1020			1									1	1	1							1		1											6
1021	1	1	2			6	2				3	1	2				1	2			2		2		2	1			1					29
1022																					1								1					2
1029			2	2							1	2	1	1							2		1				1						1	14
1033	2	2	3	2	2	2	1	1				1		2	1		1				2		2	1	1		2		2	6	2		1	39
1034		1		2				1									1				1	1		1								1	9
1036	1	2	2	1		7		1			2			1					1	1	3		1	1	3	1			1					29
1037	1	1		1	1	8		1			3	1	1				2				2		1	1	1	1						1	27
1038		1	1	2		14					1	1				1										1							22
1040		2		1	1					1					1				1		2		2		1								12
1042			1	2								1															1							5
1044	1	1	2							1	1	2		1			1				2						1		2				15
1047																					1								2					3
1052		2	2											1							1		1				2							9
1054			2					1									1																	4
1056	2	2	1					1									1				1			1									1	10
1059	2			2			2		1		2	1		1		1					2		1						2					17
1061	1		1								1							2					2			1								8
1062			3					1									1																	5
1063	2	1	1	1		4	2			3	3	1		1			1				3				1		1	1	1	4				31
1064																				1														1
1066	1	2	1	1	1	4		2				1					1		1		2	3	2		1	1	1			1				26
1067		2	2	1	2			1				2					1					1	2				1		1			1		17
1069		1	2		2		4				2	4		4		2	4				4	2	2			1	1			4	1			40
1070		2			1							1			1						3		2	1	3	1	1							16
1071	1			2								1									1								2					7
1072	1	1	3	2	1	6		1	1		1	2	1				1				2		2	1			1		1	2			2	32
1073			2			10						1	1			1					2						1		1	2				21
1074	1	2	2	1							1	1						2			1		1						1					13
1086		1	1							2		1		1							1				1				1					9
1087			2	1								3									1		1				2		1				1	12
1088																													1			1			2
1089			2					1				1					1									1								6
1091			1					1				1								1	1						1	2	1				9
1092		1	1	1								1					1				2				1		1						9
1093	2	1	2	2						2	1	1		1			1				2	1			1		1		1	2				21
1094																					1														1
1095			1					1									1									1								4
1096	1		1	1							1	1									1	1					1						1	9
1097			1							1		1									3												1	7
1098			1									2																						3
1099		1	1								1	1					1				1						1		1				1	9
1100			1									2																						3
1101			1									1									1													3
1114	3		4	3	2	6	2	2	1	1	3	2	2	1	1				1		3	2	2		1	1	1		2	2	1		1	50
1115			1			4																							1			1			7
1116			2			4						1																	1						8
1117		2	2							1		1											1						1						8
1118		1	2					1		1		1	1				1							1			1		1				1	12
1119		1	2					1				1					1							1					1				1	9
1120		1	2	1							1	1		1													1							8

1121	3		3		3		2								2		1								2				3		1		1				1			1		2				1	26
(blank)																																					2							3	5
Grand `	225	224	436	257	107	638	83	138	91	87	381	291	138	142	21	42	178	84	40	41	425	122	243	78	139	103	155	48	207	250	54	14	100	##				

Appendix E- Pivot Table: College Course

School Capitol College

Count of Lo Column Labels

Row Labels	IAE 201	IAE 301	IAE 315	IAE 321	IAE 325	IAE 402	IAE405	IAE406	IAE410	Grand Total
Computer Forensics		1		1				19	4	25
Computer Languages	2				1				1	4
Computer Network Defense	3	4		1	2	5	7	1	6	29
Computer Skills							1		1	2
Computers and Electronics				1					1	2
Configuration Management			1	2					3	6
Criminal Law		1			1			2	1	5
Cryptography	5	3		1	4				3	16
Cryptography, 7.) Wired and wireless cryptographic solutions					1					1
Data Management	1	2			1		1	1	2	8
Database Administration									1	1
Database Management Systems									6	6
Embedded Computers									1	1
Encryption	1				4				4	9
Enterprise Architecture				1					1	2
External Awareness	2						1		2	5
Forensics					1			4		5
Hardware		1	1	3					1	6
Hardware Engineering				1						1
Identity Management	2	4	4			1			6	17
Incident Management		1				4	1		1	7
Information Assurance	3	2	1	2	6	3			4	21
Information Systems Security Certification						1			2	3
Information Systems/ Network Security					1				1	2
Information Systems/Network Security	3	4	2	4	3		1		21	38
Information Technology Architecture		1							1	2
Information Technology Performance Assessment			1						6	7
Infrastructure Design		2		1	5				3	11
Knowledge Management									3	3
Legal, Government and Jurisprudence									1	1
Logical Systems Design					2				4	6
Mathematical Reasoning				1						1
Modeling and Simulation							1			1
Network Management		1	1		2				8	12
Object Technology					1					1
Operating Systems	2	1	3						18	24
Oral Communication					1					1
Organizational Awareness	4				2				1	7
Personnel Safety and Security		1							1	2
Project Management					2					2

Public Safety and Security		1								1
Quality Assurance									1	1
Reasoning							2		2	4
Requirements Analysis				1	1				2	4
Risk Management		1	1			4			1	7
Software Development				3	1		1			5
Software Engineering				3						3
Software Testing and Evaluation				1					1	2
Strategic Thinking									1	1
Surveillance									2	2
Systems Integration				1	1				4	6
Systems Life Cycle			1	1	1				8	11
Systems Testing and Evaluation					1		1		11	13
Teaching Others								1	3	4
Technology Awareness						2			7	9
Telecommunications	1	1		1	7				4	14
Vulnerabilities Assessment		4	1	5	3	2	5	1	22	43
Web Technology									3	3
Grand Total	29	36	17	35	55	22	22	29	191	436

Row Labels
Bossier Parish Community College
- CIT 101
- CIT 115
- CIT 170
- CIT 172
- CIT 220
- CIT 224
- CIT 225
- CIT 272
- CIT 279
- CIT 280

Capella University
- IT 4070
- IT 4072
- IT 4071
- IT 4073
- IT 4074
- IT 4075
- IT 4076
- IT 4803

Capitol College
- IAE 201
- IAE 301
- IAE 315
- IAE 321
- IAE 325
- IAE 402
- IAE405
- IAE406
- IAE410

Champlain College
- CIT 130
- CIT 140
- FOR 240
- FOR 270
- FOR 320
- NET 225
- NET 255
- NET215
- NET320
- SEC 250
- SEC 335
- SEC 350
- SEC 440
- SEC345

College of Southern Maryland
- ITS2090
- ITS2500
- ITS2530
- ITS2535

Florida State College at Jacksonville
- CAP 2023
- CAP 2140
- CAP 2141
- CET 1114
- CET 1630
- CET 1936
- CET1173
- CET1513
- CET2172
- CET2179
- CET2588
- CET2600
- CET2629
- CET2662
- CET2687
- CET2752
- CET2759

Frances Tuttle
- CS2713
- CS2743
- CS2783
- ECS 2224
- ECS1214
- ECS2514

George Mason University
- IT 223
- IT 353
- IT 357
- IT 366
- IT 462
- IT 466

Hagerstown Community College
- CYB 101
- CYB 201
- CYB 225
- CYB 240
- CYB 245
- IST 108
- IST/CSC 109
- IST154
- IST155
- IST156

- IST160
- IST255
- IST261

Highline Community College

- CIS 115
- CIS 160
- CIS 161
- CIS 166
- CIS 210
- CIS 215
- CIS 216
- CIS 217
- CIS 230
- CIS 235
- CIS 236

Howard Community College

- CFOR 101
- CFOR 200
- CFOR 210
- CFOR 909
- CFOR 910
- CMSY 162
- CMSY 163
- CMSY 164
- CMSY 219
- CMSY 255
- CMSY 256
- CMSY 262
- CMSY 263

Jackson State Community College

- CIS 156
- CIS 259
- CIS250
- CIS251
- CIS257

Manhattan Area Technical College

- CRT 100
- CRT 282
- CRT 289

Marymount University

- IT305
- IT310
- IT315
- IT335
- IT355
- IT370
- IT390

Mass Bay Community College

- CS 116

Mercy College
- CISC 335
- CISC 359
- IASP 420
- IASP 440

Montgomery College
- MG 288
- NW 173
- NW 245
- NW 246
- NW 261
- NW 263
- NW 275

New Jersey City University
- SECU 222
- SECU 422

Norwich University
- CJ341
- IS 240
- IS 340
- IS342
- IS407
- IS455

Oklahoma City Community College
- CS116
- CS2713
- CS2723
- CS2743
- CS2783

Prince George's Community College
- BMT 2860
- BMT 2880
- FOS 2600
- FOS 2610
- INT 1010
- INT 1620
- INT 1680
- INT 1700
- INT 2300
- INT 2680
- INT 2690
- INT2721
- INT2760

Rochester Institute of Technology
- CSCI 141
- CSCI 243
- CSCI 250

- CSEC 101
- CSEC 210
- CSEC 464
- CSEC 465
- CSEC 466
- CSEC461
- CSEC462
- GCCISCSEC362
- GCCISCSEC363
- GCCISCSEC467
- GCCISCSEC472
- ISTE 230
- NSSA 221
- NSSA 241
- NSSA 242

Rose State College

- CIT 2323
- CIT 2533
- CIT 2543
- CIT 2553
- CIT 2573
- CIT 2603
- CIT2513
- CIT2523
- CIT2563

Snead State Community College

- CIS 161
- CIS 280

Southern PolyTech

- IT 4533
- IT 4823
- IT 4833
- IT 4843
- IT 4853
- IT 4903

St. Leo University

- COM 470
- COM 475
- COM416

University of Advancing Technology

- CFR210
- CFR227
- CFR255
- CFR410
- NTS201
- NTS225
- NTS310
- NTS330

- NTS350
- NTS370
- NTS415
- NTS435
- NTS442
- NTS445
- NTS465
- NTW102
- NTW213
- NTW216

University of Maryland University College

- CMIT265
- CMIT320
- CMIT321
- CMIT369
- CMIT391
- CMSC 412
- CSIA 303
- CSIA 412
- CSIA 413
- CSIA 485
- CSIA301

University of Tennessee at Chattanooga

- CPSC 4600
- CPSC 4550
- CPSC 4670
- CPSC 4680
- CPSC4610
- CPSC4620

University of the District of Columbia

- CSCI315
- CSCI351
- CSCI352
- CSCI353
- CSCI412
- CSCI441
- CSCI453
- CSCI455

ValenciaCollege

- CET 2830C
- CET 2880C
- CET 2890C
- CET 2894C
- CET2830C
- CET2892C

ValenciaCollege

- CET 2660C
- CET 2881C

- CET 2894C

Whatcom Community College

- CIS 110
- CIS 214
- CIS 215
- CIS 216
- CIS 225

Grand Total

Appendix E- Pivot Table: Data

School	B.S / A.	Degree	Course	Course	KSA	Description	Category	Lo
Champlain College	B.S.	Computer Networking &	CIT 140	100	28	Knowledge of data administration and	Data Management	Use appropriate data
Champlain College	B.S.	Computer Networking &	CIT 140	100	90	Knowledge of operating systems	Operating Systems	Explain the functions an
Champlain College	B.S.	Computer Networking &	CIT 140	100	122	Knowledge of system administration	Operating Systems	Perform standard operating system
Champlain College	B.S.	Computer Networking &	CIT 140	100	126	Knowledge of system software and	Requirements Analysis	Describe the function and
Champlain College	B.S.	Computer Networking &	CIT 140	100	219	Skill in system administration for	Operating Systems	Perform standard operating system
Champlain College	B.S.	Computer Networking &	CIT 140	100	287	Knowledge of file system	Operating Systems	Explain file system formats
Champlain College	B.S.	Computer Networking &	CIT 140	100	344	Knowledge of virtualization	Operating Systems	Explain virtualization and
Champlain College	B.S.	Computer Networking &	CIT 140	100	1071	Knowledge of secure software deployment	Software Engineering	Describe the concepts of
Champlain College	B.S.	Computer Networking &	CIT 140	100	1120	Ability to interpret and incorporate data	Data Management	Use appropriate data
Champlain College	B.S	Computer Networking &	FOR 270	200	24	Knowledge of concepts and	Data Management	9. Identify issues related to
Champlain College	B.S	Computer Networking &	FOR 270	200	27	Knowledge of cryptology	Cryptography	5. Classify different types of
Champlain College	B.S	Computer Networking &	FOR 270	200	360	Skill in identifying and extracting data of	Computer Forensics	4. Examine and demonstrate
Champlain College	B.S	Computer Networking &	FOR 270	200	369	Skill in collecting, processing,	Forensics	3. Explain how the use of
Champlain College	B.S	Computer Networking &	FOR 270	200	379	Skill in using common digital forensics tools	Computer Forensics	
Champlain College	B.S	Computer Networking &	FOR 270	200	888	Knowledge of types of digital forensics data	Computer Forensics	4. Examine and demonstrate
Champlain College	B.S	Computer Networking &	FOR 270	200	908	Ability to decrypt digital data collections	Computer Forensics	6. Describe methods of
Champlain College	B.S	Computer Networking &	FOR 270	200	1092	Knowledge of antiforensics tactics,	Computer Forensics	1. Compare and Contrast different
Champlain College	B.S	Computer Networking &	FOR 270	200	1093	Knowledge of common forensic tool	Computer Forensics	10. Describe the operation and
Champlain College	B.S	Computer Networking &	FOR 270	200	1114	Knowledge of encryption	Cryptography	5. Classify different types of
Champlain College	B.S.	Computer and Digital Forensics	FOR 320	300	287	Knowledge of file system	Operating Systems	2. Analyze and parse the FAT
Champlain College	B.S.	Computer and Digital Forensics	FOR 320	300	1029	Knowledge of malware analysis	Computer Network Defense	4. Using incident response and
Champlain College	B.S.	Computer and Digital Forensics	FOR 320	300	1087	Skill in deep analysis of captured malicious	Computer Network Defense	4. Using incident response and
Champlain College	B.S.	Computer and Digital Forensics	FOR 320	300	1096	Knowledge of malware analysis	Computer Network Defense	4. Using incident response and
Champlain College	B.S.	Computer Networking &	CIT 130	100	12	Knowledge of communication	Infrastructure Design	2.Describe how data is
Champlain College	B.S.	Computer Networking &	CIT 130	100	15	Knowledge of capabilities and	Hardware	7. Demonstrate knowledge of
Champlain College	B.S.	Computer Networking &	CIT 130	100	22	Knowledge of computer networking	Infrastructure Design	4. Discuss the structure and
Champlain College	B.S.	Computer Networking &	CIT 130	100	28	Knowledge of data administration and	Data Management	3. Explain and identify the role
Champlain College	B.S.	Computer Networking &	CIT 130	100	41	Knowledge of organization's Local	Infrastructure Design	4. Discuss the structure and
Champlain College	B.S.	Computer Networking &	CIT 130	100	50	Knowledge of how network services and	Infrastructure Design	6. Describe the operation of

Champlain College	B.S.	Computer Networking &	CIT 130	100	72	Knowledge of local area network (LAN)	Infrastructure Design	4. Discuss the structure and
Champlain College	B.S.	Computer Networking &	CIT 130	100	77	Knowledege of current industry	Information Systems/Network	3. Explain and identify the role
Champlain College	B.S.	Computer Networking &	CIT 130	100	81	Knowledge of network	Infrastructure Design	4. Discuss the structure and
Champlain College	B.S.	Computer Networking &	CIT 130	100	88	Knowledge of new and emerging	Technology Awareness	12. Understand the security
Champlain College	B.S.	Computer Networking &	CIT 130	100	90	Knowledge of operating systems	Operating Systems	14. Describe Network
Champlain College	B.S.	Computer Networking &	CIT 130	100	92	Knowledge of how traffic flows across	Infrastructure Design	4. Discuss the structure and
Champlain College	B.S.	Computer Networking &	CIT 130	100	110	Knowledge of security management	Information Assurance	12. Understand the security
Champlain College	B.S.	Computer Networking &	CIT 130	100	113	Knowledge of server and client operating	Operating Systems	13. Explain the role of clients,
Champlain College	B.S.	Computer Networking &	CIT 130	100	122	Knowledge of system administration	Operating Systems	14. Describe Network
Champlain College	B.S.	Computer Networking &	CIT 130	100	133	Knowledge of telecommunications	Telecommunications	2. Describe how data is
Champlain College	B.S.	Computer Networking &	CIT 130	100	139	Knowledge of common networking	Infrastructure Design	4. Discuss the structure and
Champlain College	B.S.	Computer Networking &	CIT 130	100	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	12. Understand the security
Champlain College	B.S.	Computer Networking &	CIT 130	100	207	Skill in installing, configuring, and		6. Describe the operation of
Champlain College	B.S.	Computer Networking &	CIT 130	100	212	Skill in network mapping and	Infrastructure Design	7. Demonstrate knowledge of
Champlain College	B.S.	Computer Networking &	CIT 130	100	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	9. Review the history and
Champlain College	B.S.	Computer Networking &	CIT 130	100	271	Knowledge of common network	Infrastructure Design	4. Discuss the structure and
Champlain College	B.S.	Computer Networking &	CIT 130	100	278	Knowledge of different types of	Telecommunications	6. Describe the operation of
Champlain College	B.S.	Computer Networking &	CIT 130	100	341	Knowledge of UNIX and Windows systems	Operating Systems	6. Describe the operation of
Champlain College	B.S.	Computer Networking &	CIT 130	100	901	Knowledge of the capabilities of	Network Management	8. Discuss the structure and
Champlain College	B.S.	Computer Networking &	CIT 130	100	902	Knowledge of the range of existing	Network Management	6. Describe the operation of
Champlain College	B.S.	Computer Networking &	CIT 130	100	952	Knowledge of emerging security	Technology Awareness	12. Understand the security
Champlain College	B.S.	Computer Networking &	CIT 130	100	986	Knowledge of organizational	Identity Management	12. Understand the security
Champlain College	B.S.	Computer Networking &	CIT 130	100	989	Knowledge of Voice over Internet Protocol	Telecommunications	4. Discuss the structure and
Champlain College	B.S.	Computer Networking &	CIT 130	100	1008	Knowledge of how to troubleshoot basic	Operating Systems	
Champlain College	B.S.	Computer Networking &	CIT 130	100	1034	Knowledge of Personally Identifiable	Security	3. Explain and identify the role
Champlain College	B.S.	Computer Networking &	CIT 130	100	1038	Knowledge of local specialized system	Infrastructure Design	
Champlain College	B.S.	Computer Networking &	CIT 130	100	1059	Knowledge of networking protocols	Infrastructure Design	4. Discuss the structure and
Champlain College	B.S.	Computer Networking &	CIT 130	100	1072	Knowledge of network security	Information Systems/Network	6. Describe the operation of
Champlain College	B.S.	Computer Networking &	CIT 130	100	1121	Knowledge of Windows/Unix ports	Operating Systems	14. Describe Network
Champlain College	B.S.	Computer Networking &	NET215	200	50	Knowledge of how network services and	Infrastructure Design	Discuss the protocol

Champlain College	B.S.	Computer Networking &	NET215	200	81	Knowledge of network	Infrastructure Design	Compare and contrast the
Champlain College	B.S.	Computer Networking &	NET215	200	87	Knowledge of network traffic	Information Systems/Network	Analyze performance of
Champlain College	B.S.	Computer Networking &	NET215	200	92	Knowledge of how traffic flows across	Infrastructure Design	Compare and contrast the
Champlain College	B.S.	Computer Networking &	NET215	200	139	Knowledge of common networking	Infrastructure Design	Compare and contrast the
Champlain College	B.S.	Computer Networking &	NET215	200	148	Knowledge of VPN security.	Encryption	Integrate IPsec, VPNs, VOIP into
Champlain College	B.S.	Computer Networking &	NET215	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	Analyze performance of
Champlain College	B.S.	Computer Networking &	NET215	200	233	Skill in using protocol analyzers	Vulnerabilities Assessment	Analyze performance of
Champlain College	B.S.	Computer Networking &	NET215	200	234	Skill in using subnetting tools	Infrastructure Design	Articulate and construct an
Champlain College	B.S.	Computer Networking &	NET215	200	237	Skill in using Virtual Private Network	Encryption	Integrate IPsec, VPNs, VOIP into
Champlain College	B.S.	Computer Networking &	NET215	200	989	Knowledge of Voice over Internet Protocol	Telecommunications	Discuss the protocol
Champlain College	B.S.	Computer Networking &	NET215	200	1059	Knowledge of networking protocols	Infrastructure Design	Discuss the protocol
Champlain College	B.S.	Computer Networking &	NET 225	200	4	Ability to identify systemic security	Vulnerabilities Assessment	4. Describe and analyze security
Champlain College	B.S.	Computer Networking &	NET 225	200	51	Knowledge of how system components	Systems Integration	1. Describe the components of a
Champlain College	B.S.	Computer Networking &	NET 225	200	123	Knowledge of system and application	Vulnerabilities Assessment	4 Describe and analyze security
Champlain College	B.S.	Computer Networking &	NET 225	200	139	Knowledge of common networking	Infrastructure Design	5. Describe and analyze the
Champlain College	B.S.	Computer Networking &	NET 225	200	149	Knowledge of web services, including	Web Technology	1.Describe the components of a
Champlain College	B.S.	Computer Networking &	NET 225	200	171	Skill in correcting physical and technical	Network Management	3. Analyze connectivity and
Champlain College	B.S.	Computer Networking &	NET 225	200	202	Skill in identifying and anticipating server	Information Technology	3. Analyze connectivity and
Champlain College	B.S.	Computer Networking &	NET 225	200	341	Knowledge of UNIX and Windows systems	Operating Systems	6. Analyze and design web
Champlain College	B.S.	Computer Networking &	NET 225	200	1042	Abililty to apply network	Requirements Analysis	2. Construct simple
Champlain College	B.S.	Computer Networking &	NET 255	200	51	Knowledge of how system components	Systems Integration	Install an operating system,
Champlain College	B.S.	Computer Networking &	NET 255	200	76	Knowledge of measures or	Information Technology	Analyze operating system
Champlain College	B.S.	Computer Networking &	NET 255	200	88	Knowledge of new and emerging	Technology Awareness	Apply the concepts of the
Champlain College	B.S.	Computer Networking &	NET 255	200	89	Knowledge of new technological	Technology Awareness	Apply the concepts of the
Champlain College	B.S.	Computer Networking &	NET 255	200	90	Knowledge of operating systems	Operating Systems	Discuss and compare the
Champlain College	B.S.	Computer Networking &	NET 255	200	96	Knowledge of performance tuning	Information Technology	Analyze operating system
Champlain College	B.S.	Computer Networking &	NET 255	200	122	Knowledge of system administration	Operating Systems	Perform common systems
Champlain College	B.S.	Computer Networking &	NET 255	200	127	Knowledge of systems administration	Operating Systems	Perform common systems
Champlain College	B.S.	Computer Networking &	NET 255	200	171	Skill in correcting physical and technical	Network Management	Analyze operating system
Champlain College	B.S.	Computer Networking &	NET 255	200	202	Skill in identifying and anticipating server	Information Technology	Analyze operating system

Champlain College	B.S.	Computer Networking &	NET 255	200	203	Skill in identifying measures or	Information Technology	Analyze operating system
Champlain College	B.S.	Computer Networking &	NET 255	200	204	Skill in identifying possible causes of	Systems Life Cycle	Analyze operating system
Champlain College	B.S.	Computer Networking &	NET 255	200	206	Skill in installing computer and server	Systems Life Cycle	Install an operating system,
Champlain College	B.S.	Computer Networking &	NET 255	200	211	Skill in monitoring and optimizing server	Information Technology	Analyze operating system
Champlain College	B.S.	Computer Networking &	NET 255	200	219	Skill in system administration for	Operating Systems	Perform common systems
Champlain College	B.S.	Computer Networking &	NET 255	200	282	Knowledge of emerging	Technology Awareness	Apply the concepts of the
Champlain College	B.S.	Computer Networking &	NET 255	200	356	Skill in determining installed patches on	Operating Systems	Perform common systems
Champlain College	B.S.	Computer Networking &	NET 255	200	364	Skill in identifying, modifying, and	Operating Systems	Configure essential services
Champlain College	B.S.	Computer Networking &	NET 255	200	1063	Knowledge of Unix/Linux operating	Operating Systems	Discuss and compare the
Champlain College	B.S.	Computer Networking &	NET 255	200	1121	Knowledge of Windows/Unix ports	Operating Systems	Discuss and compare the
Champlain College	B.S.	Computer Networking &	FOR 240	200	24	Knowledge of concepts and	Data Management	Demonstrate the ability to perform
Champlain College	B.S.	Computer Networking &	FOR 240	200	29	Knowledge of data backup, types of	Computer Forensics	Describe the underlying
Champlain College	B.S.	Computer Networking &	FOR 240	200	217	Skill in preserving evidence integrity	Computer Forensics	Apply current industry
Champlain College	B.S.	Computer Networking &	FOR 240	200	290	Knowledge of processes for seizing	Forensics	Articulate the laws applying to
Champlain College	B.S.	Computer Networking &	FOR 240	200	302	Knowledge of investigative	Computer Forensics	Describe the role of computer
Champlain College	B.S.	Computer Networking &	FOR 240	200	305	Knowledge of laws that affect cyber	Forensics	Articulate the laws applying to
Champlain College	B.S.	Computer Networking &	FOR 240	200	310	Knowledge of legal governance related to	Criminal Law	Articulate the laws applying to
Champlain College	B.S.	Computer Networking &	FOR 240	200	316	Knowledge of processes for	Criminal Law	best practices in securing,
Champlain College	B.S.	Computer Networking &	FOR 240	200	346	Knowledge of which system files (e.g. log	Computer Forensics	Demonstrate the ability to perform
Champlain College	B.S.	Computer Networking &	FOR 240	200	369	Skill in collecting, processing,	Forensics	The course content includes
Champlain College	B.S.	Computer Networking &	FOR 240	200	379	Skill in using common digital forensics tools	Computer Forensics	Demonstrate the ability to perform
Champlain College	B.S.	Computer Networking &	FOR 240	200	381	Skill in using forensic tool suites (e.g.	Computer Forensics	current technologies and
Champlain College	B.S.	Computer Networking &	FOR 240	200	888	Knowledge of types of digital forensics data	Computer Forensics	Describe the role of computer
Champlain College	B.S.	Computer Networking &	FOR 240	200	982	Knowledge of electronic evidence	Criminal Law	Articulate the laws applying to
Champlain College	B.S.	Computer Networking &	FOR 240	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	Articulate the laws applying to
Champlain College	B.S.	Computer Networking &	FOR 240	200	1093	Knowledge of common forensic tool	Computer Forensics	Describe the role of computer
Champlain College	B.S.	Computer Networking &	NET320	300	124	Knowledge of system design tools,	Logical Systems Design	Write programs to analyze
Champlain College	B.S.	Computer Networking &	NET320	300	1008	Knowledge of how to troubleshoot basic	Operating Systems	Develop programs to
Champlain College	B.S.	Computer Networking &	NET320	300	1042	Abililty to apply network	Requirements Analysis	Learn multiple approaches to a
Champlain College	B.S.	Computer Networking &	SEC 350	300	8	Knowledge of access authentication	Identity Management	Describe and implement

Champlain College	B.S.	Computer Networking &	SEC 350	300	60	Knowledge of incident categories, incident	Incident Management	Develop an Incident
Champlain College	B.S.	Computer Networking &	SEC 350	300	61	Knowledge of incident response and	Incident Management	Develop an Incident
Champlain College	B.S.	Computer Networking &	SEC 350	300	70	Knowledge of information	Information Systems/Network	Construct and maintain firewalls
Champlain College	B.S.	Computer Networking &	SEC 350	300	148	Knowledge of VPN security.	Encryption	Describe and implement
Champlain College	B.S.	Computer Networking &	SEC 350	300	173	Skill in creating policies that relfect	Information Systems Security	Develop and analyze
Champlain College	B.S.	Computer Networking &	SEC 350	300	237	Skill in using Virtual Private Network	Encryption	Describe and implement
Champlain College	B.S.	Computer Networking &	SEC 350	300	327	Knowledge of security implications of	Information Assurance	Plan and design security
Champlain College	B.S.	Computer Networking &	SEC 350	300	891	Skill in configuring and utilizing	Configuration Management	Construct and maintain firewalls
Champlain College	B.S.	Computer Networking &	SEC 350	300	892	Skill in configuring and utilizing	Configuration Management	Construct and maintain firewalls
Champlain College	B.S.	Computer Networking &	SEC 350	300	966	Knowledge of enterprise incident	Incident Management	Develop an Incident
Champlain College	B.S.	Computer Networking &	SEC 350	300	985	Skill in configuring and utilizing network	Configuration Management	Construct and maintain firewalls
Champlain College	B.S.	Computer Networking &	SEC 350	300	986	Knowledge of organizational	Identity Management	Develop and analyze
Champlain College	B.S.	Computer Networking &	SEC 335	300	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Students will learn the
Champlain College	B.S.	Computer Networking &	SEC 335	300	17	Knowledge of certified ethical	Vulnerabilities Assessment	Scenarios will provide
Champlain College	B.S.	Computer Networking &	SEC 335	300	19	Knowledge of Computer Network	Computer Network Defense	Apply best practices for
Champlain College	B.S.	Computer Networking &	SEC 335	300	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	Describe and discuss
Champlain College	B.S.	Computer Networking &	SEC 335	300	27	Knowledge of cryptology	Cryptography	Describe and discuss
Champlain College	B.S.	Computer Networking &	SEC 335	300	49	Knowledge of host/network access	Information Systems/Network	Apply best practices for
Champlain College	B.S.	Computer Networking &	SEC 335	300	58	Knowledge of known vulnerabilities from	Information Systems/Network	Analyze the security
Champlain College	B.S.	Computer Networking &	SEC 335	300	61	Knowledge of incident response and	Incident Management	Develop plans for incident response
Champlain College	B.S.	Computer Networking &	SEC 335	300	70	Knowledge of information	Information Systems/Network	Apply best practices for
Champlain College	B.S.	Computer Networking &	SEC 335	300	77	Knowledege of current industry	Information Systems/Network	Choose the appropriate
Champlain College	B.S.	Computer Networking &	SEC 335	300	95	Knowledge of penetration testing	Vulnerabilities Assessment	Students will learn the
Champlain College	B.S.	Computer Networking &	SEC 335	300	108	Knowledge of risk management	Risk Management	Analyze the security
Champlain College	B.S.	Computer Networking &	SEC 335	300	111	Knowledge of security system design tools,	Information Systems/Network	Describe the process for
Champlain College	B.S.	Computer Networking &	SEC 335	300	123	Knowledge of system and application	Vulnerabilities Assessment	Students will learn about
Champlain College	B.S.	Computer Networking &	SEC 335	300	148	Knowledge of VPN security.	Encryption	Describe and discuss
Champlain College	B.S.	Computer Networking &	SEC 335	300	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	Analyze the security
Champlain College	B.S.	Computer Networking &	SEC 335	300	173	Skill in creating policies that relfect	Information Systems Security	Articulate best practices and
Champlain College	B.S.	Computer Networking &	SEC 335	300	177	Skill in designing countermeasures to	Vulnerabilities Assessment	Apply best practices for

Champlain College	B.S.	Computer Networking &	SEC 335	300	179	Skill in designing security controls	Information Assurance	Apply best practices for
Champlain College	B.S.	Computer Networking &	SEC 335	300	183	Skill in determining how a security system	Information Assurance	Describe the process for
Champlain College	B.S.	Computer Networking &	SEC 335	300	191	Skill in developing and applying security	Identity Management	Apply best practices for
Champlain College	B.S.	Computer Networking &	SEC 335	300	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	Analyze the security
Champlain College	B.S.	Computer Networking &	SEC 335	300	205	Skill in implementing, maintaining, and	Information Systems/Network	Describe the process for
Champlain College	B.S.	Computer Networking &	SEC 335	300	225	Skill in the use of penetration testing	Vulnerabilities Assessment	Students will learn the
Champlain College	B.S.	Computer Networking &	SEC 335	300	229	Skill in using incident handling	Incident Management	Develop plans for incident response
Champlain College	B.S.	Computer Networking &	SEC 335	300	284	Knowledge of encryption algorithms	Cryptography	Describe and discuss
Champlain College	B.S.	Computer Networking &	SEC 335	300	294	Knowledge of hacking methodologies in	Surveillance	Analyze the security
Champlain College	B.S.	Computer Networking &	SEC 335	300	313	Knowledge of logging services for network	Information Systems/Network	Describe the process for
Champlain College	B.S.	Computer Networking &	SEC 335	300	326	Knowledge of security hardware and	Information Systems/Network	Describe ways to incorporate
Champlain College	B.S.	Computer Networking &	SEC 335	300	327	Knowledge of security implications of	Information Assurance	Describe ways to incorporate
Champlain College	B.S.	Computer Networking &	SEC 335	300	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	Students will learn the
Champlain College	B.S.	Computer Networking &	SEC 335	300	918	Ability to prepare and deliver education and	Teaching Others	increasing security
Champlain College	B.S.	Computer Networking &	SEC 335	300	923	Knowledge of security event correlation	Information Systems/Network	Describe the process for
Champlain College	B.S.	Computer Networking &	SEC 335	300	968	Knowledge of softwarerelated	Information Systems/Network	Apply best practices for
Champlain College	B.S.	Computer Networking &	SEC 335	300	1011	Knowledge of processes for	Security	Describe the process for
Champlain College	B.S.	Computer Networking &	SEC 335	300	1033	Knowledge of basic system	Information Systems/Network	Apply best practices for
Champlain College	B.S.	Computer Networking &	SEC 335	300	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	Students will learn the
Champlain College	B.S.	Computer Networking &	SEC 335	300	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	Students will learn the
Champlain College	B.S.	Computer Networking &	SEC 335	300	1071	Knowledge of secure software deployment	Software Engineering	Describe ways to incorporate
Champlain College	B.S.	Computer Networking &	SEC 335	300	1114	Knowledge of encryption	Cryptography	Describe and discuss
Champlain College	B.S.	Computer Networking &	SEC 350	300	8	Knowledge of access authentication	Identity Management	Describe and implement
Champlain College	B.S.	Computer Networking &	SEC 350	300	60	Knowledge of incident categories, incident	Incident Management	Develop an Incident
Champlain College	B.S.	Computer Networking &	SEC 350	300	61	Knowledge of incident response and	Incident Management	Develop an Incident
Champlain College	B.S.	Computer Networking &	SEC 350	300	70	Knowledge of information	Information Systems/Network	Construct and maintain firewalls
Champlain College	B.S.	Computer Networking &	SEC 350	300	148	Knowledge of VPN security.	Encryption	Describe and implement
Champlain College	B.S.	Computer Networking &	SEC 350	300	173	Skill in creating policies that relfect	Information Systems Security	Develop and analyze
Champlain College	B.S.	Computer Networking &	SEC 350	300	237	Skill in using Virtual Private Network	Encryption	Describe and implement
Champlain College	B.S.	Computer Networking &	SEC 350	300	327	Knowledge of security implications of	Information Assurance	Plan and design security

Champlain College	B.S.	Computer Networking &	SEC 350	300	891	Skill in configuring and utilizing	Configuration Management	Construct and maintain firewalls
Champlain College	B.S.	Computer Networking &	SEC 350	300	892	Skill in configuring and utilizing	Configuration Management	Construct and maintain firewalls
Champlain College	B.S.	Computer Networking &	SEC 350	300	966	Knowledge of enterprise incident	Incident Management	Develop an Incident
Champlain College	B.S.	Computer Networking &	SEC 350	300	985	Skill in configuring and utilizing network	Configuration Management	Construct and maintain firewalls
Champlain College	B.S.	Computer Networking &	SEC 350	300	986	Knowledge of organizational	Identity Management	Develop and analyze
Champlain College	B.S.	Computer Networking and	SEC 440	400	55	Knowledge of Information	Information Assurance	7. Develop strategies for
Champlain College	B.S.	Computer Networking and	SEC 440	400	60	Knowledge of incident categories, incident	Incident Management	6. Assess effectiveness of
Champlain College	B.S.	Computer Networking and	SEC 440	400	61	Knowledge of incident response and	Incident Management	4. Develop incident response
Champlain College	B.S.	Computer Networking and	SEC 440	400	63	Knowledge of Information	Information Assurance	3. Maintain the confidentiality,
Champlain College	B.S.	Computer Networking and	SEC 440	400	87	Knowledge of network traffic	Information Systems/Network	1. Analyze live network traffic
Champlain College	B.S.	Computer Networking and	SEC 440	400	92	Knowledge of how traffic flows across	Infrastructure Design	Analyze live network traffic
Champlain College	B.S.	Computer Networking and	SEC 440	400	93	Knowledge of packetlevel analysis	Vulnerabilities Assessment	Analyze live network traffic
Champlain College	B.S.	Computer Networking and	SEC 440	400	98	Knowledge of policybased and risk	Identity Management	7. Develop strategies for
Champlain College	B.S.	Computer Networking and	SEC 440	400	123	Knowledge of system and application	Vulnerabilities Assessment	2. Evaluate security threats
Champlain College	B.S.	Computer Networking and	SEC 440	400	150	Knowledge of what constitutes a network	Information Systems/Network	2. Evaluate security threats
Champlain College	B.S.	Computer Networking and	SEC 440	400	153	Skill in handling malware	Computer Network Defense	5. Analyze malware and
Champlain College	B.S.	Computer Networking and	SEC 440	400	154	Skill in analyzing network traffic	Capacity Management	Analyze live network traffic
Champlain College	B.S.	Computer Networking and	SEC 440	400	156	Skill in applying confidentiality,	Information Assurance	3. Maintain the confidentiality,
Champlain College	B.S.	Computer Networking and	SEC 440	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	7. Develop strategies for
Champlain College	B.S.	Computer Networking and	SEC 440	400	231	Skill in using network management tools to	Network Management	Analyze live network traffic
Champlain College	B.S.	Computer Networking and	SEC 440	400	896	Skill in protecting a network against	Computer Network Defense	5. Analyze malware and
Champlain College	B.S.	Computer Networking and	SEC 440	400	915	Knowledge of frontend collection	Information Systems/Network	Analyze live network traffic
Champlain College	B.S.	Computer Networking and	SEC 440	400	965	Knowledge of organization's risk	Risk Management	7. Develop strategies for
Champlain College	B.S.	Computer Networking and	SEC 440	400	966	Knowledge of enterprise incident	Incident Management	3. Develop incident response
Champlain College	B.S.	Computer Networking and	SEC 440	400	1029	Knowledge of malware analysis	Computer Network Defense	5. Analyze malware and
Champlain College	B.S.	Computer Networking and	SEC 440	400	1037	Knowledge of information	Risk Management	7. Develop strategies for
Champlain College	B.S.	Computer Networking &	SEC345	300	38	Knowledge of organization's	Information Assurance	Develop a comprehensive
Champlain College	B.S.	Computer Networking &	SEC345	300	46	Knowledge of fault tolerance	Information Assurance	Develop a comprehensive
Champlain College	B.S.	Computer Networking &	SEC345	300	55	Knowledge of Information	Information Assurance	Develop a comprehensive
Champlain College	B.S.	Computer Networking &	SEC345	300	62	Knowledge of industrystandard and	Logical Systems Design	Develop a comprehensive

Champlain College	B.S.	Computer Networking &	SEC345	300	63	Knowledge of Information	Information Assurance	Describe the issues of global IT
Champlain College	B.S.	Computer Networking &	SEC345	300	77	Knowledege of current industry	Information Systems/Network	Develop a comprehensive
Champlain College	B.S.	Computer Networking &	SEC345	300	126	Knowledge of system software and	Requirements Analysis	Describe government and
Champlain College	B.S.	Computer Networking &	SEC345	300	141	Knowledge of the enterprise	Information Technology	Develop a comprehensive
Champlain College	B.S.	Computer Networking &	SEC345	300	156	Skill in applying confidentiality,	Information Assurance	Develop a comprehensive
Champlain College	B.S.	Computer Networking &	SEC345	300	179	Skill in designing security controls	Information Assurance	Develop a comprehensive
Champlain College	B.S.	Computer Networking &	SEC345	300	183	Skill in determining how a security system	Information Assurance	Develop a comprehensive
Champlain College	B.S.	Computer Networking &	SEC345	300	296	Knowledge of how information needs	External Awareness	Develop a comprehensive
Champlain College	B.S.	Computer Networking &	SEC345	300	299	Knowledge of information security	Project Management	Develop a comprehensive
Champlain College	B.S.	Computer Networking &	SEC345	300	893	Skill in securing network	Information Assurance	Develop a comprehensive
Champlain College	B.S.	Computer Networking &	SEC345	300	917	Knowledge of social dynamics of computer	External Awareness	Describe the issues of global IT
Champlain College	B.S.	Computer Networking &	SEC345	300	952	Knowledge of emerging security	Technology Awareness	Describe the issues of global IT
Champlain College	B.S.	Computer Networking &	SEC345	300	1005	Knowledge of functionality, quality,	Contracting/Procurement	Describe government and
Champlain College	B.S.	Computer Networking &	SEC345	300	1012	Knowledge of Capabilities and	Internal Controls	Describe government and
Champlain College	B.S.	Computer Networking &	SEC345	300	1034	Knowledge of Personally Identifiable	Security	Describe government and
Champlain College	B.S.	Computer Networking &	SEC 250	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	3. Evaluate vulnerability of an
Champlain College	B.S.	Computer Networking &	SEC 250	200	4	Ability to identify systemic security	Vulnerabilities Assessment	4. Demonstrate how to detect
Champlain College	B.S.	Computer Networking &	SEC 250	200	7	Knowledge of “knowledge base”	Knowledge Management	4. Demonstrate how to detect
Champlain College	B.S.	Computer Networking &	SEC 250	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	5. Evaluate the authentication
Champlain College	B.S.	Computer Networking &	SEC 250	200	27	Knowledge of cryptology	Cryptography	5. Evaluate the authentication
Champlain College	B.S.	Computer Networking &	SEC 250	200	58	Knowledge of known vulnerabilities from	Information Systems/Network	3. Evaluate vulnerability of an
Champlain College	B.S.	Computer Networking &	SEC 250	200	63	Knowledge of Information	Information Assurance	5. Evaluate the authentication
Champlain College	B.S.	Computer Networking &	SEC 250	200	70	Knowledge of information	Information Systems/Network	5. Evaluate the authentication
Champlain College	B.S.	Computer Networking &	SEC 250	200	79	Knowledge of network access,	Identity Management	6. Explain the Public Key
Champlain College	B.S.	Computer Networking &	SEC 250	200	98	Knowledge of policybased and risk	Identity Management	3. Evaluate vulnerability of an
Champlain College	B.S.	Computer Networking &	SEC 250	200	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	4. Demonstrate how to detect
Champlain College	B.S.	Computer Networking &	SEC 250	200	108	Knowledge of risk management	Risk Management	3. Evaluate vulnerability of an
Champlain College	B.S.	Computer Networking &	SEC 250	200	117	Knowledge of software design tools,	Software Development	3. Evaluate vulnerability of an
Champlain College	B.S.	Computer Networking &	SEC 250	200	123	Knowledge of system and application	Vulnerabilities Assessment	3. Evaluate vulnerability of an
Champlain College	B.S.	Computer Networking &	SEC 250	200	150	Knowledge of what constitutes a network	Information Systems/Network	2, Understand common attack

Champlain College	B.S.	Computer Networking &	SEC 250	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	3. Evaluate vulnerability of an
Champlain College	B.S.	Computer Networking &	SEC 250	200	261	Knowledge of basic concepts,	Telecommunicatio ns	7. Demonstrate how to secure a
Champlain College	B.S.	Computer Networking &	SEC 250	200	278	Knowledge of different types of	Telecommunicatio ns	3. Evaluate vulnerability of an
Champlain College	B.S.	Computer Networking &	SEC 250	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	3.Evaluate vulnerability of an
Champlain College	B.S.	Computer Networking &	SEC 250	200	895	Skill in recognizing and categorizing	Information Assurance	2. Understand common attack
Champlain College	B.S.	Computer Networking &	SEC 250	200	900	Knowledge of web filtering technologies	Web Technology	4. Demonstrate how to detect
Champlain College	B.S.	Computer Networking &	SEC 250	200	903	Knowledge of Wireless Fidelity	Network Management	7. Demonstrate how to secure a
Champlain College	B.S.	Computer Networking &	SEC 250	200	917	Knowledge of social dynamics of computer	External Awareness	2. Understand common attack
Champlain College	B.S.	Computer Networking &	SEC 250	200	922	Skill in using network analysis tools to	Vulnerabilities Assessment	3. Evaluate vulnerability of an
Champlain College	B.S.	Computer Networking &	SEC 250	200	984	Knowledge of computer network	Computer Network Defense	8. Evaluate a company's
Champlain College	B.S.	Computer Networking &	SEC 250	200	986	Knowledge of organizational	Identity Management	8. Evaluate a company's
Champlain College	B.S.	Computer Networking &	SEC 250	200	990	Knowledge of common attack	Computer Network Defense	2. Understand common attack
Champlain College	B.S.	Computer Networking &	SEC 250	200	1033	Knowledge of basic system	Information Systems/Network	1. Understand the basics of
Champlain College	B.S.	Computer Networking &	SEC 250	200	1038	Knowledge of local specialized system	Infrastructure Design	3. Evaluate vulnerability of an
Champlain College	B.S.	Computer Networking &	SEC 250	200	1040	Knowledge of relevant laws,	Criminal Law	8. Evaluate a company's
Champlain College	B.S.	Computer Networking &	SEC 250	200	1072	Knowledge of network security	Information Systems/Network	4. Demonstrate how to detect
Champlain College	B.S.	Computer Networking &	SEC 250	200	1074	Knowledge of transmission records	Telecommunicatio ns	7. Demonstrate how to secure a
Champlain College	B.S.	Computer Networking &	SEC 250	200	1114	Knowledge of encryption	Cryptography	5. Evaluate the authentication
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	12	Knowledge of communication	Infrastructure Design	Use basic tools to properly design a
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	22	Knowledge of computer networking	Infrastructure Design	Use basic tools to properly design a
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	41	Knowledge of organization's Local	Infrastructure Design	Performance of NSTISS policies
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	42	Knowledge of electrical engineering	Hardware Engineering	Awareness of automated
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	88	Knowledge of new and emerging	Technology Awareness	Explore current internet trends
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	90	Knowledge of operating systems	Operating Systems	Awareness of automated
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	92	Knowledge of how traffic flows across	Infrastructure Design	Gain an understanding of
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	113	Knowledge of server and client operating	Operating Systems	Awareness of automated
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	122	Knowledge of system administration	Operating Systems	Explore basic networking on
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	133	Knowledge of telecommunications	Telecommunicatio ns	Awareness of system operating
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	139	Knowledge of common networking	Infrastructure Design	Gain an understanding of
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	219	Skill in system administration for	Operating Systems	Explore basic networking on

Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	281	Knowledge of electronic devices	Hardware	Awareness of automated
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	902	Knowledge of the range of existing	Network Management	Awareness of the capabilities and
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	952	Knowledge of emerging security	Technology Awareness	Explore current internet trends
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	1033	Knowledge of basic system	Information Systems/Network	Explore windows network security
Bossier Parish Community	A.S	Applied Science in Cyber	CIT 101	100	1059	Knowledge of networking protocols	Infrastructure Design	Gain an understanding of
Bossier Parish Community	A.S	Cyber Technology	CIT 115	100	108	Knowledge of risk management	Risk Management	Learn risk analysis factors and
Bossier Parish Community	A.S	Cyber Technology	CIT 115	100	108	Knowledge of risk management	Risk Management	Learn risk analysis factors and
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	49	Knowledge of host/network access	Information Systems/Network	Learn discretionary
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	50	Knowledge of how network services and	Infrastructure Design	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	81	Knowledge of network	Infrastructure Design	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	87	Knowledge of network traffic	Information Systems/Network	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	111	Knowledge of security system design tools,	Information Systems/Network	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	114	Knowledge of server diagnostic tools and	Computer Forensics	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	129	Knowledge of systems lifecycle management	Systems Life Cycle	Explore NSTISS policies and
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	167	Skill in conducting server planning,	Network Management	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	171	Skill in correcting physical and technical	Network Management	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	177	Skill in designing countermeasures to	Vulnerabilities Assessment	Understand the insurance of
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	191	Skill in developing and applying security	Identity Management	Demonstrate knowledge on the
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	195	Skill in diagnosing failed servers	Network Management	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	202	Skill in identifying and anticipating server	Information Technology	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	237	Skill in using Virtual Private Network	Encryption	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	341	Knowledge of UNIX and Windows systems	Operating Systems	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 170	100	985	Skill in configuring and utilizing network	Configuration Management	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 172	100	386	Skill in using virtual machines	Operating Systems	Install Ubuntu into a virtual
Bossier Parish Community	A.S	Cyber Technology	CIT 172	100	1063	Knowledge of Unix/Linux operating	Operating Systems	Explore the EXT3 file system
Bossier Parish Community	A.S	Cyber Technology	CIT 220	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 220	200	4	Ability to identify systemic security	Vulnerabilities Assessment	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 220	200	22	Knowledge of computer networking	Infrastructure Design	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 220	200	42	Knowledge of electrical engineering	Hardware Engineering	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 220	200	49	Knowledge of host/network access	Information Systems/Network	Demonstrate knowledge of

Bossier Parish Community	A.S	Cyber Technology	CIT 220	200	111	Knowledge of security system design tools,	Information Systems/Network	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 220	200	123	Knowledge of system and application	Vulnerabilities Assessment	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 220	200	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 220	200	139	Knowledge of common networking	Infrastructure Design	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 220	200	157	Skill in applying host/network access	Identity Management	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 220	200	191	Skill in developing and applying security	Identity Management	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	33	Knowledge of database procedures	Incident Management	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	37	Knowledge of disaster recovery and	Incident Management	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	55	Knowledge of Information	Information Assurance	Demonstrate knowledge of risk
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	60	Knowledge of incident categories, incident	Incident Management	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	61	Knowledge of incident response and	Incident Management	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	63	Knowledge of Information	Information Assurance	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	64	Knowledge of information security	Information Systems/ Network	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	69	Knowledge of Risk Management	Information Systems Security	Demonstrate knowledge of risk
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	70	Knowledge of information	Information Systems/Network	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	108	Knowledge of risk management	Risk Management	Demonstrate knowledge of risk
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	156	Skill in applying confidentiality,	Information Assurance	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	183	Skill in determining how a security system	Information Assurance	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	229	Skill in using incident handling	Incident Management	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	284	Knowledge of encryption algorithms	Cryptography	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	300	Knowledge of intelligence reporting	Organizational Awareness	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	387	Skill in verifying the integrity of encrypted	Encryption	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	965	Knowledge of organization's risk	Risk Management	Demonstrate knowledge of risk
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	966	Knowledge of enterprise incident	Incident Management	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	978	Knowledge of root cause analysis for	Incident Management	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	980	Skill in performing root cause analysis for	Incident Management	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	1011	Knowledge of processes for	Security	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	1056	Knowledge of operations security	Public Safety and Security	Demonstrate knowledge of

Bossier Parish Community	A.S	Cyber Technology	CIT 224	200	1114	Knowledge of encryption	Cryptography	Demonstrate knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Carry out vulnerability
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	8	Knowledge of access authentication	Identity Management	Deploy various authentication
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	10	Knowledge of application	Vulnerabilities Assessment	Carry out the appropriate
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	12	Knowledge of communication	Infrastructure Design	Explain general cryptography,
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	19	Knowledge of Computer Network	Computer Network Defense	Determine the appropriate use
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	Differentiate between the
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	27	Knowledge of cryptology	Cryptography	Explain general cryptography,
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	33	Knowledge of database procedures	Incident Management	Differentiate between and
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	37	Knowledge of disaster recovery and	Incident Management	Implement disaster recovery
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	49	Knowledge of host/network access	Information Systems/Network	Identify and apply industry best
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	59	Knowledge of Intrusion Detection	Computer Network Defense	Determine the appropriate use
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	60	Knowledge of incident categories, incident	Incident Management	Differentiate between and
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	61	Knowledge of incident response and	Incident Management	Differentiate between and
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	63	Knowledge of Information	Information Assurance	Explain the difference
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	69	Knowledge of Risk Management	Information Systems Security	Conduct risk assessments and
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	77	Knowledege of current industry	Information Systems/Network	Determine the appropriate use
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	79	Knowledge of network access,	Identity Management	Explain and implement PKI
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	Determine the appropriate use
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	98	Knowledge of policybased and risk	Identity Management	Identify and apply industry best
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	111	Knowledge of security system design tools,	Information Systems/Network	Determine the appropriate use
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	123	Knowledge of system and application	Vulnerabilities Assessment	Differentiate among various
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	139	Knowledge of common networking	Infrastructure Design	Explain and implement
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	150	Knowledge of what constitutes a network	Information Systems/Network	Differentiate among various
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	157	Skill in applying host/network access	Identity Management	Identify and apply industry best
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	Learn the NSTISS basics
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	185	Skill in developing applications that can	Software Development	Execute proper logging
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	191	Skill in developing and applying security	Identity Management	Identify and apply industry best
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	Determine the appropriate use
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	226	Skill in the use of social engineering	Human Factors	Explain the concept of and

Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	231	Skill in using network management tools to	Network Management	Apply the appropriate
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	261	Knowledge of basic concepts,	Telecommunications	Explain the vulnerabilities
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	271	Knowledge of common network	Infrastructure Design	Determine the appropriate use
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	278	Knowledge of different types of	Telecommunications	Explain the vulnerabilities
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	284	Knowledge of encryption algorithms	Cryptography	Determine the appropriate use
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	313	Knowledge of logging services for network	Information Systems/Network	Execute proper logging
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	329	Knowledge of surveillance detection	Surveillance	Learn the NSTISS basics
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	341	Knowledge of UNIX and Windows systems	Operating Systems	Deploy various authentication
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	344	Knowledge of virtualization	Operating Systems	Explain the purpose and
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	353	Skill in collecting data from a variety of	Computer Network Defense	Apply the appropriate
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	385	Skill in using traceroute analysis	Network Management	Apply the appropriate
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	387	Skill in verifying the integrity of encrypted	Encryption	Explain general cryptography,
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	899	Skill in gathering information from	Information Management	Explain the concept of and
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	903	Knowledge of Wireless Fidelity	Network Management	Explain the vulnerabilities
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	908	Ability to decrypt digital data collections	Computer Forensics	Explain general cryptography,
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	922	Skill in using network analysis tools to	Vulnerabilities Assessment	Apply the appropriate
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	923	Knowledge of security event correlation	Information Systems/Network	Apply the appropriate
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	952	Knowledge of emerging security	Technology Awareness	Conduct risk assessments and
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	965	Knowledge of organization's risk	Risk Management	Conduct risk assessments and
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	966	Knowledge of enterprise incident	Incident Management	Differentiate between and
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	967	Knowledge of current and emerging	Information Systems/Network	Differentiate among various
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	984	Knowledge of computer network	Computer Network Defense	Identify and explain applicable
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	986	Knowledge of organizational	Identity Management	Identify and apply industry best
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	1002	Skill in conducting audits or reviews of	Information Technology	Conduct periodic audits of system
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	1033	Knowledge of basic system	Information Systems/Network	Implement OS hardening
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	1059	Knowledge of networking protocols	Infrastructure Design	Differentiate between the
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	Apply the appropriate
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	1072	Knowledge of network security	Information Systems/Network	Explain and implement
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	1074	Knowledge of transmission records	Telecommunications	Explain the vulnerabilities
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	1093	Knowledge of common forensic tool	Computer Forensics	Use monitoring tools on systems

Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	1096	Knowledge of malware analysis	Computer Network Defense	Apply the appropriate
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	1114	Knowledge of encryption	Cryptography	Explain general cryptography,
Bossier Parish Community	A.S	Cyber Technology	CIT 225	200	1121	Knowledge of Windows/Unix ports	Operating Systems	Differentiate between the
Bossier Parish Community	A.S	Cyber Technology	CIT 272	200	122	Knowledge of system administration	Operating Systems	Navigate the Linux directories,
Bossier Parish Community	A.S	Cyber Technology	CIT 272	200	219	Skill in system administration for	Operating Systems	Navigate the Linux
Bossier Parish Community	A.S	Cyber Technology	CIT 272	200	341	Knowledge of UNIX and Windows systems	Operating Systems	Discuss aspects of security, including
Bossier Parish Community	A.S	Cyber Technology	CIT 272	200	364	Skill in identifying, modifying, and	Operating Systems	Navigate the Linux directories,
Bossier Parish Community	A.S	Cyber Technology	CIT 272	200	901	Knowledge of the capabilities of	Network Management	Discuss aspects of security, including
Bossier Parish Community	A.S	Cyber Technology	CIT 272	200	1063	Knowledge of Unix/Linux operating	Operating Systems	Navigate the Linux directories,
Bossier Parish Community	A.S	Cyber Technology	CIT 272	200	1121	Knowledge of Windows/Unix ports	Operating Systems	Manage a LAN using Linux
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	4	Ability to identify systemic security	Vulnerabilities Assessment	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	8	Knowledge of access authentication	Identity Management	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	10	Knowledge of application	Vulnerabilities Assessment	Explain vulnerability
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	29	Knowledge of data backup, types of	Computer Forensics	Discuss backups; Explain the
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	33	Knowledge of database procedures	Incident Management	Explain the importance
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	37	Knowledge of disaster recovery and	Incident Management	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	49	Knowledge of host/network access	Information Systems/Network	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	55	Knowledge of Information	Information Assurance	Gain knowledge on the standards
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	56	Knowledge of information assurance	Information Assurance	Gain knowledge on the standards
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	59	Knowledge of Intrusion Detection	Computer Network Defense	Learn how to detect intrusion
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	60	Knowledge of incident categories, incident	Incident Management	Learn how to describe threats
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	61	Knowledge of incident response and	Incident Management	Learn how to describe threats
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	63	Knowledge of Information	Information Assurance	Gain knowledge on the standards
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	66	Knowledge of intrusion detection	Computer Network Defense	Learn how to detect intrusion
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	70	Knowledge of information	Information Systems/Network	Learn the description of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	77	Knowledege of current industry	Information Systems/Network	Learn the description of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	learn about security testing;
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	108	Knowledge of risk management	Risk Management	Understand NSTISS basics
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	109	Knowledge of secure configuration	Configuration Management	Discuss configuration

Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	110	Knowledge of security management	Information Assurance	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	122	Knowledge of system administration	Operating Systems	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	123	Knowledge of system and application	Vulnerabilities Assessment	Explore NSTISS basics threats to
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	124	Knowledge of system design tools,	Logical Systems Design	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	129	Knowledge of systems lifecycle management	Systems Life Cycle	Gain an a awareness
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	learn about security testing;
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	146	Knowledge of the types of Intrusion	Computer Network Defense	Learn how to detect intrusion;
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	150	Knowledge of what constitutes a network	Information Systems/Network	Explore NSTISS basics threats to
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	156	Skill in applying confidentiality,	Information Assurance	Learn the fundamentals of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	Learn NSTISS basics
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	179	Skill in designing security controls	Information Assurance	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	181	Skill in detecting host and network based	Computer Network Defense	Learn how to detect intrusion;
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	183	Skill in determining how a security system	Information Assurance	Gain knowledge on the standards
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	185	Skill in developing applications that can	Software Development	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	193	Skill in developing, testing, and	Information Assurance	Define business recoveryExplain
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	Learn the NSTISS basics facets of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	201	Skill in generating queries and reports	Database Management	Discuss risk analyst's reports
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	219	Skill in system administration for	Operating Systems	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	learn about security testing;
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	226	Skill in the use of social engineering	Human Factors	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	261	Knowledge of basic concepts,	Telecommunicatio ns	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	278	Knowledge of different types of	Telecommunicatio ns	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	299	Knowledge of information security	Project Management	Learn INFOSEC security basics
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	313	Knowledge of logging services for network	Information Systems/Network	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	327	Knowledge of security implications of	Information Assurance	Learn the NSTISS policies and
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	329	Knowledge of surveillance detection	Surveillance	Learn NSTISS basics
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	338	Knowledge of the principal methods,	Reasoning	Discuss risk analyst's reports
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	341	Knowledge of UNIX and Windows systems	Operating Systems	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	342	Knowledge of Unix command line (e.g.,	Computer Languages	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	347	Knowledge of Windows command	Operating Systems	Demonstrate knowledge on

Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	348	Knowledge of wireless network collection	Cryptography	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	891	Skill in configuring and utilizing	Configuration Management	Learn the NSTISS basics facets of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	892	Skill in configuring and utilizing	Configuration Management	Learn the NSTISS basics facets of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	895	Skill in recognizing and categorizing	Information Assurance	Discuss and explain the
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	902	Knowledge of the range of existing	Network Management	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	903	Knowledge of Wireless Fidelity	Network Management	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	918	Ability to prepare and deliver education and	Teaching Others	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	952	Knowledge of emerging security	Technology Awareness	Explain the importance of
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	965	Knowledge of organization's risk	Risk Management	Understand NSTISS basics
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	979	Knowledge of supply chain risk	Risk Management	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	991	Knowledge of different classes of	Computer Network Defense	Discuss and explain the
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	1021	Knowledge of threat assessment	Risk Management	Understand NSTISS basics
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	1037	Knowledge of information	Risk Management	Understand NSTISS basics
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	1056	Knowledge of operations security	Public Safety and Security	understand security basics
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	1061	Knowledge of the lifecycle process	Systems Life Cycle	Understand the NSTISS planning
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	1071	Knowledge of secure software deployment	Software Engineering	Learn the NSTISS policies and
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	1114	Knowledge of encryption	Cryptography	Learn how to describe
Bossier Parish Community	A.S	Cyber Technology	CIT 279	200	1121	Knowledge of Windows/Unix ports	Operating Systems	Demonstrate knowledge on
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	24	Knowledge of concepts and	Data Management	Learn necessary forensic
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	63	Knowledge of Information	Information Assurance	Explain the importance and
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	217	Skill in preserving evidence integrity	Computer Forensics	Find hidden evidence stored
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	252	Knowledge of and experience in Insider	Computer Network Defense	Learn about investigative
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	290	Knowledge of processes for seizing	Forensics	Learn necessary forensic
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	329	Knowledge of surveillance detection	Surveillance	Learn the NSTISS basics
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	340	Knowledge of types and collection of	Computer Forensics	Learn necessary forensic
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	346	Knowledge of which system files (e.g. log	Computer Forensics	Find hidden evidence stored
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	369	Skill in collecting, processing,	Forensics	Gain awareness knowledge of
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	379	Skill in using common digital forensics tools	Computer Forensics	Find hidden evidence stored
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	381	Skill in using forensic tool suites (e.g.	Computer Forensics	Learn about various tools
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	888	Knowledge of types of digital forensics data	Computer Forensics	Find hidden evidence stored

Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	908	Ability to decrypt digital data collections	Computer Forensics	Find hidden evidence stored
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	1044	Skill in identifying forensic footprints	Computer Forensics	Find hidden evidence stored
Bossier Parish Community	A.S	Cyber Technology	CIT 280	200	1093	Knowledge of common forensic tool	Computer Forensics	Learn about various tools
Florida State College at	A.S	Computer Forensics	CAP 2023	200	9	Knowledge of applicable business	Requirements Analysis	02.02 Define requirements.
Florida State College at	A.S	Computer Forensics	CAP 2023	200	16	Knowledge of capabilities and	Requirements Analysis	02.03 Analyze user
Florida State College at	A.S	Computer Forensics	CAP 2023	200	60	Knowledge of incident categories, incident	Incident Management	02.07 Develop a timeline.
Florida State College at	A.S	Computer Forensics	CAP 2023	200	107	Knowledge of resource	Project Management	09.01 Review project plans
Florida State College at	A.S	Computer Forensics	CAP 2023	200	168	Skill in conducting software debugging	Software Development	5.08 Revise program code
Florida State College at	A.S	Computer Forensics	CAP 2023	200	174	Skill in creating programs that	Software Testing and Evaluation	5.03
Florida State College at	A.S	Computer Forensics	CAP 2023	200	238	Skill in writing code that is compatible	Computer Languages	4.03
Florida State College at	A.S	Computer Forensics	CAP 2023	200	261	Knowledge of basic concepts,	Telecommunicatio ns	3.01
Florida State College at	A.S	Computer Forensics	CAP 2023	200	264	Knowledge of basic physical computer	Computers and Electronics	3.02
Florida State College at	A.S	Computer Forensics	CAP 2023	200	364	Skill in identifying, modifying, and	Operating Systems	1.02
Florida State College at	A.S	Computer Forensics	CAP 2023	200	918	Ability to prepare and deliver education and	Teaching Others	2.01
Florida State College at	A.S	Computer Forensics	CAP 2023	200	974	Ability to tailor code analysis for	Software Testing and Evaluation	4.02
Florida State College at	A.S	Computer Forensics	CAP 2023	200	1008	Knowledge of how to troubleshoot basic	Operating Systems	7.04
Florida State College at	A.S	Computer Forensics	CAP 2023	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	12.14
Florida State College at	A.S	Computer Forensics	CAP 2140	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	01.09 Identify and discuss issues
Florida State College at	A.S	Computer Forensics	CAP 2140	200	4	Ability to identify systemic security	Vulnerabilities Assessment	01.09 Identify and discuss issues
Florida State College at	A.S	Computer Forensics	CAP 2140	200	112	Knowledge of server administration and	Systems Life Cycle	08.15 Address security issues
Florida State College at	A.S	Computer Forensics	CAP 2140	200	126	Knowledge of system software and	Requirements Analysis	08.02 Establish, document and
Florida State College at	A.S	Computer Forensics	CAP 2140	200	145	Knowledge of the type and frequency of	Systems Life Cycle	04.05 Use system software to
Florida State College at	A.S	Computer Forensics	CAP 2140	200	167	Skill in conducting server planning,	Network Management	08.15 Address security issues
Florida State College at	A.S	Computer Forensics	CAP 2140	200	206	Skill in installing computer and server	Systems Life Cycle	12.03 Evaluating skills and taking
Florida State College at	A.S	Computer Forensics	CAP 2140	200	264	Knowledge of basic physical computer	Computers and Electronics	04.01 Describe the functions and
Florida State College at	A.S	Computer Forensics	CAP 2140	200	892	Skill in configuring and utilizing	Configuration Management	08.12 Install and update antivirus
Florida State College at	A.S	Computer Forensics	CAP 2140	200	952	Knowledge of emerging security	Technology Awareness	01.09 Identify and discuss issues
Florida State College at	A.S	Computer Forensics	CAP 2140	200	984	Knowledge of computer network	Computer Network Defense	08.11 Document security policies
Florida State College at	A.S	Computer Forensics	CAP 2140	200	986	Knowledge of organizational	Identity Management	08.11 Document security policies
Florida State College at	A.S	Computer Forensics	CAP 2140	200	1037	Knowledge of information	Risk Management	08.11 Document security policies

Florida State College at	A.S	Computer Forensics	CAP 2140	200	1073	Knowledge of network systems	Network Management	08.08 Perform network
Florida State College at	A.S	Computer Forensics	CAP 2141	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	01.09 Identify and discuss issues
Florida State College at	A.S	Computer Forensics	CAP 2141	200	4	Ability to identify systemic security	Vulnerabilities Assessment	01.09 Identify and discuss issues
Florida State College at	A.S	Computer Forensics	CAP 2141	200	112	Knowledge of server administration and	Systems Life Cycle	08.15 Address security issues
Florida State College at	A.S	Computer Forensics	CAP 2141	200	126	Knowledge of system software and	Requirements Analysis	08.02 Establish, document and
Florida State College at	A.S	Computer Forensics	CAP 2141	200	145	Knowledge of the type and frequency of	Systems Life Cycle	04.05 Use system software to
Florida State College at	A.S	Computer Forensics	CAP 2141	200	167	Skill in conducting server planning,	Network Management	08.15 Address security issues
Florida State College at	A.S	Computer Forensics	CAP 2141	200	206	Skill in installing computer and server	Systems Life Cycle	12.03 Evaluating skills and taking
Florida State College at	A.S	Computer Forensics	CAP 2141	200	264	Knowledge of basic physical computer	Computers and Electronics	04.01 Describe the functions and
Florida State College at	A.S	Computer Forensics	CAP 2141	200	892	Skill in configuring and utilizing	Configuration Management	08.12 Install and update antivirus
Florida State College at	A.S	Computer Forensics	CAP 2141	200	952	Knowledge of emerging security	Technology Awareness	01.09 Identify and discuss issues
Florida State College at	A.S	Computer Forensics	CAP 2141	200	984	Knowledge of computer network	Computer Network Defense	08.11 Document security policies
Florida State College at	A.S	Computer Forensics	CAP 2141	200	986	Knowledge of organizational	Identity Management	08.11 Document security policies
Florida State College at	A.S	Computer Forensics	CAP 2141	200	1037	Knowledge of information	Risk Management	08.11 Document security policies
Florida State College at	A.S	Computer Forensics	CAP 2141	200	1073	Knowledge of network systems	Network Management	08.08 Perform network
Florida State College at	A.S	Biomedical Engineering	CET 1114	100	75	Knowledge of mathematics,	Mathematical Reasoning	13.01 Add, subtract, multiply
Florida State College at	A.S	Biomedical Engineering	CET 1114	100	264	Knowledge of basic physical computer	Computers and Electronics	07.08 Understand computer
Florida State College at	A.S	Biomedical Engineering	CET 1114	100	349	Skill in analyzing data from a variety of	Reasoning	07.01 Understand basic electrical
Florida State College at	A.S	Biomedical Engineering	CET 1114	100	360	Skill in identifying and extracting data of	Computer Forensics	07.07 Understand data acquisition
Florida State College at	A.S	Biomedical Engineering	CET 1114	100	1038	Knowledge of local specialized system	Infrastructure Design	07.15 Demonstrate
Florida State College at	N/A	N/A	CET1173	100	16	Knowledge of capabilities and	Requirements Analysis	06.01 Understand basic network
Florida State College at	N/A	N/A	CET1173	100	22	Knowledge of computer networking	Infrastructure Design	06.01 Understand basic network
Florida State College at	N/A	N/A	CET1173	100	32	Knowledge of database	Database Management	03.07 Demonstrate
Florida State College at	N/A	N/A	CET1173	100	34	Knowledge of database systems	Database Management	03.02 Understand database
Florida State College at	N/A	N/A	CET1173	100	81	Knowledge of network	Infrastructure Design	06.04 Demonstrate
Florida State College at	N/A	N/A	CET1173	100	90	Knowledge of operating systems	Operating Systems	02.01 Load and run operating
Florida State College at	N/A	N/A	CET1173	100	92	Knowledge of how traffic flows across	Infrastructure Design	06.04 Demonstrate
Florida State College at	N/A	N/A	CET1173	100	128	Knowledge of systems diagnostic tools and	Systems Testing and Evaluation	02.02 Load and run diagnostic
Florida State College at	N/A	N/A	CET1173	100	139	Knowledge of common networking	Infrastructure Design	06.04 Demonstrate
Florida State College at	N/A	N/A	CET1173	100	201	Skill in generating queries and reports	Database Management	03.07 Demonstrate

Florida State College at	N/A	N/A	CET1173	100	278	Knowledge of different types of	Telecommunications	06.03 Demonstrate
Florida State College at	N/A	N/A	CET1173	100	287	Knowledge of file system	Operating Systems	09.03 Describe various disk
Florida State College at	N/A	N/A	CET1173	100	347	Knowledge of Windows command	Operating Systems	09.08 Program using the
Florida State College at	N/A	N/A	CET1173	100	902	Knowledge of the range of existing	Network Management	06.03 Demonstrate
Florida State College at	N/A	N/A	CET1513	100	90	Knowledge of operating systems	Operating Systems	02.01 Load and run operating
Florida State College at	N/A	N/A	CET1513	100	128	Knowledge of systems diagnostic tools and	Systems Testing and Evaluation	02.02 Load and run diagnostic
Florida State College at	N/A	N/A	CET1513	100	287	Knowledge of file system	Operating Systems	09.03 Describe various disk
Florida State College at	N/A	N/A	CET1513	100	347	Knowledge of Windows command	Operating Systems	09.08 Program using the
Florida State College at	A.S	Engineering Technology	CET 1630	100	9	Knowledge of applicable business	Requirements Analysis	05.02 Calculate and determine
Florida State College at	A.S	Engineering Technology	CET 1630	100	16	Knowledge of capabilities and	Requirements Analysis	05.02 Calculate and determine
Florida State College at	A.S	Engineering Technology	CET 1630	100	1038	Knowledge of local specialized system	Infrastructure Design	05.02 Calculate and determine
Florida State College at	N/A	N/A	CET 1936	100	9	Knowledge of applicable business	Requirements Analysis	05.02 Calculate and determine
Florida State College at	N/A	N/A	CET 1936	100	16	Knowledge of capabilities and	Requirements Analysis	05.02 Calculate and determine
Florida State College at	N/A	N/A	CET 1936	100	1038	Knowledge of local specialized system	Infrastructure Design	05.02 Calculate and determine
Florida State College at	N/A	N/A	CET2172	200	18	Knowledge of circuit analysis	Computers and Electronics	07.13 Demonstrate
Florida State College at	N/A	N/A	CET2172	200	42	Knowledge of electrical engineering	Hardware Engineering	07.01 Understand basic electrical
Florida State College at	N/A	N/A	CET2172	200	43	Knowledge of embedded systems	Embedded Computers	07.07 Understand microprocessors
Florida State College at	N/A	N/A	CET2172	200	52	Knowledge of humancomputer	Human Factors	11.08 Pointing devices for
Florida State College at	N/A	N/A	CET2172	200	78	Knowledge of microprocessors	Computers and Electronics	07.07 Understand microprocessors
Florida State College at	N/A	N/A	CET2172	200	121	Knowledge of structured analysis	Logical Systems Design	01.01 Draw and explain systems
Florida State College at	N/A	N/A	CET2172	200	137	Knowledge of the characteristics of	Data Management	11.02 Analyze various types of
Florida State College at	N/A	N/A	CET2172	200	143	Knowledge of the organization’s	Enterprise Architecture	12.02 Read and understand
Florida State College at	N/A	N/A	CET2172	200	235	Skill in using the appropriate tools for	Computers and Electronics	02.09 Analyze firmware
Florida State College at	N/A	N/A	CET2172	200	264	Knowledge of basic physical computer	Computers and Electronics	07.10 Understand computer
Florida State College at	N/A	N/A	CET2172	200	340	Knowledge of types and collection of	Computer Forensics	07.09 Understand data acquisition
Florida State College at	N/A	N/A	CET2172	200	942	Knowledge of the organization's core	Organizational Awareness	12.02 Read and understand
Florida State College at	N/A	N/A	CET2172	200	986	Knowledge of organizational	Identity Management	12.02 Read and understand
Florida State College at	N/A	N/A	CET2179	200	43	Knowledge of embedded systems	Embedded Computers	03.02 Identify, define and
Florida State College at	N/A	N/A	CET2179	200	76	Knowledge of measures or	Information Technology	03.04 Identify and define
Florida State College at	N/A	N/A	CET2179	200	81	Knowledge of network	Infrastructure Design	03.05 Identify and define

Florida State College at	N/A	N/A	CET2179	200	92	Knowledge of how traffic flows across	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2179	200	96	Knowledge of performance tuning	Information Technology	03.04 Identify and define
Florida State College at	N/A	N/A	CET2179	200	137	Knowledge of the characteristics of	Data Management	04.06 Define environmental
Florida State College at	N/A	N/A	CET2179	200	139	Knowledge of common networking	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2179	200	154	Skill in analyzing network traffic	Capacity Management	03.04 Identify and define
Florida State College at	N/A	N/A	CET2179	200	264	Knowledge of basic physical computer	Computers and Electronics	03.01 Identify and define serial
Florida State College at	N/A	N/A	CET2179	200	287	Knowledge of file system	Operating Systems	09.03 Describe various disk
Florida State College at	N/A	N/A	CET2179	200	322	Knowledge of router and routing	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2179	200	364	Skill in identifying, modifying, and	Operating Systems	03.07 Identify and define
Florida State College at	N/A	N/A	CET2179	200	901	Knowledge of the capabilities of	Network Management	03.05 Identify and define
Florida State College at	N/A	N/A	CET2179	200	1002	Skill in conducting audits or reviews of	Information Technology	03.04 Identify and define
Florida State College at	N/A	N/A	CET2179	200	1038	Knowledge of local specialized system	Infrastructure Design	03.04 Identify and define
Florida State College at	N/A	N/A	CET2179	200	1073	Knowledge of network systems	Network Management	03.04 Identify and define
Florida State College at	A.S	Networking Services	CET2588	200	15	Knowledge of capabilities and	Hardware	01.21 Design a LAN, including
Florida State College at	A.S	Networking Services	CET2588	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	08.13 Describe current
Florida State College at	A.S	Networking Services	CET2588	200	29	Knowledge of data backup, types of	Computer Forensics	04.05 Use system software to
Florida State College at	A.S	Networking Services	CET2588	200	63	Knowledge of Information	Information Assurance	07.18 Explain three major
Florida State College at	A.S	Networking Services	CET2588	200	70	Knowledge of information	Information Systems/Network	08.14 Describe the functions and
Florida State College at	A.S	Networking Services	CET2588	200	72	Knowledge of local area network (LAN)	Infrastructure Design	08.35 Describe typical WAN links
Florida State College at	A.S	Networking Services	CET2588	200	77	Knowledege of current industry	Information Systems/Network	08.08 Perform network
Florida State College at	A.S	Networking Services	CET2588	200	79	Knowledge of network access,	Identity Management	08.13 Describe current
Florida State College at	A.S	Networking Services	CET2588	200	82	Knowledge of network design	Infrastructure Design	01.07 Identify several
Florida State College at	A.S	Networking Services	CET2588	200	83	Knowledge of network hardware	Hardware	01.21 Design a LAN, including
Florida State College at	A.S	Networking Services	CET2588	200	88	Knowledge of new and emerging	Technology Awareness	01.18 Identify major emerging
Florida State College at	A.S	Networking Services	CET2588	200	92	Knowledge of how traffic flows across	Infrastructure Design	01.11 List and define layers in
Florida State College at	A.S	Networking Services	CET2588	200	113	Knowledge of server and client operating	Operating Systems	06.02 Compare and contrast
Florida State College at	A.S	Networking Services	CET2588	200	128	Knowledge of systems diagnostic tools and	Systems Testing and Evaluation	09.01 Describe the use and
Florida State College at	A.S	Networking Services	CET2588	200	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	03.13 Design and implement test
Florida State College at	A.S	Networking Services	CET2588	200	133	Knowledge of telecommunications	Telecommunications	02.01 Differentiate
Florida State College at	A.S	Networking Services	CET2588	200	142	Knowledge of the operations and	Systems Life Cycle	09.02 Describe effective

Florida State College at	A.S	Networking Services	CET2588	200	145	Knowledge of the type and frequency of	Systems Life Cycle	04.05 Use system software to
Florida State College at	A.S	Networking Services	CET2588	200	156	Skill in applying confidentiality,	Information Assurance	08.08 Perform network
Florida State College at	A.S	Networking Services	CET2588	200	194	Skill in diagnosing connectivity problems	Network Management	09.05 Trace for connectivity
Florida State College at	A.S	Networking Services	CET2588	200	212	Skill in network mapping and	Infrastructure Design	01.13 Illustrate typical network
Florida State College at	A.S	Networking Services	CET2588	200	221	Skill in testing and configuring network	Network Management	05.15 Describe the requirements
Florida State College at	A.S	Networking Services	CET2588	200	261	Knowledge of basic concepts,	Telecommunications	02.03 Compare and contrast
Florida State College at	A.S	Networking Services	CET2588	200	278	Knowledge of different types of	Telecommunications	05.10 Identify advantages and
Florida State College at	A.S	Networking Services	CET2588	200	281	Knowledge of electronic devices	Hardware	02.05 Describe the functioning of
Florida State College at	A.S	Networking Services	CET2588	200	341	Knowledge of UNIX and Windows systems	Operating Systems	08.16 Discuss the functions of
Florida State College at	A.S	Networking Services	CET2588	200	346	Knowledge of which system files (e.g. log	Computer Forensics	04.08 Create, use, and maintain
Florida State College at	A.S	Networking Services	CET2588	200	364	Skill in identifying, modifying, and	Operating Systems	01.10 Identify and discuss issues
Florida State College at	A.S	Networking Services	CET2588	200	952	Knowledge of emerging security	Technology Awareness	01.18 Identify major emerging
Florida State College at	A.S	Networking Services	CET2588	200	985	Skill in configuring and utilizing network	Configuration Management	08.16 Discuss the functions of
Florida State College at	A.S	Networking Services	CET2588	200	1008	Knowledge of how to troubleshoot basic	Operating Systems	09.02 Describe effective
Florida State College at	A.S	Networking Services	CET2588	200	1037	Knowledge of information	Risk Management	08.09 Establish procedures for
Florida State College at	A.S	Networking Services	CET2588	200	1063	Knowledge of Unix/Linux operating	Operating Systems	04.06 Use operating
Florida State College at	A.S	Networking Services	CET2588	200	1115	Skill in reading Hexadecimal data	Computer Languages	01.03 Convert numbers among
Florida State College at	A.S	Networking Services	CET2588	200	1116	Skill in identifying common encoding	Computer Languages	01.05 Identify various coding
Florida State College at	Certifica	Information Technology	CET2600	200	15	Knowledge of capabilities and	Hardware	01.21 Design a LAN, including
Florida State College at	Certifica	Information Technology	CET2600	200	16	Knowledge of capabilities and	Requirements Analysis	06.01 Understand basic network
Florida State College at	Certifica	Information Technology	CET2600	200	22	Knowledge of computer networking	Infrastructure Design	06.01 Understand basic network
Florida State College at	Certifica	Information Technology	CET2600	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	08.13 Describe current
Florida State College at	Certifica	Information Technology	CET2600	200	29	Knowledge of data backup, types of	Computer Forensics	04.05 Use system software to
Florida State College at	Certifica	Information Technology	CET2600	200	35	Knowledge of digital rights management	Encryption	14.10 Identify and discuss
Florida State College at	Certifica	Information Technology	CET2600	200	41	Knowledge of organization's Local	Infrastructure Design	01.21 Design a LAN, including
Florida State College at	Certifica	Information Technology	CET2600	200	63	Knowledge of Information	Information Assurance	07.18 Explain three major
Florida State College at	Certifica	Information Technology	CET2600	200	70	Knowledge of information	Information Systems/Network	07.16 Explain the function and
Florida State College at	Certifica	Information Technology	CET2600	200	72	Knowledge of local area network (LAN)	Infrastructure Design	07.02 Differentiate
Florida State College at	Certifica	Information Technology	CET2600	200	75	Knowledge of mathematics,	Mathematical Reasoning	13.01 Add, subtract, multiply
Florida State College at	Certifica	Information Technology	CET2600	200	77	Knowledege of current industry	Information Systems/Network	08.08 Perform network

Florida State College at	Certifica	Information Technology	CET2600	200	79	Knowledge of network access,	Identity Management	08.13 Describe current
Florida State College at	Certifica	Information Technology	CET2600	200	81	Knowledge of network	Infrastructure Design	03.05 Identify and define
Florida State College at	Certifica	Information Technology	CET2600	200	82	Knowledge of network design	Infrastructure Design	01.07 Identify several
Florida State College at	Certifica	Information Technology	CET2600	200	83	Knowledge of network hardware	Hardware	01.21 Design a LAN, including
Florida State College at	Certifica	Information Technology	CET2600	200	88	Knowledge of new and emerging	Technology Awareness	01.18 Identify major emerging
Florida State College at	Certifica	Information Technology	CET2600	200	90	Knowledge of operating systems	Operating Systems	04.02 Identify current operating
Florida State College at	Certifica	Information Technology	CET2600	200	92	Knowledge of how traffic flows across	Infrastructure Design	01.11 List and define layers in
Florida State College at	Certifica	Information Technology	CET2600	200	113	Knowledge of server and client operating	Operating Systems	06.02 Compare and contrast
Florida State College at	Certifica	Information Technology	CET2600	200	122	Knowledge of system administration	Operating Systems	04.01 Describe the functions and
Florida State College at	Certifica	Information Technology	CET2600	200	126	Knowledge of system software and	Requirements Analysis	08.03 Create and test account
Florida State College at	Certifica	Information Technology	CET2600	200	128	Knowledge of systems diagnostic tools and	Systems Testing and Evaluation	09.01 Describe the use and
Florida State College at	Certifica	Information Technology	CET2600	200	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	03.13 Design and implement test
Florida State College at	Certifica	Information Technology	CET2600	200	133	Knowledge of telecommunications	Telecommunicatio ns	02.01 Differentiate
Florida State College at	Certifica	Information Technology	CET2600	200	139	Knowledge of common networking	Infrastructure Design	06.04 Demonstrate
Florida State College at	Certifica	Information Technology	CET2600	200	142	Knowledge of the operations and	Systems Life Cycle	09.02 Describe effective
Florida State College at	Certifica	Information Technology	CET2600	200	145	Knowledge of the type and frequency of	Systems Life Cycle	04.05 Use system software to
Florida State College at	Certifica	Information Technology	CET2600	200	156	Skill in applying confidentiality,	Information Assurance	08.08 Perform network
Florida State College at	Certifica	Information Technology	CET2600	200	167	Skill in conducting server planning,	Network Management	09.12 Define windows of
Florida State College at	Certifica	Information Technology	CET2600	200	194	Skill in diagnosing connectivity problems	Network Management	09.05 Trace for connectivity
Florida State College at	Certifica	Information Technology	CET2600	200	204	Skill in identifying possible causes of	Systems Life Cycle	09.13 Determine type of
Florida State College at	Certifica	Information Technology	CET2600	200	205	Skill in implementing, maintaining, and	Information Systems/Network	09.14 Determine service intervals
Florida State College at	Certifica	Information Technology	CET2600	200	212	Skill in network mapping and	Infrastructure Design	01.13 Illustrate typical network
Florida State College at	Certifica	Information Technology	CET2600	200	221	Skill in testing and configuring network	Network Management	05.15 Describe the requirements
Florida State College at	Certifica	Information Technology	CET2600	200	231	Skill in using network management tools to	Network Management	08.29 Use network
Florida State College at	Certifica	Information Technology	CET2600	200	261	Knowledge of basic concepts,	Telecommunicatio ns	02.03 Compare and contrast
Florida State College at	Certifica	Information Technology	CET2600	200	264	Knowledge of basic physical computer	Computers and Electronics	05.01 Describe the major
Florida State College at	Certifica	Information Technology	CET2600	200	278	Knowledge of different types of	Telecommunicatio ns	05.10 Identify advantages and
Florida State College at	Certifica	Information Technology	CET2600	200	281	Knowledge of electronic devices	Hardware	02.05 Describe the functioning of
Florida State College at	Certifica	Information Technology	CET2600	200	322	Knowledge of router and routing	Infrastructure Design	07.03 Compare and contrast
Florida State College at	Certifica	Information Technology	CET2600	200	332	Ability to develop curriculum that	Teaching Others	11.06 Develop an ongoing training

Florida State College at	Certifica	Information Technology	CET2600	200	341	Knowledge of UNIX and Windows systems	Operating Systems	08.16 Discuss the functions of
Florida State College at	Certifica	Information Technology	CET2600	200	346	Knowledge of which system files (e.g. log	Computer Forensics	04.08 Create, use, and maintain
Florida State College at	Certifica	Information Technology	CET2600	200	347	Knowledge of Windows command	Operating Systems	06.02 Understand basic network
Florida State College at	Certifica	Information Technology	CET2600	200	349	Skill in analyzing data from a variety of	Reasoning	07.01 Understand basic electrical
Florida State College at	Certifica	Information Technology	CET2600	200	358	Skill in determining tactics, techniques,	Strategic Thinking	09.07 Follow standard
Florida State College at	Certifica	Information Technology	CET2600	200	360	Skill in identifying and extracting data of	Computer Forensics	07.07 Understand data acquisition
Florida State College at	Certifica	Information Technology	CET2600	200	364	Skill in identifying, modifying, and	Operating Systems	01.10 Identify and discuss issues
Florida State College at	Certifica	Information Technology	CET2600	200	902	Knowledge of the range of existing	Network Management	06.03 Demonstrate
Florida State College at	Certifica	Information Technology	CET2600	200	915	Knowledge of frontend collection	Information Systems/Network	07.17 Configure access lists to
Florida State College at	Certifica	Information Technology	CET2600	200	952	Knowledge of emerging security	Technology Awareness	01.18 Identify major emerging
Florida State College at	Certifica	Information Technology	CET2600	200	985	Skill in configuring and utilizing network	Configuration Management	08.16 Discuss the functions of
Florida State College at	Certifica	Information Technology	CET2600	200	986	Knowledge of organizational	Identity Management	08.05 Grant/deny access to
Florida State College at	Certifica	Information Technology	CET2600	200	1008	Knowledge of how to troubleshoot basic	Operating Systems	09.02 Describe effective
Florida State College at	Certifica	Information Technology	CET2600	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	14.12 Identify and discuss
Florida State College at	Certifica	Information Technology	CET2600	200	1037	Knowledge of information	Risk Management	08.09 Establish procedures for
Florida State College at	Certifica	Information Technology	CET2600	200	1038	Knowledge of local specialized system	Infrastructure Design	07.15 Demonstrate
Florida State College at	Certifica	Information Technology	CET2600	200	1063	Knowledge of Unix/Linux operating	Operating Systems	04.06 Use operating
Florida State College at	Certifica	Information Technology	CET2600	200	1073	Knowledge of network systems	Network Management	08.30 Explain RMON and SNMP
Florida State College at	Certifica	Information Technology	CET2600	200	1114	Knowledge of encryption	Cryptography	14.13 Identify and discuss
Florida State College at	Certifica	Information Technology	CET2600	200	1115	Skill in reading Hexadecimal data	Computer Languages	01.03 Convert numbers among
Florida State College at	Certifica	Information Technology	CET2600	200	1116	Skill in identifying common encoding	Computer Languages	01.05 Identify various coding
Florida State College at	A.S	Networking Services	CET2629	200	15	Knowledge of capabilities and	Hardware	01.21 Design a LAN, including
Florida State College at	A.S	Networking Services	CET2629	200	63	Knowledge of Information	Information Assurance	07.18 Explain three major
Florida State College at	A.S	Networking Services	CET2629	200	82	Knowledge of network design	Infrastructure Design	01.09 Identify and discuss issues
Florida State College at	A.S	Networking Services	CET2629	200	83	Knowledge of network hardware	Hardware	01.21 Design a LAN, including
Florida State College at	A.S	Networking Services	CET2629	200	88	Knowledge of new and emerging	Technology Awareness	01.18 Identify major emerging
Florida State College at	A.S	Networking Services	CET2629	200	92	Knowledge of how traffic flows across	Infrastructure Design	07.06 Explain how the first
Florida State College at	A.S	Networking Services	CET2629	200	142	Knowledge of the operations and	Systems Life Cycle	09.02 Describe effective
Florida State College at	A.S	Networking Services	CET2629	200	156	Skill in applying confidentiality,	Information Assurance	08.08 Perform network
Florida State College at	A.S	Networking Services	CET2629	200	167	Skill in conducting server planning,	Network Management	12.03 Evaluating skills and taking

Florida State College at	A.S	Networking Services	CET2629	200	194	Skill in diagnosing connectivity problems	Network Management	09.05 Trace for connectivity
Florida State College at	A.S	Networking Services	CET2629	200	212	Skill in network mapping and	Infrastructure Design	01.13 Illustrate typical network
Florida State College at	A.S	Networking Services	CET2629	200	221	Skill in testing and configuring network	Network Management	05.15 Describe the requirements
Florida State College at	A.S	Networking Services	CET2629	200	231	Skill in using network management tools to	Network Management	08.29 Use network
Florida State College at	A.S	Networking Services	CET2629	200	261	Knowledge of basic concepts,	Telecommunications	05.09 Describe current wireless
Florida State College at	A.S	Networking Services	CET2629	200	264	Knowledge of basic physical computer	Computers and Electronics	07.08 Understand computer
Florida State College at	A.S	Networking Services	CET2629	200	278	Knowledge of different types of	Telecommunications	05.10 Identify advantages and
Florida State College at	A.S	Networking Services	CET2629	200	346	Knowledge of which system files (e.g. log	Computer Forensics	09.03 Recognize and resolve basic
Florida State College at	A.S	Networking Services	CET2629	200	358	Skill in determining tactics, techniques,	Strategic Thinking	09.07 Follow standard
Florida State College at	A.S	Networking Services	CET2629	200	364	Skill in identifying, modifying, and	Operating Systems	01.10 Identify and discuss issues
Florida State College at	A.S	Networking Services	CET2629	200	915	Knowledge of frontend collection	Information Systems/Network	07.17 Configure access lists to
Florida State College at	A.S	Networking Services	CET2629	200	918	Ability to prepare and deliver education and	Teaching Others	14.03 Participate in group
Florida State College at	A.S	Networking Services	CET2629	200	952	Knowledge of emerging security	Technology Awareness	01.18 Identify major emerging
Florida State College at	A.S	Networking Services	CET2629	200	986	Knowledge of organizational	Identity Management	08.05 Grant/deny access to
Florida State College at	A.S	Networking Services	CET2629	200	1008	Knowledge of how to troubleshoot basic	Operating Systems	09.02 Describe effective
Florida State College at	A.S	Networking Services	CET2629	200	1038	Knowledge of local specialized system	Infrastructure Design	07.15 Demonstrate
Florida State College at	Certifica	Program Computer	CET2662	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	06.05 Employ cryptographic
Florida State College at	Certifica	Program Computer	CET2662	200	35	Knowledge of digital rights management	Encryption	18.09 Identify and discuss
Florida State College at	Certifica	Program Computer	CET2662	200	37	Knowledge of disaster recovery and	Incident Management	13.02 Diagnose an enterprise's
Florida State College at	Certifica	Program Computer	CET2662	200	59	Knowledge of Intrusion Detection	Computer Network Defense	05.12 Monitor the network
Florida State College at	Certifica	Program Computer	CET2662	200	60	Knowledge of incident categories, incident	Incident Management	17.06 Identify the major categories
Florida State College at	Certifica	Program Computer	CET2662	200	63	Knowledge of Information	Information Assurance	06.03 Utilize various forms of
Florida State College at	Certifica	Program Computer	CET2662	200	66	Knowledge of intrusion detection	Computer Network Defense	05.11 Demonstrate an
Florida State College at	Certifica	Program Computer	CET2662	200	92	Knowledge of how traffic flows across	Infrastructure Design	07.01 Utilize protocol layering
Florida State College at	Certifica	Program Computer	CET2662	200	137	Knowledge of the characteristics of	Data Management	15.09 Compare different forms of
Florida State College at	Certifica	Program Computer	CET2662	200	139	Knowledge of common networking	Infrastructure Design	07.07 Discuss the security
Florida State College at	Certifica	Program Computer	CET2662	200	175	Skill in developing and deploying signatures	Information Systems/Network	06.04 Discuss the creation and use
Florida State College at	Certifica	Program Computer	CET2662	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	13.03 Specify possible
Florida State College at	Certifica	Program Computer	CET2662	200	179	Skill in designing security controls	Information Assurance	10.06 Discuss the steps necessary
Florida State College at	Certifica	Program Computer	CET2662	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	05.11 Demonstrate an

Florida State College at	Certifica	Program Computer	CET2662	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	14.13 Perform penetration
Florida State College at	Certifica	Program Computer	CET2662	200	226	Skill in the use of social engineering	Human Factors	14.13 Perform penetration
Florida State College at	Certifica	Program Computer	CET2662	200	261	Knowledge of basic concepts,	Telecommunicatio ns	07.02 Evaluate the security
Florida State College at	Certifica	Program Computer	CET2662	200	284	Knowledge of encryption algorithms	Cryptography	06.08 Utilize application and
Florida State College at	Certifica	Program Computer	CET2662	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	05.13 Investigate audit trails for
Florida State College at	Certifica	Program Computer	CET2662	200	895	Skill in recognizing and categorizing	Information Assurance	05.10 Analyze methods of
Florida State College at	Certifica	Program Computer	CET2662	200	896	Skill in protecting a network against	Computer Network Defense	15.06 Analyze local environment
Florida State College at	Certifica	Program Computer	CET2662	200	915	Knowledge of frontend collection	Information Systems/Network	05.11 Demonstrate an
Florida State College at	Certifica	Program Computer	CET2662	200	917	Knowledge of social dynamics of computer	External Awareness	13.01 Identify the physical threats
Florida State College at	Certifica	Program Computer	CET2662	200	965	Knowledge of organization's risk	Risk Management	14.14 Understand principles of risk
Florida State College at	Certifica	Program Computer	CET2662	200	985	Skill in configuring and utilizing network	Configuration Management	13.05 Evaluate the applicability
Florida State College at	Certifica	Program Computer	CET2662	200	1021	Knowledge of threat assessment	Risk Management	13.01 Identify the physical threats
Florida State College at	Certifica	Program Computer	CET2662	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	17.01 Understand the major
Florida State College at	Certifica	Program Computer	CET2662	200	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	05.14 Perform penetration
Florida State College at	Certifica	Program Computer	CET2662	200	1072	Knowledge of network security	Information Systems/Network	07.03 Describe security concerns
Florida State College at	Certifica	Program Computer	CET2662	200	1114	Knowledge of encryption	Cryptography	06.01 Demonstrate an
Florida State College at	N/A	N/A	CET2687	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	06.05 Employ cryptographic
Florida State College at	N/A	N/A	CET2687	200	35	Knowledge of digital rights management	Encryption	18.09 Identify and discuss
Florida State College at	N/A	N/A	CET2687	200	37	Knowledge of disaster recovery and	Incident Management	13.02 Diagnose an enterprise’s
Florida State College at	N/A	N/A	CET2687	200	59	Knowledge of Intrusion Detection	Computer Network Defense	05.12 Monitor the network
Florida State College at	N/A	N/A	CET2687	200	60	Knowledge of incident categories, incident	Incident Management	17.06 Identify the major categories
Florida State College at	N/A	N/A	CET2687	200	63	Knowledge of Information	Information Assurance	06.03 Utilize various forms of
Florida State College at	N/A	N/A	CET2687	200	66	Knowledge of intrusion detection	Computer Network Defense	05.11 Demonstrate an
Florida State College at	N/A	N/A	CET2687	200	92	Knowledge of how traffic flows across	Infrastructure Design	07.01 Utilize protocol layering
Florida State College at	N/A	N/A	CET2687	200	137	Knowledge of the characteristics of	Data Management	15.09 Compare different forms of
Florida State College at	N/A	N/A	CET2687	200	139	Knowledge of common networking	Infrastructure Design	07.07 Discuss the security
Florida State College at	N/A	N/A	CET2687	200	175	Skill in developing and deploying signatures	Information Systems/Network	06.04 Discuss the creation and use
Florida State College at	N/A	N/A	CET2687	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	13.03 Specify possible
Florida State College at	N/A	N/A	CET2687	200	179	Skill in designing security controls	Information Assurance	10.06 Discuss the steps necessary
Florida State College at	N/A	N/A	CET2687	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	05.11 Demonstrate an

Florida State College at	N/A	N/A	CET2687	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	14.13 Perform penetration
Florida State College at	N/A	N/A	CET2687	200	226	Skill in the use of social engineering	Human Factors	14.13 Perform penetration
Florida State College at	N/A	N/A	CET2687	200	261	Knowledge of basic concepts,	Telecommunicatio ns	07.02 Evaluate the security
Florida State College at	N/A	N/A	CET2687	200	284	Knowledge of encryption algorithms	Cryptography	06.08 Utilize application and
Florida State College at	N/A	N/A	CET2687	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	05.13 Investigate audit trails for
Florida State College at	N/A	N/A	CET2687	200	895	Skill in recognizing and categorizing	Information Assurance	05.10 Analyze methods of
Florida State College at	N/A	N/A	CET2687	200	896	Skill in protecting a network against	Computer Network Defense	15.06 Analyze local environment
Florida State College at	N/A	N/A	CET2687	200	915	Knowledge of frontend collection	Information Systems/Network	05.11 Demonstrate an
Florida State College at	N/A	N/A	CET2687	200	917	Knowledge of social dynamics of computer	External Awareness	13.01 Identify the physical threats
Florida State College at	N/A	N/A	CET2687	200	965	Knowledge of organization's risk	Risk Management	14.14 Understand principles of risk
Florida State College at	N/A	N/A	CET2687	200	985	Skill in configuring and utilizing network	Configuration Management	13.05 Evaluate the applicability
Florida State College at	N/A	N/A	CET2687	200	1021	Knowledge of threat assessment	Risk Management	13.01 Identify the physical threats
Florida State College at	N/A	N/A	CET2687	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	17.01 Understand the major
Florida State College at	N/A	N/A	CET2687	200	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	05.14 Perform penetration
Florida State College at	N/A	N/A	CET2687	200	1072	Knowledge of network security	Information Systems/Network	07.03 Describe security concerns
Florida State College at	N/A	N/A	CET2687	200	1114	Knowledge of encryption	Cryptography	06.01 Demonstrate an
Florida State College at	N/A	N/A	CET2752	200	4	Ability to identify systemic security	Vulnerabilities Assessment	14.07 Determine what resources,
Florida State College at	N/A	N/A	CET2752	200	29	Knowledge of data backup, types of	Computer Forensics	14.03 Perform backups of critical
Florida State College at	N/A	N/A	CET2752	200	81	Knowledge of network	Infrastructure Design	02.04 Describe the functions and
Florida State College at	N/A	N/A	CET2752	200	83	Knowledge of network hardware	Hardware	02.05 Describe the major
Florida State College at	N/A	N/A	CET2752	200	87	Knowledge of network traffic	Information Systems/Network	14.11 Utilize monitoring tools
Florida State College at	N/A	N/A	CET2752	200	98	Knowledge of policybased and risk	Identity Management	14.06 Demonstrate an
Florida State College at	N/A	N/A	CET2752	200	137	Knowledge of the characteristics of	Data Management	02.08 Describe the function of
Florida State College at	N/A	N/A	CET2752	200	145	Knowledge of the type and frequency of	Systems Life Cycle	01.05 Perform preventive
Florida State College at	N/A	N/A	CET2752	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	13.03 Specify possible
Florida State College at	N/A	N/A	CET2752	200	179	Skill in designing security controls	Information Assurance	14.04 Protect the privacy of
Florida State College at	N/A	N/A	CET2752	200	191	Skill in developing and applying security	Identity Management	05.01 Specify by access control
Florida State College at	N/A	N/A	CET2752	200	221	Skill in testing and configuring network	Network Management	01.06 Set up and configure
Florida State College at	N/A	N/A	CET2752	200	231	Skill in using network management tools to	Network Management	14.11 Utilize monitoring tools
Florida State College at	N/A	N/A	CET2752	200	264	Knowledge of basic physical computer	Computers and Electronics	01.02 Identify the architecture of

Florida State College at	N/A	N/A	CET2752	200	341	Knowledge of UNIX and Windows systems	Operating Systems	03.09 Install and configure client
Florida State College at	N/A	N/A	CET2752	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	05.13 Investigate audit trails for
Florida State College at	N/A	N/A	CET2752	200	364	Skill in identifying, modifying, and	Operating Systems	05.03 Administer computer, group,
Florida State College at	N/A	N/A	CET2752	200	892	Skill in configuring and utilizing	Configuration Management	03.07 Install and configure a
Florida State College at	N/A	N/A	CET2752	200	917	Knowledge of social dynamics of computer	External Awareness	13.01 Identify the physical threats
Florida State College at	N/A	N/A	CET2752	200	952	Knowledge of emerging security	Technology Awareness	01.04 Discuss the potential impact
Florida State College at	N/A	N/A	CET2752	200	986	Knowledge of organizational	Identity Management	05.01 Specify by access control
Florida State College at	N/A	N/A	CET2752	200	1021	Knowledge of threat assessment	Risk Management	13.01 Identify the physical threats
Florida State College at	N/A	N/A	CET2752	200	1033	Knowledge of basic system	Information Systems/Network	05.02 Compare and contrast
Florida State College at	N/A	N/A	CET2752	200	1072	Knowledge of network security	Information Systems/Network	02.01 Discuss fundamental
Florida State College at	N/A	N/A	CET2759	200	15	Knowledge of capabilities and	Hardware	10.05 Identify and define
Florida State College at	N/A	N/A	CET2759	200	22	Knowledge of computer networking	Infrastructure Design	8.01 Identify and define computer
Florida State College at	N/A	N/A	CET2759	200	42	Knowledge of electrical engineering	Hardware Engineering	10.06 Apply digital
Florida State College at	N/A	N/A	CET2759	200	43	Knowledge of embedded systems	Embedded Computers	03.02 Identify, define and
Florida State College at	N/A	N/A	CET2759	200	50	Knowledge of how network services and	Infrastructure Design	10.09 Define communication
Florida State College at	N/A	N/A	CET2759	200	76	Knowledge of measures or	Information Technology	03.04 Identify and define
Florida State College at	N/A	N/A	CET2759	200	81	Knowledge of network	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2759	200	92	Knowledge of how traffic flows across	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2759	200	96	Knowledge of performance tuning	Information Technology	03.04 Identify and define
Florida State College at	N/A	N/A	CET2759	200	139	Knowledge of common networking	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2759	200	154	Skill in analyzing network traffic	Capacity Management	03.04 Identify and define
Florida State College at	N/A	N/A	CET2759	200	212	Skill in network mapping and	Infrastructure Design	8.01 Identify and define computer
Florida State College at	N/A	N/A	CET2759	200	264	Knowledge of basic physical computer	Computers and Electronics	03.01 Identify and define serial
Florida State College at	N/A	N/A	CET2759	200	322	Knowledge of router and routing	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2759	200	364	Skill in identifying, modifying, and	Operating Systems	03.07 Identify and define
Florida State College at	N/A	N/A	CET2759	200	901	Knowledge of the capabilities of	Network Management	03.05 Identify and define
Florida State College at	N/A	N/A	CET2759	200	1002	Skill in conducting audits or reviews of	Information Technology	03.04 Identify and define
Florida State College at	N/A	N/A	CET2759	200	1038	Knowledge of local specialized system	Infrastructure Design	03.04 Identify and define
Florida State College at	N/A	N/A	CET2759	200	1073	Knowledge of network systems	Network Management	03.04 Identify and define
Capitol College	B.S	Computer Engineering	IAE 201	200	8	Knowledge of access authentication	Identity Management	15. Describe and classify examples

Capitol College	B.S	Computer Engineering	IAE 201	200	27	Knowledge of cryptology	Cryptography	6. Describe and give examples of
Capitol College	B.S	Computer Engineering	IAE 201	200	59	Knowledge of Intrusion Detection	Computer Network Defense	19. Describe the purpose of the
Capitol College	B.S	Computer Engineering	IAE 201	200	63	Knowledge of Information	Information Assurance	3. Define, distinguish
Capitol College	B.S	Computer Engineering	IAE 201	200	70	Knowledge of information	Information Systems/Network	6. Describe and give examples of
Capitol College	B.S	Computer Engineering	IAE 201	200	98	Knowledge of policybased and risk	Identity Management	6. Describe and give examples of
Capitol College	B.S	Computer Engineering	IAE 201	200	148	Knowledge of VPN security.	Encryption	19. Describe the purpose of the
Capitol College	B.S	Computer Engineering	IAE 201	200	261	Knowledge of basic concepts,	Telecommunications	18. Describe the basic theory
Capitol College	B.S	Computer Engineering	IAE 201	200	277	Knowledge of defense indepth principles and	Computer Network Defense	10. Describe the concept of
Capitol College	B.S	Computer Engineering	IAE 201	200	300	Knowledge of intelligence reporting	Organizational Awareness	24. Write an effective and
Capitol College	B.S	Computer Engineering	IAE 201	200	348	Knowledge of wireless network collection	Cryptography	18. Describe the basic theory
Capitol College	B.S	Computer Engineering	IAE 201	200	895	Skill in recognizing and categorizing	Information Assurance	1. Define, distinguish
Capitol College	B.S	Computer Engineering	IAE 201	200	917	Knowledge of social dynamics of computer	External Awareness	5. Describe the different types of
Capitol College	B.S	Computer Engineering	IAE 201	200	942	Knowledge of the organization's core	Organizational Awareness	23. Discuss Organizational
Capitol College	B.S	Computer Engineering	IAE 201	200	1114	Knowledge of encryption	Cryptography	7. Describe the principles behind
Capitol College	B.S	Computer Engineering	IAE 201	200	277	Knowledge of defense indepth principles and	Computer Network Defense	10. Describe the concept of
Capitol College	B.S	Computer Engineering	IAE 201	200	300	Knowledge of intelligence reporting	Organizational Awareness	24. Write an effective and
Capitol College	B.S	Computer Engineering	IAE 201	200	348	Knowledge of wireless network collection	Cryptography	18. Describe the basic theory
Capitol College	B.S	Computer Engineering	IAE 201	200	895	Skill in recognizing and categorizing	Information Assurance	1. Define, distinguish
Capitol College	B.S	Computer Engineering	IAE 201	200	917	Knowledge of social dynamics of computer	External Awareness	5. Describe the different types of
Capitol College	B.S	Computer Engineering	IAE 201	200	942	Knowledge of the organization's core	Organizational Awareness	23. Discuss Organizational
Capitol College	B.S	Computer Engineering	IAE 201	200	1114	Knowledge of encryption	Cryptography	7. Describe the principles behind
Capitol College	B.S	Computer Engineering	IAE 201	200	1115	Skill in reading Hexadecimal data	Computer Languages	1. Define, distinguish
Capitol College	B.S	Computer Engineering	IAE 201	200	1116	Skill in identifying common encoding	Computer Languages	2. Identify and describe
Capitol College	B.S	Computer Engineering	IAE 201	200	1117	Skill in utilizing virtual networks for testing	Operating Systems	4. Define, distinguish
Capitol College	B.S	Computer Engineering	IAE 201	200	1118	Skill in reading and interpreting	Information Systems/Network	11. Explain the concept of
Capitol College	B.S	Computer Engineering	IAE 201	200	1119	Knowledge of signature	Information Systems/Network	12. Define and describe
Capitol College	B.S	Computer Engineering	IAE 201	200	1120	Ability to interpret and incorporate data	Data Management	13. Define and describe
Capitol College	B.S	Computer Engineering	IAE 201	200	1121	Knowledge of Windows/Unix ports	Operating Systems	21. Security documentation
Capitol College	B.S	Computer Engineering	IAE 301	300	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	1. Learn and understand basic
Capitol College	B.S	Computer Engineering	IAE 301	300	4	Ability to identify systemic security	Vulnerabilities Assessment	13. Learn and understand the

Capitol College	B.S	Computer Engineering	IAE 301	300	24	Knowledge of concepts and	Data Management	18. Learn and understand the
Capitol College	B.S	Computer Engineering	IAE 301	300	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	5. Learn and understand
Capitol College	B.S	Computer Engineering	IAE 301	300	27	Knowledge of cryptology	Cryptography	5. Learn and understand
Capitol College	B.S	Computer Engineering	IAE 301	300	37	Knowledge of disaster recovery and	Incident Management	14. Learn and understand the
Capitol College	B.S	Computer Engineering	IAE 301	300	38	Knowledge of organization's	Information Assurance	3. Learn and understand about
Capitol College	B.S	Computer Engineering	IAE 301	300	49	Knowledge of host/network access	Information Systems/Network	6. Learn and Understand
Capitol College	B.S	Computer Engineering	IAE 301	300	59	Knowledge of Intrusion Detection	Computer Network Defense	8. Learn and understand about
Capitol College	B.S	Computer Engineering	IAE 301	300	79	Knowledge of network access,	Identity Management	5. Learn and understand
Capitol College	B.S	Computer Engineering	IAE 301	300	82	Knowledge of network design	Infrastructure Design	6. Learn and Understand
Capitol College	B.S	Computer Engineering	IAE 301	300	83	Knowledge of network hardware	Hardware	6. Learn and Understand
Capitol College	B.S	Computer Engineering	IAE 301	300	95	Knowledge of penetration testing	Vulnerabilities Assessment	19. Through the use of weekly
Capitol College	B.S	Computer Engineering	IAE 301	300	100	Knowledge of Privacy Impact Assessments	Personnel Safety and Security	4. Learn and understand the
Capitol College	B.S	Computer Engineering	IAE 301	300	106	Knowledge of remote access technology	Information Technology	7. Learn and understand the
Capitol College	B.S	Computer Engineering	IAE 301	300	108	Knowledge of risk management	Risk Management	15. Identify the purpose of Risk
Capitol College	B.S	Computer Engineering	IAE 301	300	146	Knowledge of the types of Intrusion	Computer Network Defense	8. Learn and understand about
Capitol College	B.S	Computer Engineering	IAE 301	300	150	Knowledge of what constitutes a network	Information Systems/Network	11. Learn and identify the
Capitol College	B.S	Computer Engineering	IAE 301	300	157	Skill in applying host/network access	Identity Management	2. Determine various methods
Capitol College	B.S	Computer Engineering	IAE 301	300	191	Skill in developing and applying security	Identity Management	2. Determine various methods
Capitol College	B.S	Computer Engineering	IAE 301	300	212	Skill in network mapping and	Infrastructure Design	6. Learn and Understand
Capitol College	B.S	Computer Engineering	IAE 301	300	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	19. Through the use of weekly
Capitol College	B.S	Computer Engineering	IAE 301	300	278	Knowledge of different types of	Telecommunicatio ns	10. Learn and understand the
Capitol College	B.S	Computer Engineering	IAE 301	300	284	Knowledge of encryption algorithms	Cryptography	5. Learn and understand
Capitol College	B.S	Computer Engineering	IAE 301	300	895	Skill in recognizing and categorizing	Information Assurance	11. Learn and identify the
Capitol College	B.S	Computer Engineering	IAE 301	300	901	Knowledge of the capabilities of	Network Management	12. Learn and understand the
Capitol College	B.S	Computer Engineering	IAE 301	300	986	Knowledge of organizational	Identity Management	2. Determine various methods
Capitol College	B.S	Computer Engineering	IAE 301	300	991	Knowledge of different classes of	Computer Network Defense	11. Learn and identify the
Capitol College	B.S	Computer Engineering	IAE 301	300	1029	Knowledge of malware analysis	Computer Network Defense	11. Learn and identify the
Capitol College	B.S	Computer Engineering	IAE 301	300	1033	Knowledge of basic system	Information Systems/Network	9. Learn and understand the
Capitol College	B.S	Computer Engineering	IAE 301	300	1036	Knowledge of applicable laws (e.g.,	Criminal Law	4. Learn and understand the
Capitol College	B.S	Computer Engineering	IAE 301	300	1056	Knowledge of operations security	Public Safety and Security	3. Learn and understand about

Capitol College	B.S	Computer Engineering	IAE 301	300	1072	Knowledge of network security	Information Systems/Network	6. Learn and Understand
Capitol College	B.S	Computer Engineering	IAE 301	300	1093	Knowledge of common forensic tool	Computer Forensics	19. Through the use of weekly
Capitol College	B.S	Computer Engineering	IAE 301	300	1120	Ability to interpret and incorporate data	Data Management	16. Learn and understand the
Capitol College	B.S	Computer Engineering	IAE 301	300	1121	Knowledge of Windows/Unix ports	Operating Systems	17. Learn and understand the
Capitol College	B.S	Computer Engineering	IAE 315	300	15	Knowledge of capabilities and	Hardware	4. How to configure,
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	49	Knowledge of host/network access	Information Systems/Network	3. Access control methodologies,
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	55	Knowledge of Information	Information Assurance	5. Risk mitigation, acceptance, and
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	90	Knowledge of operating systems	Operating Systems	2. Built in security controls of
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	98	Knowledge of policybased and risk	Identity Management	3. Access control methodologies,
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	108	Knowledge of risk management	Risk Management	5. Risk mitigation, acceptance, and
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	113	Knowledge of server and client operating	Operating Systems	4. How to configure,
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	157	Skill in applying host/network access	Identity Management	3. Access control methodologies,
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	167	Skill in conducting server planning,	Network Management	4. How to configure,
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	177	Skill in designing countermeasures to	Vulnerabilities Assessment	5. Risk mitigation, acceptance, and
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	191	Skill in developing and applying security	Identity Management	3. Access control methodologies,
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	202	Skill in identifying and anticipating server	Information Technology	4. How to configure,
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	206	Skill in installing computer and server	Systems Life Cycle	4. How to configure,
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	356	Skill in determining installed patches on	Operating Systems	6. How to identify and remediate
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	891	Skill in configuring and utilizing	Configuration Management	4. How to configure,
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	986	Knowledge of organizational	Identity Management	3. Access control methodologies,
Capitol College	B.S	Telecommunications Engineering	IAE 315	300	1033	Knowledge of basic system	Information Systems/Network	2. Built in security controls of
Capitol College	B.S	Information Assurance	IAE 321	300	15	Knowledge of capabilities and	Hardware	Wireless hardware,
Capitol College	B.S	Information Assurance	IAE 321	300	42	Knowledge of electrical engineering	Hardware Engineering	Wireless hardware,
Capitol College	B.S	Information Assurance	IAE 321	300	44	Knowledge of enterprise messaging	Enterprise Architecture	Wireless software (WAP, HTML5,
Capitol College	B.S	Information Assurance	IAE 321	300	56	Knowledge of information assurance	Information Assurance	Wireless software (WAP, HTML5,
Capitol College	B.S	Information Assurance	IAE 321	300	75	Knowledge of mathematics,	Mathematical Reasoning	RF Mathematics (Link Budget,
Capitol College	B.S	Information Assurance	IAE 321	300	82	Knowledge of network design	Infrastructure Design	Wireless security tools of the trade,
Capitol College	B.S	Information Assurance	IAE 321	300	83	Knowledge of network hardware	Hardware	Wireless hardware,
Capitol College	B.S	Information Assurance	IAE 321	300	95	Knowledge of penetration testing	Vulnerabilities Assessment	Wireless penetration
Capitol College	B.S	Information Assurance	IAE 321	300	116	Knowledge of software debugging	Software Development	Wireless software (WAP, HTML5,

Capitol College	B.S	Information Assurance	IAE 321	300	117	Knowledge of software design tools,	Software Development	Wireless software (WAP, HTML5,
Capitol College	B.S	Information Assurance	IAE 321	300	118	Knowledge of software	Software Engineering	Wireless software (WAP, HTML5,
Capitol College	B.S	Information Assurance	IAE 321	300	119	Knowledge of software engineering	Software Engineering	Wireless software (WAP, HTML5,
Capitol College	B.S	Information Assurance	IAE 321	300	123	Knowledge of system and application	Vulnerabilities Assessment	1) Wireless threats: (cracking,
Capitol College	B.S	Information Assurance	IAE 321	300	126	Knowledge of system software and	Requirements Analysis	Wireless software (WAP, HTML5,
Capitol College	B.S	Information Assurance	IAE 321	300	129	Knowledge of systems lifecycle management	Systems Life Cycle	Wireless software (WAP, HTML5,
Capitol College	B.S	Information Assurance	IAE 321	300	146	Knowledge of the types of Intrusion	Computer Network Defense	Wireless hardware,
Capitol College	B.S	Information Assurance	IAE 321	300	150	Knowledge of what constitutes a network	Information Systems/Network	Wireless threats: (cracking,
Capitol College	B.S	Information Assurance	IAE 321	300	168	Skill in conducting software debugging	Software Development	Wireless software (WAP, HTML5,
Capitol College	B.S	Information Assurance	IAE 321	300	170	Skill in configuring and optimizing	Software Engineering	Wireless software (WAP, HTML5,
Capitol College	B.S	Information Assurance	IAE 321	300	174	Skill in creating programs that	Software Testing and Evaluation	Wireless software (WAP, HTML5,
Capitol College	B.S	Information Assurance	IAE 321	300	180	Skill in designing the integration of	Systems Integration	Wireless hardware,
Capitol College	B.S	Information Assurance	IAE 321	300	225	Skill in the use of penetration testing	Vulnerabilities Assessment	1) Wireless penetration
Capitol College	B.S	Information Assurance	IAE 321	300	235	Skill in using the appropriate tools for	Computers and Electronics	Wireless hardware,
Capitol College	B.S	Information Assurance	IAE 321	300	278	Knowledge of different types of	Telecommunications	Wireless security best practices:
Capitol College	B.S	Information Assurance	IAE 321	300	281	Knowledge of electronic devices	Hardware	Wireless hardware,
Capitol College	B.S	Information Assurance	IAE 321	300	302	Knowledge of investigative	Computer Forensics	Wireless hardware,
Capitol College	B.S	Information Assurance	IAE 321	300	326	Knowledge of security hardware and	Information Systems/Network	Wireless hardware,
Capitol College	B.S	Information Assurance	IAE 321	300	327	Knowledge of security implications of	Information Assurance	Wireless software (WAP, HTML5,
Capitol College	B.S	Information Assurance	IAE 321	300	348	Knowledge of wireless network collection	Cryptography	Wireless network design principles
Capitol College	B.S	Information Assurance	IAE 321	300	886	Skill in wireless network target	Vulnerabilities Assessment	Wireless network design principles
Capitol College	B.S	Information Assurance	IAE 321	300	891	Skill in configuring and utilizing	Configuration Management	Wireless hardware,
Capitol College	B.S	Information Assurance	IAE 321	300	892	Skill in configuring and utilizing	Configuration Management	Wireless software (WAP, HTML5,
Capitol College	B.S	Information Assurance	IAE 321	300	967	Knowledge of current and emerging	Information Systems/Network	Wireless threats: (cracking,
Capitol College	B.S	Information Assurance	IAE 321	300	968	Knowledge of softwarerelated	Information Systems/Network	Wireless software (WAP, HTML5,
Capitol College	B.S	Information Assurance	IAE 321	300	1054	Knowledge of hardware reverse	Vulnerabilities Assessment	Wireless hardware,
Capitol College	B.S	Information Assurance	IAE 325	300	9	Knowledge of applicable business	Requirements Analysis	Business requirements
Capitol College	B.S	Information Assurance	IAE 325	300	12	Knowledge of communication	Infrastructure Design	2.) Cryptographic standards, 5.)
Capitol College	B.S	Information Assurance	IAE 325	300	17	Knowledge of certified ethical	Vulnerabilities Assessment	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	23	Knowledge of computer	Object Technology	6.) Principles of certificates, key

Capitol College	B.S	Information Assurance	IAE 325	300	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	2.) Cryptographic standards, 7.)
Capitol College	B.S	Information Assurance	IAE 325	300	27	Knowledge of cryptology	Cryptography	2.) Cryptographic standards, 7.)
Capitol College	B.S	Information Assurance	IAE 325	300	31	Knowledge of data mining and data	Data Management	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	35	Knowledge of digital rights management	Encryption	1.)The history of encryption
Capitol College	B.S	Information Assurance	IAE 325	300	50	Knowledge of how network services and	Infrastructure Design	3.)Secure data communications
Capitol College	B.S	Information Assurance	IAE 325	300	55	Knowledge of Information	Information Assurance	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	56	Knowledge of information assurance	Information Assurance	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	62	Knowledge of industrystandard and	Logical Systems Design	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	63	Knowledge of Information	Information Assurance	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	64	Knowledge of information security	Information Systems/ Network	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	70	Knowledge of information	Information Systems/Network	1.) The history of encryption, 6.)
Capitol College	B.S	Information Assurance	IAE 325	300	72	Knowledge of local area network (LAN)	Infrastructure Design	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	81	Knowledge of network	Infrastructure Design	1. Secure communication
Capitol College	B.S	Information Assurance	IAE 325	300	95	Knowledge of penetration testing	Vulnerabilities Assessment	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	99	Knowledge of principles and	Systems Integration	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	107	Knowledge of resource	Project Management	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	116	Knowledge of software debugging	Software Development	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	121	Knowledge of structured analysis	Logical Systems Design	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	129	Knowledge of systems lifecycle management	Systems Life Cycle	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	133	Knowledge of telecommunications	Telecommunications	3.) Secure data communications
Capitol College	B.S	Information Assurance	IAE 325	300	139	Knowledge of common networking	Infrastructure Design	3.) Secure data communications
Capitol College	B.S	Information Assurance	IAE 325	300	148	Knowledge of VPN security.	Encryption	The history of encryption
Capitol College	B.S	Information Assurance	IAE 325	300	156	Skill in applying confidentiality,	Information Assurance	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	158	Skill in applying organizationspecific	Systems Testing and Evaluation	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	179	Skill in designing security controls	Information Assurance	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	237	Skill in using Virtual Private Network	Encryption	The history of encryption
Capitol College	B.S	Information Assurance	IAE 325	300	238	Skill in writing code that is compatible	Computer Languages	Business requirements
Capitol College	B.S	Information Assurance	IAE 325	300	261	Knowledge of basic concepts,	Telecommunications	3.) Secure data communications
Capitol College	B.S	Information Assurance	IAE 325	300	274	Knowledge of concepts, principles,	Computer Network Defense	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	277	Knowledge of defense indepth principles and	Computer Network Defense	6.) Principles of certificates, key

Capitol College	B.S	Information Assurance	IAE 325	300	278	Knowledge of different types of	Telecommunicatio ns	3.) Secure data communications
Capitol College	B.S	Information Assurance	IAE 325	300	284	Knowledge of encryption algorithms	Cryptography, 7.) Wired and wireless	1.) The history of encryption, 2.)
Capitol College	B.S	Information Assurance	IAE 325	300	299	Knowledge of information security	Project Management	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	300	Knowledge of intelligence reporting	Organizational Awareness	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	305	Knowledge of laws that affect cyber	Forensics	1. Secure communication
Capitol College	B.S	Information Assurance	IAE 325	300	336	Knowledge of the nature and function	Telecommunicatio ns	3.) Secure data communications
Capitol College	B.S	Information Assurance	IAE 325	300	348	Knowledge of wireless network collection	Cryptography	2.) Cryptographic standards, 7.)
Capitol College	B.S	Information Assurance	IAE 325	300	376	Skill in talking to others to convey	Oral Communication	5.) Secure communication
Capitol College	B.S	Information Assurance	IAE 325	300	387	Skill in verifying the integrity of encrypted	Encryption	1.) The history of encryption, 8.)
Capitol College	B.S	Information Assurance	IAE 325	300	893	Skill in securing network	Information Assurance	3.) Secure data communications
Capitol College	B.S	Information Assurance	IAE 325	300	901	Knowledge of the capabilities of	Network Management	5.) Secure communication
Capitol College	B.S	Information Assurance	IAE 325	300	942	Knowledge of the organization's core	Organizational Awareness	Business requirements
Capitol College	B.S	Information Assurance	IAE 325	300	968	Knowledge of softwarerelated	Information Systems/Network	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	989	Knowledge of Voice over Internet Protocol	Telecommunicatio ns	3.) Secure data communications
Capitol College	B.S	Information Assurance	IAE 325	300	1036	Knowledge of applicable laws (e.g.,	Criminal Law	3.) Secure data communications
Capitol College	B.S	Information Assurance	IAE 325	300	1052	Knowledge of Global Systems for Mobile	Telecommunicatio ns	3.) Secure data communications
Capitol College	B.S	Information Assurance	IAE 325	300	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	3.) Secure data communications
Capitol College	B.S	Information Assurance	IAE 325	300	1072	Knowledge of network security	Information Systems/Network	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	1073	Knowledge of network systems	Network Management	6.) Principles of certificates, key
Capitol College	B.S	Information Assurance	IAE 325	300	1074	Knowledge of transmission records	Telecommunicatio ns	3.) Secure data communications
Capitol College	B.S	Information Assurance	IAE 325	300	1114	Knowledge of encryption	Cryptography	1.)The history of encryption, 2.)
Capitol College	B.S	Information Assurance	IAE 402	400	55	Knowledge of Information	Information Assurance	(1) Explain the risk management
Capitol College	B.S	Information Assurance	IAE 402	400	60	Knowledge of incident categories, incident	Incident Management	(3)Give a scenario of a computer
Capitol College	B.S	Information Assurance	IAE 402	400	61	Knowledge of incident response and	Incident Management	(2)Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE 402	400	69	Knowledge of Risk Management	Information Systems Security	(6)Given a computer with a
Capitol College	B.S	Information Assurance	IAE 402	400	98	Knowledge of policybased and risk	Identity Management	(3)Given a scenario of a
Capitol College	B.S	Information Assurance	IAE 402	400	108	Knowledge of risk management	Risk Management	(1)Explain the risk management and
Capitol College	B.S	Information Assurance	IAE 402	400	153	Skill in handling malware	Computer Network Defense	(5)explain the ways to prevent
Capitol College	B.S	Information Assurance	IAE 402	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	(4)Explain the different types of
Capitol College	B.S	Information Assurance	IAE 402	400	229	Skill in using incident handling	Incident Management	(2)Demostrate the tools and

Capitol College	B.S	Information Assurance	IAE 402	400	895	Skill in recognizing and categorizing	Information Assurance	(4)Explain the different types of
Capitol College	B.S	Information Assurance	IAE 402	400	896	Skill in protecting a network against	Computer Network Defense	(2)Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE 402	400	897	Skill in performing damage assessments	Information Assurance	(1)Explain the risk management and
Capitol College	B.S	Information Assurance	IAE 402	400	921	Ability to identify possible threat actor	Technology Awareness	(4)Explain the different types of
Capitol College	B.S	Information Assurance	IAE 402	400	922	Skill in using network analysis tools to	Vulnerabilities Assessment	(2)Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE 402	400	952	Knowledge of emerging security	Technology Awareness	(1)Explain risk management and
Capitol College	B.S	Information Assurance	IAE 402	400	965	Knowledge of organization's risk	Risk Management	(1)Explain risk management and
Capitol College	B.S	Information Assurance	IAE 402	400	978	Knowledge of root cause analysis for	Incident Management	(5)Explain the way to prevent
Capitol College	B.S	Information Assurance	IAE 402	400	979	Knowledge of supply chain risk	Risk Management	(2)Demostrate tools and
Capitol College	B.S	Information Assurance	IAE 402	400	1021	Knowledge of threat assessment	Risk Management	(4)Explain the different types of
Capitol College	B.S	Information Assurance	IAE 402	400	1087	Skill in deep analysis of captured malicious	Computer Network Defense	(2)Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE 402	400	1096	Knowledge of malware analysis	Computer Network Defense	(2)Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE 402	400	1098	Skill in analyzing anomalous code as	Computer Network Defense	(4) Explain the different types of
Capitol College	B.S	Information Assurance	IAE405	400	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	(4)Identify malware through
Capitol College	B.S	Information Assurance	IAE405	400	123	Knowledge of system and application	Vulnerabilities Assessment	(4) Identifying malware through
Capitol College	B.S	Information Assurance	IAE405	400	128	Knowledge of systems diagnostic tools and	Systems Testing and Evaluation	(3)How to collect malware
Capitol College	B.S	Information Assurance	IAE405	400	153	Skill in handling malware	Computer Network Defense	(2) Types of malware.(4)
Capitol College	B.S	Information Assurance	IAE405	400	168	Skill in conducting software debugging	Software Development	(5) Reversing engineering of
Capitol College	B.S	Information Assurance	IAE405	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	(4)Identifying malware through
Capitol College	B.S	Information Assurance	IAE405	400	186	Skill in developing data dictionaries	Data Management	(1)History of malicious
Capitol College	B.S	Information Assurance	IAE405	400	187	Skill in developing data models	Modeling and Simulation	(3)How to collect malware samples.
Capitol College	B.S	Information Assurance	IAE405	400	205	Skill in implementing, maintaining, and	Information Systems/Network	(6)malware defenses
Capitol College	B.S	Information Assurance	IAE405	400	222	Skill in the basic operation of	Computer Skills	(5)Reverse engineering of
Capitol College	B.S	Information Assurance	IAE405	400	229	Skill in using incident handling	Incident Management	(3)How to collect malware
Capitol College	B.S	Information Assurance	IAE405	400	274	Knowledge of concepts, principles,	Computer Network Defense	(5)Reverse engineering of
Capitol College	B.S	Information Assurance	IAE405	400	296	Knowledge of how information needs	External Awareness	(3)How to collect malware
Capitol College	B.S	Information Assurance	IAE405	400	338	Knowledge of the principal methods,	Reasoning	(1)History of malicious
Capitol College	B.S	Information Assurance	IAE405	400	350	Skill in analyzing memory dumps to	Reasoning	(3)How to collect malware samples
Capitol College	B.S	Information Assurance	IAE405	400	896	Skill in protecting a network against	Computer Network Defense	(5)Reverse engineering of
Capitol College	B.S	Information Assurance	IAE405	400	991	Knowledge of different classes of	Computer Network Defense	(1)History of malicious

Capitol College	B.S	Information Assurance	IAE405	400	1029	Knowledge of malware analysis	Computer Network Defense	(2)Types of malware.
Capitol College	B.S	Information Assurance	IAE405	400	1062	Knowledge of software reverse	Vulnerabilities Assessment	(5)Reverse engineering of
Capitol College	B.S	Information Assurance	IAE405	400	1087	Skill in deep analysis of captured malicious	Computer Network Defense	(3)How to collect malware samples
Capitol College	B.S	Information Assurance	IAE405	400	1089	Knowledge of reverse engineering concepts	Vulnerabilities Assessment	(5)Reversing engineering of
Capitol College	B.S	Information Assurance	IAE405	400	1097	Knowledge of virtual machine aware	Computer Network Defense	(5) Reversing engineering of
Capitol College	B.S	Information Assurance	IAE406	400	24	Knowledge of concepts and	Data Management	(2) Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE406	400	29	Knowledge of data backup, types of	Computer Forensics	(7) Identify forensic
Capitol College	B.S	Information Assurance	IAE406	400	114	Knowledge of server diagnostic tools and	Computer Forensics	(2) Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE406	400	217	Skill in preserving evidence integrity	Computer Forensics	(1) Given a scenario, explain
Capitol College	B.S	Information Assurance	IAE406	400	290	Knowledge of processes for seizing	Forensics	(3)Given a scenario,
Capitol College	B.S	Information Assurance	IAE406	400	302	Knowledge of investigative	Computer Forensics	(2) Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE406	400	305	Knowledge of laws that affect cyber	Forensics	(3) Given a scenario,
Capitol College	B.S	Information Assurance	IAE406	400	310	Knowledge of legal governance related to	Criminal Law	(3) Given a scenario,
Capitol College	B.S	Information Assurance	IAE406	400	332	Ability to develop curriculum that	Teaching Others	(1) Explain the methods of
Capitol College	B.S	Information Assurance	IAE406	400	340	Knowledge of types and collection of	Computer Forensics	(2) Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE406	400	346	Knowledge of which system files (e.g. log	Computer Forensics	(2) Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE406	400	359	Skill in developing and executing technical	Computer Forensics	(2) Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE406	400	360	Skill in identifying and extracting data of	Computer Forensics	(4) Explain the methods of
Capitol College	B.S	Information Assurance	IAE406	400	369	Skill in collecting, processing,	Forensics	(1) Given a scenario, explain
Capitol College	B.S	Information Assurance	IAE406	400	374	Skill in setting up a forensic workstation	Forensics	(5) Explain the investigative
Capitol College	B.S	Information Assurance	IAE406	400	379	Skill in using common digital forensics tools	Computer Forensics	(2) Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE406	400	381	Skill in using forensic tool suites (e.g.	Computer Forensics	(7) Identify forensic
Capitol College	B.S	Information Assurance	IAE406	400	888	Knowledge of types of digital forensics data	Computer Forensics	(2) Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE406	400	889	Knowledge of deployable forensics	Computer Forensics	(1) Given a scenario, explain
Capitol College	B.S	Information Assurance	IAE406	400	890	Skill in conducting forensic analyses in	Computer Forensics	(7) Identify forensic
Capitol College	B.S	Information Assurance	IAE406	400	908	Ability to decrypt digital data collections	Computer Forensics	(2) Demostrate the tools and the
Capitol College	B.S	Information Assurance	IAE406	400	982	Knowledge of electronic evidence	Criminal Law	(6) Explain the use of digital
Capitol College	B.S	Information Assurance	IAE406	400	1044	Skill in identifying forensic footprints	Computer Forensics	(5) Explain the investigative
Capitol College	B.S	Information Assurance	IAE406	400	1062	Knowledge of software reverse	Vulnerabilities Assessment	(2)Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE406	400	1086	Knowledge of data carving tools and	Computer Forensics	(8) Identify forensic

Capitol College	B.S	Information Assurance	IAE406	400	1092	Knowledge of antiforensics tactics,	Computer Forensics	(2)Demostrate the tools and
Capitol College	B.S	Information Assurance	IAE406	400	1093	Knowledge of common forensic tool	Computer Forensics	(7) Identify forensic
Capitol College	B.S	Information Assurance	IAE406	400	1099	Skill in analyzing volatile data	Computer Forensics	(5) Explain the investigative
Capitol College	B.S	Information Assurance	IAE406	400	1101	Skill in interpreting results of debugger to	Computer Network Defense	(7) Identify forensic
Capitol College	B.S	Information Assurance	IAE410	400	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	4	Ability to identify systemic security	Vulnerabilities Assessment	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	5	Ability to match the appropriate	Knowledge Management	d.) tester's knowledge of the
Capitol College	B.S	Information Assurance	IAE410	400	7	Knowledge of "knowledge base"	Knowledge Management	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	8	Knowledge of access authentication	Identity Management	vv.) Describe the steps on how to
Capitol College	B.S	Information Assurance	IAE410	400	10	Knowledge of application	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	17	Knowledge of certified ethical	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	32	Knowledge of database	Database Management	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	34	Knowledge of database systems	Database Management	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	35	Knowledge of digital rights management	Encryption	tt.) Describe how WEP, WPA, and
Capitol College	B.S	Information Assurance	IAE410	400	40	Knowledge of organization's	Systems Testing and Evaluation	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	43	Knowledge of embedded systems	Embedded Computers	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	44	Knowledge of enterprise messaging	Enterprise Architecture	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	49	Knowledge of host/network access	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	51	Knowledge of how system components	Systems Integration	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	53	Knowledge of the Security Assessment	Information Assurance	g.) Prepare a risk assessment
Capitol College	B.S	Information Assurance	IAE410	400	58	Knowledge of known vulnerabilities from	Information Systems/Network	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	62	Knowledge of industrystandard and	Logical Systems Design	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	64	Knowledge of information security	Information Systems/ Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	69	Knowledge of Risk Management	Information Systems Security	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	70	Knowledge of information	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	76	Knowledge of measures or	Information Technology	g.) Prepare a risk assessment
Capitol College	B.S	Information Assurance	IAE410	400	77	Knowledege of current industry	Information Systems/Network	g.) Prepare a risk assessment
Capitol College	B.S	Information Assurance	IAE410	400	79	Knowledge of network access,	Identity Management	vv.) Describe the steps on how to
Capitol College	B.S	Information Assurance	IAE410	400	81	Knowledge of network	Infrastructure Design	dd.) Develop different attack
Capitol College	B.S	Information Assurance	IAE410	400	87	Knowledge of network traffic	Information Systems/Network	p.) live systems, ports,

Capitol College	B.S	Information Assurance	IAE410	400	89	Knowledge of new technological	Technology Awareness	dd.) Develop different attack
Capitol College	B.S	Information Assurance	IAE410	400	90	Knowledge of operating systems	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	93	Knowledge of packetlevel analysis	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	95	Knowledge of penetration testing	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	96	Knowledge of performance tuning	Information Technology	g.) Prepare a risk assessment
Capitol College	B.S	Information Assurance	IAE410	400	98	Knowledge of policybased and risk	Identity Management	vv.) Describe the steps on how to
Capitol College	B.S	Information Assurance	IAE410	400	99	Knowledge of principles and	Systems Integration	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	100	Knowledge of Privacy Impact Assessments	Personnel Safety and Security	g.) Prepare a risk assessment
Capitol College	B.S	Information Assurance	IAE410	400	101	Knowledge of process engineering concepts	Logical Systems Design	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	104	Knowledge of query languages such as	Database Management	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	106	Knowledge of remote access technology	Information Technology	vv.) Describe the steps on how to
Capitol College	B.S	Information Assurance	IAE410	400	111	Knowledge of security system design tools,	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	112	Knowledge of server administration and	Systems Life Cycle	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	113	Knowledge of server and client operating	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	121	Knowledge of structured analysis	Logical Systems Design	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	122	Knowledge of system administration	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	123	Knowledge of system and application	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	124	Knowledge of system design tools,	Logical Systems Design	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	127	Knowledge of systems administration	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	129	Knowledge of systems lifecycle management	Systems Life Cycle	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	132	Knowledge of technoloy integration	Systems Integration	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	134	Knowledge of the capabilities and	Technology Awareness	pp.) Discuss the various
Capitol College	B.S	Information Assurance	IAE410	400	135	Knowledge of the capabilities and	Data Management	pp.) Discuss the various
Capitol College	B.S	Information Assurance	IAE410	400	136	Knowledge of the capabilities and	Technology Awareness	pp.) Discuss the various
Capitol College	B.S	Information Assurance	IAE410	400	138	Knowledge of the computer network	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	139	Knowledge of common networking	Infrastructure Design	y.) Describe the various processes
Capitol College	B.S	Information Assurance	IAE410	400	142	Knowledge of the operations and	Systems Life Cycle	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	144	Knowledge of the systems engineering	Systems Life Cycle	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	145	Knowledge of the type and frequency of	Systems Life Cycle	p.) live systems, ports,

Capitol College	B.S	Information Assurance	IAE410	400	148	Knowledge of VPN security.	Encryption	tt.) Describe how WEP, WPA, and
Capitol College	B.S	Information Assurance	IAE410	400	149	Knowledge of web services, including	Web Technology	y.) Describe the various processes
Capitol College	B.S	Information Assurance	IAE410	400	150	Knowledge of what constitutes a network	Information Systems/Network	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	152	Skill in allocating storage capacity in	Database Administration	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	157	Skill in applying host/network access	Identity Management	vv.) Describe the steps on how to
Capitol College	B.S	Information Assurance	IAE410	400	158	Skill in applying organizationspecific	Systems Testing and Evaluation	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	162	Skill in conducting capabilities and	Requirements Analysis	ff.) Conduct a bruteforce attack
Capitol College	B.S	Information Assurance	IAE410	400	163	Skill in conducting information searches	Computer Skills	ff.) Conduct a bruteforce attack
Capitol College	B.S	Information Assurance	IAE410	400	165	Skill in conducting open source research	Knowledge Management	u.) Determine the difference
Capitol College	B.S	Information Assurance	IAE410	400	166	Skill in conducting queries and	Database Management	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	167	Skill in conducting server planning,	Network Management	dd.) Develop different attack
Capitol College	B.S	Information Assurance	IAE410	400	169	Skill in conducting test events	Systems Testing and Evaluation	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	171	Skill in correcting physical and technical	Network Management	dd.) Develop different attack
Capitol College	B.S	Information Assurance	IAE410	400	173	Skill in creating policies that relfect	Information Systems Security	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	174	Skill in creating programs that	Software Testing and Evaluation	d.) tester's knowledge of the
Capitol College	B.S	Information Assurance	IAE410	400	175	Skill in developing and deploying signatures	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	176	Skill in designing a data analysis	Systems Testing and Evaluation	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	180	Skill in designing the integration of	Systems Integration	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	182	Skill in determining an appropriate level of	Systems Testing and Evaluation	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	183	Skill in determining how a security system	Information Assurance	d.) tester's knowledge of the
Capitol College	B.S	Information Assurance	IAE410	400	190	Skill in developing operationsbased	Systems Testing and Evaluation	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	191	Skill in developing and applying security	Identity Management	vv.) Describe the steps on how to
Capitol College	B.S	Information Assurance	IAE410	400	195	Skill in diagnosing failed servers	Network Management	dd.) Develop different attack
Capitol College	B.S	Information Assurance	IAE410	400	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	201	Skill in generating queries and reports	Database Management	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	202	Skill in identifying and anticipating server	Information Technology	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	203	Skill in identifying measures or	Information Technology	a.) Identify the differences

Capitol College	B.S	Information Assurance	IAE410	400	204	Skill in identifying possible causes of	Systems Life Cycle	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	205	Skill in implementing, maintaining, and	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	206	Skill in installing computer and server	Systems Life Cycle	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	208	Skill in maintaining databases	Database Management	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	211	Skill in monitoring and optimizing server	Information Technology	g.) Prepare a risk assessment
Capitol College	B.S	Information Assurance	IAE410	400	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	216	Skill in recovering failed servers	Incident Management	dd.) Develop different attack
Capitol College	B.S	Information Assurance	IAE410	400	219	Skill in system administration for	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	220	Skill in systems integration testing	Systems Testing and Evaluation	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	225	Skill in the use of penetration testing	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	233	Skill in using protocol analyzers	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	237	Skill in using Virtual Private Network	Encryption	tt.) Describe how WEP, WPA, and
Capitol College	B.S	Information Assurance	IAE410	400	239	Skill in writing test plans	Systems Testing and Evaluation	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	261	Knowledge of basic concepts,	Telecommunicatio ns	qq.) ng wireless access points
Capitol College	B.S	Information Assurance	IAE410	400	264	Knowledge of basic physical computer	Computers and Electronics	pp.) Discuss the various
Capitol College	B.S	Information Assurance	IAE410	400	278	Knowledge of different types of	Telecommunicatio ns	qq.) ng wireless access points
Capitol College	B.S	Information Assurance	IAE410	400	281	Knowledge of electronic devices	Hardware	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	284	Knowledge of encryption algorithms	Cryptography	tt.) Describe how WEP, WPA, and
Capitol College	B.S	Information Assurance	IAE410	400	286	Knowledge of file extensions (e.g., .dll,	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	287	Knowledge of file system	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	294	Knowledge of hacking methodologies in	Surveillance	d.) tester's knowledge of the
Capitol College	B.S	Information Assurance	IAE410	400	296	Knowledge of how information needs	External Awareness	ww.) Describe the available tools
Capitol College	B.S	Information Assurance	IAE410	400	297	Knowledge of industry indicators	Technology Awareness	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	302	Knowledge of investigative	Computer Forensics	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	310	Knowledge of legal governance related to	Criminal Law	h.)Prepare a "Rules of
Capitol College	B.S	Information Assurance	IAE410	400	313	Knowledge of logging services for network	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	321	Knowledge of products and	Technology Awareness	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	326	Knowledge of security hardware and	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	329	Knowledge of surveillance detection	Surveillance	r.) security countermeasures.
Capitol College	B.S	Information Assurance	IAE410	400	332	Ability to develop curriculum that	Teaching Others	e.) Gather reconnaissance

Capitol College	B.S	Information Assurance	IAE410	400	339	Knowledge of the structure and intent	Organizational Awareness	h.)Prepare a "Rules of
Capitol College	B.S	Information Assurance	IAE410	400	341	Knowledge of UNIX and Windows systems	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	344	Knowledge of virtualization	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	345	Knowledge of web mail collection,	Web Technology	y.) Describe the various processes
Capitol College	B.S	Information Assurance	IAE410	400	347	Knowledge of Windows command	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	348	Knowledge of wireless network collection	Cryptography	qq.) ng wireless access points
Capitol College	B.S	Information Assurance	IAE410	400	350	Skill in analyzing memory dumps to	Reasoning	a. Extract metadata from
Capitol College	B.S	Information Assurance	IAE410	400	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	b.) auditing, penetration
Capitol College	B.S	Information Assurance	IAE410	400	356	Skill in determining installed patches on	Operating Systems	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	357	Skill in determining the effects of various	Configuration Management	d.) tester's knowledge of the
Capitol College	B.S	Information Assurance	IAE410	400	360	Skill in identifying and extracting data of	Computer Forensics	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	363	Skill in identifying gaps in technical	Teaching Others	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	364	Skill in identifying, modifying, and	Operating Systems	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	371	Skill in reading, interpreting, writing,	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	375	Skill in survey, collection, and	Network Management	qq.) ng wireless access points
Capitol College	B.S	Information Assurance	IAE410	400	377	Skill in tracking and analyzing technical	Legal, Government and Jurisprudence	ww.) Describe the available tools
Capitol College	B.S	Information Assurance	IAE410	400	383	Skill in using scientific rules and methods to	Reasoning	h.)Prepare a "Rules of
Capitol College	B.S	Information Assurance	IAE410	400	386	Skill in using virtual machines	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	387	Skill in verifying the integrity of encrypted	Encryption	tt.) Describe how WEP, WPA, and
Capitol College	B.S	Information Assurance	IAE410	400	886	Skill in wireless network target	Vulnerabilities Assessment	e.) Gather reconnaissance
Capitol College	B.S	Information Assurance	IAE410	400	890	Skill in conducting forensic analyses in	Computer Forensics	d.) tester's knowledge of the
Capitol College	B.S	Information Assurance	IAE410	400	891	Skill in configuring and utilizing	Configuration Management	dd.) Develop different attack
Capitol College	B.S	Information Assurance	IAE410	400	895	Skill in recognizing and categorizing	Information Assurance	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	897	Skill in performing damage assessments	Information Assurance	g.) Prepare a risk assessment
Capitol College	B.S	Information Assurance	IAE410	400	900	Knowledge of web filtering technologies	Web Technology	y.) Describe the various processes
Capitol College	B.S	Information Assurance	IAE410	400	901	Knowledge of the capabilities of	Network Management	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	902	Knowledge of the range of existing	Network Management	qq.) ng wireless access points
Capitol College	B.S	Information Assurance	IAE410	400	903	Knowledge of Wireless Fidelity	Network Management	qq.) ng wireless access points
Capitol College	B.S	Information Assurance	IAE410	400	914	Skill in identifying gaps in cyber	Strategic Thinking	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	915	Knowledge of frontend collection	Information Systems/Network	p.) live systems, ports,

Capitol College	B.S	Information Assurance	IAE410	400	917	Knowledge of social dynamics of computer	External Awareness	gg.) Correctly execute the
Capitol College	B.S	Information Assurance	IAE410	400	918	Ability to prepare and deliver education and	Teaching Others	g.) Prepare a risk assessment
Capitol College	B.S	Information Assurance	IAE410	400	921	Ability to identify possible threat actor	Technology Awareness	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	922	Skill in using network analysis tools to	Vulnerabilities Assessment	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	923	Knowledge of security event correlation	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	950	Skill in evaluating test plans for applicability	Systems Testing and Evaluation	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	952	Knowledge of emerging security	Technology Awareness	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	967	Knowledge of current and emerging	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	968	Knowledge of softwarerelated	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	975	Skill in integrating black box security	Quality Assurance	c.) Discuss the difference in
Capitol College	B.S	Information Assurance	IAE410	400	985	Skill in configuring and utilizing network	Configuration Management	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	986	Knowledge of organizational	Identity Management	h.)Prepare a “Rules of
Capitol College	B.S	Information Assurance	IAE410	400	990	Knowledge of common attack	Computer Network Defense	gg.) Correctly execute the
Capitol College	B.S	Information Assurance	IAE410	400	991	Knowledge of different classes of	Computer Network Defense	gg.) Correctly execute the
Capitol College	B.S	Information Assurance	IAE410	400	992	Knowledge of different operational	Computer Network Defense	d.) tester’s knowledge of the
Capitol College	B.S	Information Assurance	IAE410	400	1002	Skill in conducting audits or reviews of	Information Technology	g.) Prepare a risk assessment
Capitol College	B.S	Information Assurance	IAE410	400	1008	Knowledge of how to troubleshoot basic	Operating Systems	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	1020	Skill in secure test plan deisn (i.e., unit,	Systems Testing and Evaluation	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	1021	Knowledge of threat assessment	Risk Management	g.) Prepare a risk assessment
Capitol College	B.S	Information Assurance	IAE410	400	1033	Knowledge of basic system	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	1038	Knowledge of local specialized system	Infrastructure Design	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	1042	Abililty to apply network	Requirements Analysis	u.) Determine the difference
Capitol College	B.S	Information Assurance	IAE410	400	1044	Skill in identifying forensic footprints	Computer Forensics	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	1052	Knowledge of Global Systems for Mobile	Telecommunicatio ns	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	1054	Knowledge of hardware reverse	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	1061	Knowledge of the lifecycle process	Systems Life Cycle	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	1062	Knowledge of software reverse	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	1063	Knowledge of Unix/Linux operating	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	a.) Identify the differences

Capitol College	B.S	Information Assurance	IAE410	400	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	m.) Determine the proper
Capitol College	B.S	Information Assurance	IAE410	400	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	m.) Determine the proper
Capitol College	B.S	Information Assurance	IAE410	400	1072	Knowledge of network security	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	1073	Knowledge of network systems	Network Management	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	1074	Knowledge of transmission records	Telecommunications	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	1089	Knowledge of reverse engineering concepts	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	1091	Skill in one way hash functions (e.g., Secure	Data Management	ii.) Properly execute Pwdump
Capitol College	B.S	Information Assurance	IAE410	400	1095	Knowledge of how different file types can	Vulnerabilities Assessment	f.) Determine various types of
Capitol College	B.S	Information Assurance	IAE410	400	1100	Skill in identifying obfusification	Computer Network Defense	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	1114	Knowledge of encryption	Cryptography	tt.) Describe how WEP, WPA, and
Capitol College	B.S	Information Assurance	IAE410	400	1116	Skill in identifying common encoding	Computer Languages	a.) Identify the differences
Capitol College	B.S	Information Assurance	IAE410	400	1117	Skill in utilizing virtual networks for testing	Operating Systems	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	1118	Skill in reading and interpreting	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	1119	Knowledge of signature	Information Systems/Network	p.) live systems, ports,
Capitol College	B.S	Information Assurance	IAE410	400	1121	Knowledge of Windows/Unix ports	Operating Systems	p.) live systems, ports,
College of Southern	A.S	Information Systems Security	ITS2090	200	12	Knowledge of communication	Infrastructure Design	Explain network design elements
College of Southern	A.S	Information Systems Security	ITS2090	200	19	Knowledge of Computer Network	Computer Network Defense	Explain network design elements
College of Southern	A.S	Information Systems Security	ITS2090	200	22	Knowledge of computer networking	Infrastructure Design	Explain network design elements
College of Southern	A.S	Information Systems Security	ITS2090	200	27	Knowledge of cryptology	Cryptography	Compare basic cryptography
College of Southern	A.S	Information Systems Security	ITS2090	200	49	Knowledge of host/network access	Information Systems/Network	Identify and apply industry best
College of Southern	A.S	Information Systems Security	ITS2090	200	70	Knowledge of information	Information Systems/Network	Compare basic cryptography
College of Southern	A.S	Information Systems Security	ITS2090	200	82	Knowledge of network design	Infrastructure Design	Explain network design elements
College of Southern	A.S	Information Systems Security	ITS2090	200	98	Knowledge of policybased and risk	Identity Management	Identify and apply industry best
College of Southern	A.S	Information Systems Security	ITS2090	200	108	Knowledge of risk management	Risk Management	Conduct computer/networ
College of Southern	A.S	Information Systems Security	ITS2090	200	111	Knowledge of security system design tools,	Information Systems/Network	Explain network design elements
College of Southern	A.S	Information Systems Security	ITS2090	200	123	Knowledge of system and application	Vulnerabilities Assessment	Differentiate amongst various
College of Southern	A.S	Information Systems Security	ITS2090	200	157	Skill in applying host/network access	Identity Management	Identify and apply industry best
College of Southern	A.S	Information Systems Security	ITS2090	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	Differentiate amongst various
College of Southern	A.S	Information Systems Security	ITS2090	200	191	Skill in developing and applying security	Identity Management	Identify and apply industry best
College of Southern	A.S	Information Systems Security	ITS2090	200	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	Conduct computer/networ

College of Southern	A.S	Information Systems Security	ITS2090	200	271	Knowledge of common network	Infrastructure Design	Explain network design elements
College of Southern	A.S	Information Systems Security	ITS2090	200	284	Knowledge of encryption algorithms	Cryptography	Compare basic cryptography
College of Southern	A.S	Information Systems Security	ITS2090	200	897	Skill in performing damage assessments	Information Assurance	Conduct computer/networ
College of Southern	A.S	Information Systems Security	ITS2090	200	922	Skill in using network analysis tools to	Vulnerabilities Assessment	Explain network design elements
College of Southern	A.S	Information Systems Security	ITS2090	200	986	Knowledge of organizational	Identity Management	Identify physical access security
College of Southern	A.S	Information Systems Security	ITS2090	200	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	Explain network design elements
College of Southern	A.S	Information Systems Security	ITS2090	200	1114	Knowledge of encryption	Cryptography	Compare basic cryptography
College of Southern	A.S	Information Systems Security	ITS2500	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Analyze and assess a
College of Southern	A.S	Information Systems Security	ITS2500	200	4	Ability to identify systemic security	Vulnerabilities Assessment	Analyze and assess a
College of Southern	A.S	Information Systems Security	ITS2500	200	17	Knowledge of certified ethical	Vulnerabilities Assessment	Outline the ethical standards
College of Southern	A.S	Information Systems Security	ITS2500	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	Use various tools, systems and
College of Southern	A.S	Information Systems Security	ITS2500	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	Use various tools, systems and
College of Southern	A.S	Information Systems Security	ITS2500	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	Use various tools, systems and
College of Southern	A.S	Information Systems Security	ITS2500	200	274	Knowledge of concepts, principles,	Computer Network Defense	Use various tools, systems and
College of Southern	A.S	Information Systems Security	ITS2500	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	Outline the ethical standards
College of Southern	A.S	Information Systems Security	ITS2500	200	922	Skill in using network analysis tools to	Vulnerabilities Assessment	Analyze and assess a
College of Southern	A.S	Information Systems Security	ITS2500	200	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	Use various tools, systems and
College of Southern	A.S	Information Systems Security	ITS2500	200	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	Use various tools, systems and
College of Southern	A.S	Information Systems Security	ITS2500	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Explain the process of
College of Southern	A.S	Information Systems Security	ITS2500	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Explain the process of
College of Southern	B.S	Information Systems Security	ITS2530	200	12	Knowledge of communication	Infrastructure Design	Cryptography
College of Southern	B.S	Information Systems Security	ITS2530	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	Cryptography
College of Southern	B.S	Information Systems Security	ITS2530	200	27	Knowledge of cryptology	Cryptography	Cryptography
College of Southern	B.S	Information Systems Security	ITS2530	200	55	Knowledge of Information	Information Assurance	Performing Risk Analysis
College of Southern	B.S	Information Systems Security	ITS2530	200	69	Knowledge of Risk Management	Information Systems Security	Performing Risk Analysis
College of Southern	B.S	Information Systems Security	ITS2530	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	Penetration Testing
College of Southern	B.S	Information Systems Security	ITS2530	200	98	Knowledge of policybased and risk	Identity Management	Performing Risk Analysis
College of Southern	B.S	Information Systems Security	ITS2530	200	108	Knowledge of risk management	Risk Management	Performing Risk Analysis
College of Southern	B.S	Information Systems Security	ITS2530	200	122	Knowledge of system administration	Operating Systems	Hardening Linux Systems
College of Southern	B.S	Information Systems Security	ITS2530	200	219	Skill in system administration for	Operating Systems	Hardening Linux Systems

College of Southern	B.S	Information Systems Security	ITS2530	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	Penetration Testing
College of Southern	B.S	Information Systems Security	ITS2530	200	284	Knowledge of encryption algorithms	Cryptography	Cryptography
College of Southern	B.S	Information Systems Security	ITS2530	200	294	Knowledge of hacking methodologies in	Surveillance	Hardening Linux Systems
College of Southern	B.S	Information Systems Security	ITS2530	200	348	Knowledge of wireless network collection	Cryptography	Cryptography
College of Southern	B.S	Information Systems Security	ITS2530	200	364	Skill in identifying, modifying, and	Operating Systems	Hardening Linux Systems
College of Southern	B.S	Information Systems Security	ITS2530	200	918	Ability to prepare and deliver education and	Teaching Others	Creating Security Policies
College of Southern	B.S	Information Systems Security	ITS2530	200	952	Knowledge of emerging security	Technology Awareness	Performing Risk Analysis
College of Southern	B.S	Information Systems Security	ITS2530	200	954	Knowledge of Export Control regulations	Contracting/Procurement	Performing Risk Analysis
College of Southern	B.S	Information Systems Security	ITS2530	200	965	Knowledge of organization's risk	Risk Management	Performing Risk Analysis
College of Southern	B.S	Information Systems Security	ITS2530	200	979	Knowledge of supply chain risk	Risk Management	Performing Risk Analysis
College of Southern	B.S	Information Systems Security	ITS2530	200	986	Knowledge of organizational	Identity Management	Creating Security Policies
College of Southern	B.S	Information Systems Security	ITS2530	200	1033	Knowledge of basic system	Information Systems/Network	Hardening Linux Systems
College of Southern	B.S	Information Systems Security	ITS2530	200	1114	Knowledge of encryption	Cryptography	Cryptography
College of Southern	B.S	Information Systems Security	ITS2535	200	28	Knowledge of data administration and	Data Management	Policies Standards
College of Southern	B.S	Information Systems Security	ITS2535	200	33	Knowledge of database procedures	Incident Management	Establish a Incident
College of Southern	B.S	Information Systems Security	ITS2535	200	37	Knowledge of disaster recovery and	Incident Management	Establish a Incident
College of Southern	B.S	Information Systems Security	ITS2535	200	49	Knowledge of host/network access	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	58	Knowledge of known vulnerabilities from	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	60	Knowledge of incident categories, incident	Incident Management	Establish a Incident
College of Southern	B.S	Information Systems Security	ITS2535	200	61	Knowledge of incident response and	Incident Management	Establish a Incident
College of Southern	B.S	Information Systems Security	ITS2535	200	64	Knowledge of information security	Information Systems/ Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	70	Knowledge of information	Information Systems/Network	Network Security, Configure
College of Southern	B.S	Information Systems Security	ITS2535	200	77	Knowledege of current industry	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	87	Knowledge of network traffic	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	Vulnerability Testing and
College of Southern	B.S	Information Systems Security	ITS2535	200	111	Knowledge of security system design tools,	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	126	Knowledge of system software and	Requirements Analysis	Policies Standards
College of Southern	B.S	Information Systems Security	ITS2535	200	138	Knowledge of the computer network	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	148	Knowledge of VPN security.	Encryption	Configure firewalls and
College of Southern	B.S	Information Systems Security	ITS2535	200	150	Knowledge of what constitutes a network	Information Systems/Network	Network Security

College of Southern	B.S	Information Systems Security	ITS2535	200	173	Skill in creating policies that relfect	Information Systems Security	Policies Standards
College of Southern	B.S	Information Systems Security	ITS2535	200	175	Skill in developing and deploying signatures	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	205	Skill in implementing, maintaining, and	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	216	Skill in recovering failed servers	Incident Management	Establish a Incident
College of Southern	B.S	Information Systems Security	ITS2535	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	Vulnerability Testing and
College of Southern	B.S	Information Systems Security	ITS2535	200	229	Skill in using incident handling	Incident Management	Establish a Incident
College of Southern	B.S	Information Systems Security	ITS2535	200	237	Skill in using Virtual Private Network	Encryption	Configure firewalls and
College of Southern	B.S	Information Systems Security	ITS2535	200	277	Knowledge of defense indepth principles and	Computer Network Defense	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	300	Knowledge of intelligence reporting	Organizational Awareness	Policies Standards
College of Southern	B.S	Information Systems Security	ITS2535	200	313	Knowledge of logging services for network	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	326	Knowledge of security hardware and	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	341	Knowledge of UNIX and Windows systems	Operating Systems	Configure firewalls and
College of Southern	B.S	Information Systems Security	ITS2535	200	891	Skill in configuring and utilizing	Configuration Management	Configure firewalls and
College of Southern	B.S	Information Systems Security	ITS2535	200	892	Skill in configuring and utilizing	Configuration Management	Configure firewalls and
College of Southern	B.S	Information Systems Security	ITS2535	200	915	Knowledge of frontend collection	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	918	Ability to prepare and deliver education and	Teaching Others	Policies Standards
College of Southern	B.S	Information Systems Security	ITS2535	200	923	Knowledge of security event correlation	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	966	Knowledge of enterprise incident	Incident Management	Establish a Incident
College of Southern	B.S	Information Systems Security	ITS2535	200	967	Knowledge of current and emerging	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	968	Knowledge of softwarerelated	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	978	Knowledge of root cause analysis for	Incident Management	Establish a Incident
College of Southern	B.S	Information Systems Security	ITS2535	200	980	Skill in performing root cause analysis for	Incident Management	Establish a Incident
College of Southern	B.S	Information Systems Security	ITS2535	200	984	Knowledge of computer network	Computer Network Defense	Policies Standards
College of Southern	B.S	Information Systems Security	ITS2535	200	985	Skill in configuring and utilizing network	Configuration Management	Configure firewalls and
College of Southern	B.S	Information Systems Security	ITS2535	200	986	Knowledge of organizational	Identity Management	Policies Standards
College of Southern	B.S	Information Systems Security	ITS2535	200	1011	Knowledge of processes for	Security	Network Security, Establish a
College of Southern	B.S	Information Systems Security	ITS2535	200	1033	Knowledge of basic system	Information Systems/Network	Network Security
College of Southern	B.S	Information Systems Security	ITS2535	200	1037	Knowledge of information	Risk Management	Policies Standards
College of Southern	B.S	Information Systems Security	ITS2535	200	1040	Knowledge of relevant laws,	Criminal Law	Policies Standards

College of Southern	B.S	Information Systems Security	ITS2535	200	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	Policies Standards
College of Southern	B.S	Information Systems Security	ITS2535	200	1072	Knowledge of network security	Information Systems/Network	Network Security
George Mason University	B.S	Applied Information	IT 223	200	4	Ability to identify systemic security	Vulnerabilities Assessment	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	8	Knowledge of access authentication	Identity Management	1. Organizational policy to define
George Mason University	B.S	Applied Information	IT 223	200	38	Knowledge of organization's	Information Assurance	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	49	Knowledge of host/network access	Information Systems/Network	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	53	Knowledge of the Security Assessment	Information Assurance	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	58	Knowledge of known vulnerabilities from	Information Systems/Network	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	63	Knowledge of Information	Information Assurance	1. Organizational policy to define
George Mason University	B.S	Applied Information	IT 223	200	65	Knowledge of information theory	Mathematical Reasoning	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	69	Knowledge of Risk Management	Information Systems Security	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	70	Knowledge of information	Information Systems/Network	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	77	Knowledege of current industry	Information Systems/Network	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	82	Knowledge of network design	Infrastructure Design	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	87	Knowledge of network traffic	Information Systems/Network	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	88	Knowledge of new and emerging	Technology Awareness	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	156	Skill in applying confidentiality,	Information Assurance	1. Organizational policy to define
George Mason University	B.S	Applied Information	IT 223	200	217	Skill in preserving evidence integrity	Computer Forensics	1. Organizational policy to define
George Mason University	B.S	Applied Information	IT 223	200	341	Knowledge of UNIX and Windows systems	Operating Systems	1. Organizational policy to define
George Mason University	B.S	Applied Information	IT 223	200	387	Skill in verifying the integrity of encrypted	Encryption	1. Organizational policy to define
George Mason University	B.S	Applied Information	IT 223	200	915	Knowledge of frontend collection	Information Systems/Network	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	918	Ability to prepare and deliver education and	Teaching Others	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	923	Knowledge of security event correlation	Information Systems/Network	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	952	Knowledge of emerging security	Technology Awareness	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	967	Knowledge of current and emerging	Information Systems/Network	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	968	Knowledge of softwarerelated	Information Systems/Network	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	975	Skill in integrating black box security	Quality Assurance	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	981	Knowledge of International Traffic in	Criminal Law	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	986	Knowledge of organizational	Identity Management	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	1005	Knowledge of functionality, quality,	Contracting/Procurement	2. Different types of security

George Mason University	B.S	Applied Information	IT 223	200	1011	Knowledge of processes for	Security	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	1033	Knowledge of basic system	Information Systems/Network	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	1034	Knowledge of Personally Identifiable	Security	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	1037	Knowledge of information	Risk Management	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	1056	Knowledge of operations security	Public Safety and Security	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	1072	Knowledge of network security	Information Systems/Network	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	1118	Skill in reading and interpreting	Information Systems/Network	2. Different types of security
George Mason University	B.S	Applied Information	IT 223	200	1119	Knowledge of signature	Information Systems/Network	2. Different types of security
George Mason University	B.S	Applied Information	IT 353	300	12	Knowledge of communication	Infrastructure Design	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	15	Knowledge of capabilities and	Hardware	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	19	Knowledge of Computer Network	Computer Network Defense	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	41	Knowledge of organization's Local	Infrastructure Design	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	49	Knowledge of host/network access	Information Systems/Network	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	50	Knowledge of how network services and	Infrastructure Design	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	58	Knowledge of known vulnerabilities from	Information Systems/Network	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	59	Knowledge of Intrusion Detection	Computer Network Defense	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	64	Knowledge of information security	Information Systems/ Network	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	66	Knowledge of intrusion detection	Computer Network Defense	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	70	Knowledge of information	Information Systems/Network	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	72	Knowledge of local area network (LAN)	Infrastructure Design	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	77	Knowledege of current industry	Information Systems/Network	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	79	Knowledge of network access,	Identity Management	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	81	Knowledge of network	Infrastructure Design	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	82	Knowledge of network design	Infrastructure Design	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	83	Knowledge of network hardware	Hardware	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	87	Knowledge of network traffic	Information Systems/Network	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	92	Knowledge of how traffic flows across	Infrastructure Design	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	111	Knowledge of security system design tools,	Information Systems/Network	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	115	Knowledge of content development	Computer Network Defense	3. Network centric warfare

George Mason University	B.S	Applied Information	IT 353	300	138	Knowledge of the computer network	Information Systems/Network	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	139	Knowledge of common networking	Infrastructure Design	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	146	Knowledge of the types of Intrusion	Computer Network Defense	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	150	Knowledge of what constitutes a network	Information Systems/Network	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	153	Skill in handling malware	Computer Network Defense	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	154	Skill in analyzing network traffic	Capacity Management	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	157	Skill in applying host/network access	Identity Management	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	167	Skill in conducting server planning,	Network Management	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	171	Skill in correcting physical and technical	Network Management	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	175	Skill in developing and deploying signatures	Information Systems/Network	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	181	Skill in detecting host and network based	Computer Network Defense	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	193	Skill in developing, testing, and	Information Assurance	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	194	Skill in diagnosing connectivity problems	Network Management	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	195	Skill in diagnosing failed servers	Network Management	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	205	Skill in implementing, maintaining, and	Information Systems/Network	3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	207	Skill in installing, configuring, and		3. Network centric warfare
George Mason University	B.S	Applied Information	IT 353	300	294	Knowledge of hacking methodologies in	Surveillance	8. recconaissance and survaillance
George Mason University	B.S	Applied Information	IT 353	300	329	Knowledge of surveillance detection	Surveillance	8. recconaissance and survaillance
George Mason University	B.S	Applied Information	IT 353	300	1036	Knowledge of applicable laws (e.g.,	Criminal Law	8. recconaissance and survaillance
George Mason University	B.S	Applied Information	IT 357	300	217	Skill in preserving evidence integrity	Computer Forensics	2. Legal principles such as chain of
George Mason University	B.S	Applied Information	IT 357	300	290	Knowledge of processes for seizing	Forensics	2. Legal principles such as chain of
George Mason University	B.S	Applied Information	IT 357	300	310	Knowledge of legal governance related to	Criminal Law	2. Legal principles such as chain of
George Mason University	B.S	Applied Information	IT 357	300	316	Knowledge of processes for	Criminal Law	2. Legal principles such as chain of
George Mason University	B.S	Applied Information	IT 357	300	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	1. presents auditing, logging,
George Mason University	B.S	Applied Information	IT 357	300	369	Skill in collecting, processing,	Forensics	2. Legal principles such as chain of
George Mason University	B.S	Applied Information	IT 357	300	982	Knowledge of electronic evidence	Criminal Law	2. Legal principles such as chain of
George Mason University	B.S	Applied Information	IT 357	300	1002	Skill in conducting audits or reviews of	Information Technology	1. presents auditing, logging,
George Mason university	B.S	Applied Information	IT 366	300	12	Knowledge of communication	Infrastructure Design	1. Symmetric and asymmetric
George Mason university	B.S	Applied Information	IT 366	300	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	1. Symmetric and asymmetric

George Mason university	B.S	Applied Information	IT 366	300	27	Knowledge of cryptology	Cryptography	1. Symmetric and asymmetric
George Mason university	B.S	Applied Information	IT 366	300	79	Knowledge of network access,	Identity Management	4. digital certificates and
George Mason university	B.S	Applied Information	IT 366	300	284	Knowledge of encryption algorithms	Cryptography	1. Symmetric and asymmetric
George Mason university	B.S	Applied Information	IT 366	300	348	Knowledge of wireless network collection	Cryptography	1. Symmetric and asymmetric
George Mason university	B.S	Applied Information	IT 366	300	1091	Skill in one way hash functions (e.g., Secure	Data Management	3. Hash functions and digital
George Mason university	B.S	Applied Information	IT 366	300	1114	Knowledge of encryption	Cryptography	1. Symmetric and asymmetric
George Mason University	B.S	Applied Information	IT 466	400	12	Knowledge of communication	Infrastructure Design	1. symmetric and asymmetric
George Mason University	B.S	Applied Information	IT 466	400	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	1. symmetric and asymmetric
George Mason University	B.S	Applied Information	IT 466	400	27	Knowledge of cryptology	Cryptography	1. symmetric and asymmetric
George Mason University	B.S	Applied Information	IT 466	400	93	Knowledge of packetlevel analysis	Vulnerabilities Assessment	2. Analysis of network data
George Mason University	B.S	Applied Information	IT 466	400	95	Knowledge of penetration testing	Vulnerabilities Assessment	4. Testing secure networks,
George Mason University	B.S	Applied Information	IT 466	400	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	2. Analysis of network data
George Mason University	B.S	Applied Information	IT 466	400	225	Skill in the use of penetration testing	Vulnerabilities Assessment	4. Testing secure networks,
George Mason University	B.S	Applied Information	IT 466	400	284	Knowledge of encryption algorithms	Cryptography	1. symmetric and asymmetric
George Mason University	B.S	Applied Information	IT 466	400	348	Knowledge of wireless network collection	Cryptography	1. symmetric and asymmetric
George Mason University	B.S	Applied Information	IT 466	400	990	Knowledge of common attack	Computer Network Defense	3. Security at different network
George Mason University	B.S	Applied Information	IT 466	400	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	2. Analysis of network data
George Mason University	B.S	Applied Information	IT 466	400	1114	Knowledge of encryption	Cryptography	1. symmetric and asymmetric
George Mason University	B.S	Applied Information	IT 462	400	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	4	Ability to identify systemic security	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	8	Knowledge of access authentication	Identity Management	3. Authentication technologies.
George Mason University	B.S	Applied Information	IT 462	400	10	Knowledge of application	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	17	Knowledge of certified ethical	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	58	Knowledge of known vulnerabilities from	Information Systems/Network	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	63	Knowledge of Information	Information Assurance	3. Authentication technologies.
George Mason University	B.S	Applied Information	IT 462	400	93	Knowledge of packetlevel analysis	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	95	Knowledge of penetration testing	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	123	Knowledge of system and application	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	150	Knowledge of what constitutes a network	Information Systems/Network	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	4. Common system

George Mason University	B.S	Applied Information	IT 462	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	225	Skill in the use of penetration testing	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	233	Skill in using protocol analyzers	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	321	Knowledge of products and	Technology Awareness	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	341	Knowledge of UNIX and Windows systems	Operating Systems	3. Authentication technologies.
George Mason University	B.S	Applied Information	IT 462	400	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	886	Skill in wireless network target	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	895	Skill in recognizing and categorizing	Information Assurance	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	918	Ability to prepare and deliver education and	Teaching Others	1. Security policies, models
George Mason University	B.S	Applied Information	IT 462	400	922	Skill in using network analysis tools to	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	952	Knowledge of emerging security	Technology Awareness	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	986	Knowledge of organizational	Identity Management	1. Security policies, models
George Mason University	B.S	Applied Information	IT 462	400	1054	Knowledge of hardware reverse	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	1062	Knowledge of software reverse	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	1089	Knowledge of reverse engineering concepts	Vulnerabilities Assessment	4. Common system
George Mason University	B.S	Applied Information	IT 462	400	1095	Knowledge of how different file types can	Vulnerabilities Assessment	4. Common system
Jackson State Community	CIS	Cyber Defense, Networking,	CIS 156	100	4	Ability to identify systemic security	Vulnerabilities Assessment	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	7	Knowledge of “knowledge base”	Knowledge Management	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	9	Knowledge of applicable business	Requirements Analysis	• 2. Learn how information
Jackson State Community	CIS	Elective	CIS 156	100	202	Skill in identifying and anticipating server	Information Technology	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	203	Skill in identifying measures or	Information Technology	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	204	Skill in identifying possible causes of	Systems Life Cycle	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	205	Skill in implementing, maintaining, and	Information Systems/Network	• 4. Learn how to maintain
Jackson State Community	CIS	Elective	CIS 156	100	208	Skill in maintaining databases	Database Management	• 4. Learn how to maintain
Jackson State Community	CIS	Elective	CIS 156	100	209	Skill in maintaining directory services	Identity Management	• 4. Learn how to maintain
Jackson State Community	CIS	Elective	CIS 156	100	238	Skill in writing code that is compatible	Computer Languages	• 2. Learn how information

Jackson State Community	CIS	Elective	CIS 156	100	297	Knowledge of industry indicators	Technology Awareness	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	356	Skill in determining installed patches on	Operating Systems	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	360	Skill in identifying and extracting data of	Computer Forensics	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	363	Skill in identifying gaps in technical	Teaching Others	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	364	Skill in identifying, modifying, and	Operating Systems	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	914	Skill in identifying gaps in cyber	Strategic Thinking	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	918	Ability to prepare and deliver education and	Teaching Others	• 3. Understand security policies.
Jackson State Community	CIS	Elective	CIS 156	100	921	Ability to identify possible threat actor	Technology Awareness	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	922	Skill in using network analysis tools to	Vulnerabilities Assessment	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	942	Knowledge of the organization's core	Organizational Awareness	• 2. Learn how information
Jackson State Community	CIS	Elective	CIS 156	100	986	Knowledge of organizational	Identity Management	• 3. Understand security policies.
Jackson State Community	CIS	Elective	CIS 156	100	1008	Knowledge of how to troubleshoot basic	Operating Systems	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	1044	Skill in identifying forensic footprints	Computer Forensics	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	• 4. Learn how to maintain
Jackson State Community	CIS	Elective	CIS 156	100	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	• 4. Learn how to maintain
Jackson State Community	CIS	Elective	CIS 156	100	1100	Skill in identifying obfusification	Computer Network Defense	• 1. Identify the threats posed to
Jackson State Community	CIS	Elective	CIS 156	100	1116	Skill in identifying common encoding	Computer Languages	• 1. Identify the threats posed to
Jackson State Community	A.S	Cyber Defense	CIS250	200	12	Knowledge of communication	Infrastructure Design	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	24	Knowledge of concepts and	Data Management	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	5. Identify and be able to
Jackson State Community	A.S	Cyber Defense	CIS250	200	27	Knowledge of cryptology	Cryptography	5. Identify and be able to
Jackson State Community	A.S	Cyber Defense	CIS250	200	29	Knowledge of data backup, types of	Computer Forensics	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	49	Knowledge of host/network access	Information Systems/Network	1. Be able to recognize and
Jackson State Community	A.S	Cyber Defense	CIS250	200	68	Knowledge of information	Information Technology	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	72	Knowledge of local area network (LAN)	Infrastructure Design	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	77	Knowledege of current industry	Information Systems/Network	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	94	Knowledge of parallel and distributed	Information Technology	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	101	Knowledge of process engineering concepts	Logical Systems Design	4. Understand the security

Jackson State Community	A.S	Cyber Defense	CIS250	200	106	Knowledge of remote access technology	Information Technology	3. Understand the
Jackson State Community	A.S	Cyber Defense	CIS250	200	112	Knowledge of server administration and	Systems Life Cycle	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	122	Knowledge of system administration	Operating Systems	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	127	Knowledge of systems administration	Operating Systems	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	133	Knowledge of telecommunications	Telecommunications	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	157	Skill in applying host/network access	Identity Management	1. Be able to recognize and
Jackson State Community	A.S	Cyber Defense	CIS250	200	261	Knowledge of basic concepts,	Telecommunications	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	274	Knowledge of concepts, principles,	Computer Network Defense	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	281	Knowledge of electronic devices	Hardware	1. Be able to recognize and
Jackson State Community	A.S	Cyber Defense	CIS250	200	284	Knowledge of encryption algorithms	Cryptography	5. Identify and be able to
Jackson State Community	A.S	Cyber Defense	CIS250	200	348	Knowledge of wireless network collection	Cryptography	5. Identify and be able to
Jackson State Community	A.S	Cyber Defense	CIS250	200	355	Skill in creating plans in support of remote	Requirements Analysis	3. Understand the
Jackson State Community	A.S	Cyber Defense	CIS250	200	371	Skill in reading, interpreting, writing,	Operating Systems	3. Understand the
Jackson State Community	A.S	Cyber Defense	CIS250	200	1029	Knowledge of malware analysis	Computer Network Defense	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	1072	Knowledge of network security	Information Systems/Network	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	1087	Skill in deep analysis of captured malicious	Computer Network Defense	2. Recognize various types of
Jackson State Community	A.S	Cyber Defense	CIS250	200	1089	Knowledge of reverse engineering concepts	Vulnerabilities Assessment	4. Understand the security
Jackson State Community	A.S	Cyber Defense	CIS250	200	1098	Skill in analyzing anomalous code as	Computer Network Defense	2. Recognize various types of
Jackson State Community	A.S	Cyber Defense	CIS250	200	1114	Knowledge of encryption	Cryptography	5. Identify and be able to
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	29	Knowledge of data backup, types of	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	33	Knowledge of database procedures	Incident Management	• 3. Processing Crime and
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	37	Knowledge of disaster recovery and	Incident Management	• 3. Processing Crime and
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	60	Knowledge of incident categories, incident	Incident Management	• 3. Processing Crime and
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	61	Knowledge of incident response and	Incident Management	• 3. Processing Crime and
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	114	Knowledge of server diagnostic tools and	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	216	Skill in recovering failed servers	Incident Management	• 3. Processing Crime and
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	217	Skill in preserving evidence integrity	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	229	Skill in using incident handling	Incident Management	• 3. Processing Crime and
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	252	Knowledge of and experience in Insider	Computer Network Defense	• 1. Understanding
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	290	Knowledge of processes for seizing	Forensics	• 4. Current Computer

Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	302	Knowledge of investigative	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	305	Knowledge of laws that affect cyber	Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	325	Knowledge of secure acquisitions (e.g.,	Contracting/Procurement	• 2. Data Acquisition
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	340	Knowledge of types and collection of	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	346	Knowledge of which system files (e.g. log	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	359	Skill in developing and executing technical	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	360	Skill in identifying and extracting data of	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	369	Skill in collecting, processing,	Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	374	Skill in setting up a forensic workstation	Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	379	Skill in using common digital forensics tools	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	381	Skill in using forensic tool suites (e.g.	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	888	Knowledge of types of digital forensics data	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	889	Knowledge of deployable forensics	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	890	Skill in conducting forensic analyses in	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	901	Knowledge of the capabilities of	Network Management	• 7. Email Investigations • 9.
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	908	Ability to decrypt digital data collections	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	966	Knowledge of enterprise incident	Incident Management	• 3. Processing Crime and
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	978	Knowledge of root cause analysis for	Incident Management	• 3. Processing Crime and
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	980	Skill in performing root cause analysis for	Incident Management	• 3. Processing Crime and
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	1011	Knowledge of processes for	Security	• 3. Processing Crime and
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	1044	Skill in identifying forensic footprints	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	1086	Knowledge of data carving tools and	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	1087	Skill in deep analysis of captured malicious	Computer Network Defense	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	1092	Knowledge of antiforensics tactics,	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	1093	Knowledge of common forensic tool	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS251	200	1099	Skill in analyzing volatile data	Computer Forensics	• 4. Current Computer
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	5	Ability to match the appropriate	Knowledge Management	9. Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	7	Knowledge of “knowledge base”	Knowledge Management	9. Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	12	Knowledge of communication	Infrastructure Design	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	15	Knowledge of capabilities and	Hardware	1. Explain the concepts of a

Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	19	Knowledge of Computer Network	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	22	Knowledge of computer networking	Infrastructure Design	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	24	Knowledge of concepts and	Data Management	3. Examine the implementation
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	2.) Examine concepts of
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	27	Knowledge of cryptology	Cryptography	2.) Examine concepts of
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	28	Knowledge of data administration and	Data Management	9. Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	31	Knowledge of data mining and data	Data Management	9. Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	32	Knowledge of database	Database Management	9. Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	33	Knowledge of database procedures	Incident Management	9. Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	34	Knowledge of database systems	Database Management	9. Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	35	Knowledge of digital rights management	Encryption	3.) Examine the implementation
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	37	Knowledge of disaster recovery and	Incident Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	41	Knowledge of organization's Local	Infrastructure Design	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	49	Knowledge of host/network access	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	50	Knowledge of how network services and	Infrastructure Design	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	55	Knowledge of Information	Information Assurance	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	58	Knowledge of known vulnerabilities from	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	59	Knowledge of Intrusion Detection	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	60	Knowledge of incident categories, incident	Incident Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	61	Knowledge of incident response and	Incident Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	64	Knowledge of information security	Information Systems/ Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	66	Knowledge of intrusion detection	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	69	Knowledge of Risk Management	Information Systems Security	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	70	Knowledge of information	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	72	Knowledge of local area network (LAN)	Infrastructure Design	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	77	Knowledege of current industry	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	79	Knowledge of network access,	Identity Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	81	Knowledge of network	Infrastructure Design	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	82	Knowledge of network design	Infrastructure Design	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	83	Knowledge of network hardware	Hardware	1. Explain the concepts of a

Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	87	Knowledge of network traffic	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	92	Knowledge of how traffic flows across	Infrastructure Design	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	98	Knowledge of policybased and risk	Identity Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	104	Knowledge of query languages such as	Database Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	107	Knowledge of resource	Project Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	108	Knowledge of risk management	Risk Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	109	Knowledge of secure configuration	Configuration Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	110	Knowledge of security management	Information Assurance	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	111	Knowledge of security system design tools,	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	115	Knowledge of content development	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	120	Knowledge of sources,	Data Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	122	Knowledge of system administration	Operating Systems	8. Create a Linux certificate
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	129	Knowledge of systems lifecycle management	Systems Life Cycle	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	134	Knowledge of the capabilities and	Technology Awareness	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	135	Knowledge of the capabilities and	Data Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	137	Knowledge of the characteristics of	Data Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	138	Knowledge of the computer network	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	139	Knowledge of common networking	Infrastructure Design	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	146	Knowledge of the types of Intrusion	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	150	Knowledge of what constitutes a network	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	152	Skill in allocating storage capacity in	Database Administration	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	153	Skill in handling malware	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	154	Skill in analyzing network traffic	Capacity Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	157	Skill in applying host/network access	Identity Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	164	Skill in conducting knowledge mapping	Knowledge Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	165	Skill in conducting open source research	Knowledge Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	166	Skill in conducting queries and	Database Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	167	Skill in conducting server planning,	Network Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	171	Skill in correcting physical and technical	Network Management	1. Explain the concepts of a

Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	175	Skill in developing and deploying signatures	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	181	Skill in detecting host and network based	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	186	Skill in developing data dictionaries	Data Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	188	Skill in developing data repositories	Data Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	191	Skill in developing and applying security	Identity Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	193	Skill in developing, testing, and	Information Assurance	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	194	Skill in diagnosing connectivity problems	Network Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	195	Skill in diagnosing failed servers	Network Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	201	Skill in generating queries and reports	Database Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	205	Skill in implementing, maintaining, and	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	207	Skill in installing, configuring, and		1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	208	Skill in maintaining databases	Database Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	209	Skill in maintaining directory services	Identity Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	210	Skill in mimicking threat behaviors	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	212	Skill in network mapping and	Infrastructure Design	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	216	Skill in recovering failed servers	Incident Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	219	Skill in system administration for	Operating Systems	8. Create a Linux certificate
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	221	Skill in testing and configuring network	Network Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	223	Skill in the measuring and reporting of	Knowledge Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	227	Skill in tuning sensors	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	229	Skill in using incident handling	Incident Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	230	Skill in using knowledge	Knowledge Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	231	Skill in using network management tools to	Network Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	252	Knowledge of and experience in Insider	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	261	Knowledge of basic concepts,	Telecommunicatio ns	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	264	Knowledge of basic physical computer	Computers and Electronics	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	269	Knowledge of CNE/CNA/CNO	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	270	Knowledge of common adversary	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	271	Knowledge of common network	Infrastructure Design	1. Explain the concepts of a

Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	274	Knowledge of concepts, principles,	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	277	Knowledge of defense indepth principles and	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	278	Knowledge of different types of	Telecommunications	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	281	Knowledge of electronic devices	Hardware	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	284	Knowledge of encryption algorithms	Cryptography	2.) Examine concepts of
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	290	Knowledge of processes for seizing	Forensics	3.) Examine the implementation
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	294	Knowledge of hacking methodologies in	Surveillance	8. Create a Linux certificate
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	299	Knowledge of information security	Project Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	302	Knowledge of investigative	Computer Forensics	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	313	Knowledge of logging services for network	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	325	Knowledge of secure acquisitions (e.g.,	Contracting/Procurement	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	326	Knowledge of security hardware and	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	341	Knowledge of UNIX and Windows systems	Operating Systems	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	348	Knowledge of wireless network collection	Cryptography	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	349	Skill in analyzing data from a variety of	Reasoning	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	353	Skill in collecting data from a variety of	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	357	Skill in determining the effects of various	Configuration Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	364	Skill in identifying, modifying, and	Operating Systems	8. Create a Linux certificate
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	375	Skill in survey, collection, and	Network Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	379	Skill in using common digital forensics tools	Computer Forensics	3.) Examine the implementation
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	385	Skill in using traceroute analysis	Network Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	886	Skill in wireless network target	Vulnerabilities Assessment	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	888	Knowledge of types of digital forensics data	Computer Forensics	3.) Examine the implementation
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	891	Skill in configuring and utilizing	Configuration Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	892	Skill in configuring and utilizing	Configuration Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	893	Skill in securing network	Information Assurance	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	896	Skill in protecting a network against	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	899	Skill in gathering information from	Information Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	901	Knowledge of the capabilities of	Network Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	902	Knowledge of the range of existing	Network Management	1. Explain the concepts of a

Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	903	Knowledge of Wireless Fidelity	Network Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	905	Knowledge of secure coding techniques	Computer Languages	11.) Secure email
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	907	Skill in data mining techniques	Data Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	908	Ability to decrypt digital data collections	Computer Forensics	3.) Examine the implementation
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	910	Knowledge of database theory	Data Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	912	Knowledge of collection	Configuration Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	913	Knowledge of how passive and active	Information Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	915	Knowledge of frontend collection	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	918	Ability to prepare and deliver education and	Teaching Others	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	922	Skill in using network analysis tools to	Vulnerabilities Assessment	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	923	Knowledge of security event correlation	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	965	Knowledge of organization's risk	Risk Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	966	Knowledge of enterprise incident	Incident Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	967	Knowledge of current and emerging	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	968	Knowledge of softwarerelated	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	978	Knowledge of root cause analysis for	Incident Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	979	Knowledge of supply chain risk	Risk Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	980	Skill in performing root cause analysis for	Incident Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	984	Knowledge of computer network	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	985	Skill in configuring and utilizing network	Configuration Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	986	Knowledge of organizational	Identity Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	990	Knowledge of common attack	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	991	Knowledge of different classes of	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	992	Knowledge of different operational	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1007	Skills in data reduction	Data Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1011	Knowledge of processes for	Security	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1020	Skill in secure test plan deisn (i.e., unit,	Systems Testing and Evaluation	11.) Secure email
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1021	Knowledge of threat assessment	Risk Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1029	Knowledge of malware analysis	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1033	Knowledge of basic system	Information Systems/Network	1. Explain the concepts of a

Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1037	Knowledge of information	Risk Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1038	Knowledge of local specialized system	Infrastructure Design	10.) Secure local resources
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1042	Abililty to apply network	Requirements Analysis	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1059	Knowledge of networking protocols	Infrastructure Design	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1063	Knowledge of Unix/Linux operating	Operating Systems	8. Create a Linux certificate
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1071	Knowledge of secure software deployment	Software Engineering	11.) Secure email
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1072	Knowledge of network security	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1073	Knowledge of network systems	Network Management	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1074	Knowledge of transmission records	Telecommunicatio ns	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1087	Skill in deep analysis of captured malicious	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1091	Skill in one way hash functions (e.g., Secure	Data Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1096	Knowledge of malware analysis	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1097	Knowledge of virtual machine aware	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1098	Skill in analyzing anomalous code as	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1100	Skill in identifying obfusification	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1101	Skill in interpreting results of debugger to	Computer Network Defense	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1114	Knowledge of encryption	Cryptography	2.) Examine concepts of
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1117	Skill in utilizing virtual networks for testing	Operating Systems	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1118	Skill in reading and interpreting	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1119	Knowledge of signature	Information Systems/Network	1. Explain the concepts of a
Jackson State Community	A.S	Cyber Defense, Networking,	CIS257	200	1120	Ability to interpret and incorporate data	Data Management	9.) Manage certificates
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	38	Knowledge of organization's	Information Assurance	F1A1. Define and outline
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	55	Knowledge of Information	Information Assurance	F1A12. Define and describe
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	63	Knowledge of Information	Information Assurance	F1A12. Define and describe
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	69	Knowledge of Risk Management	Information Systems Security	F1B1 Describe the dominant
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	70	Knowledge of information	Information Systems/Network	F1B1 Describe the dominant
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	77	Knowledge of current industry methods for	Information Systems/Network	F1A15. Define magnetic media

Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	111	Knowledge of security system design tools,	Information Systems/Network	F1A18. Discuss the phases of the
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	141	Knowledge of the enterprise	Information Technology	F1A3. Describe the dominant
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	143	Knowledge of the organization's	Enterprise Architecture	F1A11. Define generally
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	156	Skill in applying confidentiality,	Information Assurance	F1A12. Define and describe
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	179	Skill in designing security controls	Information Assurance	F1A12. Define and describe
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	191	Skill in developing and applying security	Identity Management	F1B2 Explain why access control is
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	221	Skill in testing and configuring network	Network Management	F1A19. Describe workstation
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	277	Knowledge of defense indepth principles and	Computer Network Defense	F1A8. Define defense in depth
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	942	Knowledge of the organization's core	Organizational Awareness	F1A1. Define and outline
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	986	Knowledge of organizational	Identity Management	F1A1. Define and outline
Jackson State Community	A.S	Cyber Defense, Networking,	CIS 259	200	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	F1A2. Define and Discuss emerging
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	15	Knowledge of capabilities and	Hardware	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	22	Knowledge of computer networking	Infrastructure Design	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	50	Knowledge of how network services and	Infrastructure Design	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	70	Knowledge of information	Information Systems/Network	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	83	Knowledge of network hardware	Hardware	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	92	Knowledge of how traffic flows across	Infrastructure Design	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	205	Skill in implementing, maintaining, and	Information Systems/Network	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	226	Skill in the use of social engineering	Human Factors	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	278	Knowledge of different types of	Telecommunicatio ns	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	327	Knowledge of security implications of	Information Assurance	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	356	Skill in determining installed patches on	Operating Systems	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	387	Skill in verifying the integrity of encrypted	Encryption	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	892	Skill in configuring and utilizing	Configuration Management	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	893	Skill in securing network	Information Assurance	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	895	Skill in recognizing and categorizing	Information Assurance	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	896	Skill in protecting a network against	Computer Network Defense	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	903	Knowledge of Wireless Fidelity	Network Management	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	1029	Knowledge of malware analysis	Computer Network Defense	To introduce students to the
Manhattan Area Technical	A.S	Information and Network	CRT 100	100	1114	Knowledge of encryption	Cryptography	To introduce students to the

Manhattan Area Technical	A.S	Information and Network	CRT 282	200	8	Knowledge of access authentication	Identity Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	63	Knowledge of Information	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	70	Knowledge of information	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	77	Knowledege of current industry	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	82	Knowledge of network design	Infrastructure Design	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	83	Knowledge of network hardware	Hardware	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	98	Knowledge of policybased and risk	Identity Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	123	Knowledge of system and application	Vulnerabilities Assessment	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	156	Skill in applying confidentiality,	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	157	Skill in applying host/network access	Identity Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	173	Skill in creating policies that relfect	Information Systems Security	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	191	Skill in developing and applying security	Identity Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	237	Skill in using Virtual Private Network	Encryption	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	321	Knowledge of products and	Technology Awareness	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	891	Skill in configuring and utilizing	Configuration Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	895	Skill in recognizing and categorizing	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	967	Knowledge of current and emerging	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	985	Skill in configuring and utilizing network	Configuration Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	986	Knowledge of organizational	Identity Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	990	Knowledge of common attack	Computer Network Defense	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 282	200	1021	Knowledge of threat assessment	Risk Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	4	Ability to identify systemic security	Vulnerabilities Assessment	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	8	Knowledge of access authentication	Identity Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	10	Knowledge of application	Vulnerabilities Assessment	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	19	Knowledge of Computer Network	Computer Network Defense	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	24	Knowledge of concepts and	Data Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	This course is intended to

Manhattan Area Technical	A.S	Information and Network	CRT 289	200	27	Knowledge of cryptology	Cryptography	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	31	Knowledge of data mining and data	Data Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	35	Knowledge of digital rights management	Encryption	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	37	Knowledge of disaster recovery and	Incident Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	38	Knowledge of organization's	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	49	Knowledge of host/network access	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	55	Knowledge of Information	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	58	Knowledge of known vulnerabilities from	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	59	Knowledge of Intrusion Detection	Computer Network Defense	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	63	Knowledge of Information	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	66	Knowledge of intrusion detection	Computer Network Defense	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	69	Knowledge of Risk Management	Information Systems Security	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	70	Knowledge of information	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	77	Knowledege of current industry	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	82	Knowledge of network design	Infrastructure Design	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	87	Knowledge of network traffic	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	88	Knowledge of new and emerging	Technology Awareness	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	93	Knowledge of packetlevel analysis	Vulnerabilities Assessment	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	98	Knowledge of policybased and risk	Identity Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	108	Knowledge of risk management	Risk Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	109	Knowledge of secure configuration	Configuration Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	110	Knowledge of security management	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	111	Knowledge of security system design tools,	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	123	Knowledge of system and application	Vulnerabilities Assessment	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	129	Knowledge of systems lifecycle management	Systems Life Cycle	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	146	Knowledge of the types of Intrusion	Computer Network Defense	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	148	Knowledge of VPN security.	Encryption	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	150	Knowledge of what constitutes a network	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	153	Skill in handling malware	Computer Network Defense	This course is intended to

Manhattan Area Technical	A.S	Information and Network	CRT 289	200	156	Skill in applying confidentiality,	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	157	Skill in applying host/network access	Identity Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	173	Skill in creating policies that relfect	Information Systems Security	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	175	Skill in developing and deploying signatures	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	179	Skill in designing security controls	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	181	Skill in detecting host and network based	Computer Network Defense	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	183	Skill in determining how a security system	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	191	Skill in developing and applying security	Identity Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	193	Skill in developing, testing, and	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	217	Skill in preserving evidence integrity	Computer Forensics	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	226	Skill in the use of social engineering	Human Factors	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	233	Skill in using protocol analyzers	Vulnerabilities Assessment	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	237	Skill in using Virtual Private Network	Encryption	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	264	Knowledge of basic physical computer	Computers and Electronics	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	277	Knowledge of defense indepth principles and	Computer Network Defense	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	290	Knowledge of processes for seizing	Forensics	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	294	Knowledge of hacking methodologies in	Surveillance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	299	Knowledge of information security	Project Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	310	Knowledge of legal governance related to	Criminal Law	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	316	Knowledge of processes for	Criminal Law	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	321	Knowledge of products and	Technology Awareness	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	327	Knowledge of security implications of	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	349	Skill in analyzing data from a variety of	Reasoning	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	This course is intended to

Manhattan Area Technical	A.S	Information and Network	CRT 289	200	387	Skill in verifying the integrity of encrypted	Encryption	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	888	Knowledge of types of digital forensics data	Computer Forensics	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	891	Skill in configuring and utilizing	Configuration Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	892	Skill in configuring and utilizing	Configuration Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	893	Skill in securing network	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	895	Skill in recognizing and categorizing	Information Assurance	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	896	Skill in protecting a network against	Computer Network Defense	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	907	Skill in data mining techniques	Data Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	915	Knowledge of frontend collection	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	918	Ability to prepare and deliver education and	Teaching Others	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	922	Skill in using network analysis tools to	Vulnerabilities Assessment	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	952	Knowledge of emerging security	Technology Awareness	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	967	Knowledge of current and emerging	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	968	Knowledge of softwarerelated	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	982	Knowledge of electronic evidence	Criminal Law	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	985	Skill in configuring and utilizing network	Configuration Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	986	Knowledge of organizational	Identity Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	989	Knowledge of Voice over Internet Protocol	Telecommunicatio ns	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	990	Knowledge of common attack	Computer Network Defense	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	992	Knowledge of different operational	Computer Network Defense	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	993	Knowledge of the methods, standards,	Enterprise Architecture	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	1011	Knowledge of processes for	Security	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	1020	Skill in secure test plan deisn (i.e., unit,	Systems Testing and Evaluation	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	1021	Knowledge of threat assessment	Risk Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	1037	Knowledge of information	Risk Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	1072	Knowledge of network security	Information Systems/Network	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	1073	Knowledge of network systems	Network Management	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	1114	Knowledge of encryption	Cryptography	This course is intended to
Manhattan Area Technical	A.S	Information and Network	CRT 289	200	1118	Skill in reading and interpreting	Information Systems/Network	This course is intended to
Montgomery College	A.S	Information and Network	MG 288	200	37	Knowledge of disaster recovery and	Incident Management	(4) Identify steps required for

Montgomery College	A.S	Information and Network	MG 288	200	108	Knowledge of risk management	Risk Management	(3) Explain the implementation
Montgomery College	A.S	Information and Network	MG 288	200	965	Knowledge of organization's risk	Risk Management	(1) Describe and discuss the
Montgomery College	A.S	Information and Network	MG 288	200	979	Knowledge of supply chain risk	Risk Management	(1) Describe and discuss the
Montgomery College	A.S	Information and Network	MG 288	200	1021	Knowledge of threat assessment	Risk Management	(1) Describe and discuss the
Montgomery College	A.S	Information and Network	MG 288	200	1037	Knowledge of information	Risk Management	(3) Explain the implementation
Montgomery College	A.S	Information and Network	NW 173	100	8	Knowledge of access authentication	Identity Management	2. Describe authentication
Montgomery College	A.S	Information and Network	NW 173	100	15	Knowledge of capabilities and	Hardware	10. Identify firewalls, drafting
Montgomery College	A.S	Information and Network	NW 173	100	63	Knowledge of Information	Information Assurance	2. Describe authentication
Montgomery College	A.S	Information and Network	NW 173	100	70	Knowledge of information	Information Systems/Network	10. Identify firewalls, drafting
Montgomery College	A.S	Information and Network	NW 173	100	106	Knowledge of remote access technology	Information Technology	4. Describe remote access,
Montgomery College	A.S	Information and Network	NW 173	100	123	Knowledge of system and application	Vulnerabilities Assessment	7. Describe security threats,
Montgomery College	A.S	Information and Network	NW 173	100	139	Knowledge of common networking	Infrastructure Design	5. Describe securing Email
Montgomery College	A.S	Information and Network	NW 173	100	150	Knowledge of what constitutes a network	Information Systems/Network	1. Describe attacks and
Montgomery College	A.S	Information and Network	NW 173	100	156	Skill in applying confidentiality,	Information Assurance	7. Describe security threats,
Montgomery College	A.S	Information and Network	NW 173	100	209	Skill in maintaining directory services	Identity Management	3. Describe directory and file
Montgomery College	A.S	Information and Network	NW 173	100	237	Skill in using Virtual Private Network	Encryption	4. Describe remote access,
Montgomery College	A.S	Information and Network	NW 173	100	284	Knowledge of encryption algorithms	Cryptography	5. Describe securing Email
Montgomery College	A.S	Information and Network	NW 173	100	322	Knowledge of router and routing	Infrastructure Design	10. Identify firewalls, drafting
Montgomery College	A.S	Information and Network	NW 173	100	891	Skill in configuring and utilizing	Configuration Management	10. Identify firewalls, drafting
Montgomery College	A.S	Information and Network	NW 173	100	895	Skill in recognizing and categorizing	Information Assurance	1. Describe attacks and
Montgomery College	A.S	Information and Network	NW 173	100	901	Knowledge of the capabilities of	Network Management	9. Describe wireless and
Montgomery College	A.S	Information and Network	NW 173	100	985	Skill in configuring and utilizing network	Configuration Management	10. Identify firewalls, drafting
Montgomery College	A.S	Information and Network	NW 173	100	986	Knowledge of organizational	Identity Management	2. Describe authentication
Montgomery College	A.S	Information and Network	NW 173	100	991	Knowledge of different classes of	Computer Network Defense	1. Describe attacks and
Montgomery College	A.S	Information and Network	NW 245	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	8. Work with the secure version of
Montgomery College	A.S	Information and Network	NW 245	200	29	Knowledge of data backup, types of	Computer Forensics	4. Investigate measures that
Montgomery College	A.S	Information and Network	NW 245	200	37	Knowledge of disaster recovery and	Incident Management	4. Investigate measures that
Montgomery College	A.S	Information and Network	NW 245	200	81	Knowledge of network	Infrastructure Design	3. Investigate advanced
Montgomery College	A.S	Information and Network	NW 245	200	92	Knowledge of how traffic flows across	Infrastructure Design	3. Investigate advanced
Montgomery College	A.S	Information and Network	NW 245	200	122	Knowledge of system administration	Operating Systems	5. Secure Linux computers and

Montgomery College	A.S	Information and Network	NW 245	200	139	Knowledge of common networking	Infrastructure Design	3. Investigate advanced
Montgomery College	A.S	Information and Network	NW 245	200	193	Skill in developing, testing, and	Information Assurance	4. Investigate measures that
Montgomery College	A.S	Information and Network	NW 245	200	219	Skill in system administration for	Operating Systems	5. Secure Linux computers and
Montgomery College	A.S	Information and Network	NW 245	200	294	Knowledge of hacking methodologies in	Surveillance	1. Define common Internet
Montgomery College	A.S	Information and Network	NW 245	200	322	Knowledge of router and routing	Infrastructure Design	6. Secure routers by using access
Montgomery College	A.S	Information and Network	NW 245	200	364	Skill in identifying, modifying, and	Operating Systems	5. Secure Linux computers and
Montgomery College	A.S	Information and Network	NW 245	200	991	Knowledge of different classes of	Computer Network Defense	1. Define common Internet
Montgomery College	A.S	Information and Network	NW 245	200	1063	Knowledge of Unix/Linux operating	Operating Systems	5. Secure Linux computers and
Montgomery College	A.S	Information and Network	NW 245	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	1. Define common Internet
Montgomery College	A.S	Information and Network	NW 245	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	2. Examine and work with
Montgomery College	A.S	Information and Network	NW 245	200	1121	Knowledge of Windows/Unix ports	Operating Systems	7. Secure workstations and
Montgomery College	A.S	Information and Network	NW 246	200	49	Knowledge of host/network access	Information Systems/Network	7. Identify the basic components
Montgomery College	A.S	Information and Network	NW 246	200	66	Knowledge of intrusion detection	Computer Network Defense	4. Describe the key concepts of
Montgomery College	A.S	Information and Network	NW 246	200	70	Knowledge of information	Information Systems/Network	6. Identify key concepts and
Montgomery College	A.S	Information and Network	NW 246	200	79	Knowledge of network access,	Identity Management	7. Identify the basic components
Montgomery College	A.S	Information and Network	NW 246	200	93	Knowledge of packetlevel analysis	Vulnerabilities Assessment	2. Describe core concepts of
Montgomery College	A.S	Information and Network	NW 246	200	108	Knowledge of risk management	Risk Management	3. Describe the concepts and
Montgomery College	A.S	Information and Network	NW 246	200	146	Knowledge of the types of Intrusion	Computer Network Defense	8. Implement and configure a
Montgomery College	A.S	Information and Network	NW 246	200	148	Knowledge of VPN security.	Encryption	5. Describe virtual private
Montgomery College	A.S	Information and Network	NW 246	200	891	Skill in configuring and utilizing	Configuration Management	9. Implement and configure
Montgomery College	A.S	Information and Network	NW 246	200	985	Skill in configuring and utilizing network	Configuration Management	8. Implement and configure a
Montgomery College	A.S	Information and Network	NW 246	200	986	Knowledge of organizational	Identity Management	1. Configure and implement
Montgomery College	A.S	Information and Network	NW 261	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	4	Ability to identify systemic security	Vulnerabilities Assessment	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	8	Knowledge of access authentication	Identity Management	1.) Configure and manage Cisco
Montgomery College	A.S	Information and Network	NW 261	200	10	Knowledge of application	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	17	Knowledge of certified ethical	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	38	Knowledge of organization's	Information Assurance	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	49	Knowledge of host/network access	Information Systems/Network	1.) Configure and manage Cisco
Montgomery College	A.S	Information and Network	NW 261	200	50	Knowledge of how network services and	Infrastructure Design	• 11. Manage Layer 2 security

Montgomery College	A.S	Information and Network	NW 261	200	53	Knowledge of the Security Assessment	Information Assurance	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	58	Knowledge of known vulnerabilities from	Information Systems/Network	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	64	Knowledge of information security	Information Systems/ Network	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	69	Knowledge of Risk Management	Information Systems Security	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	70	Knowledge of information	Information Systems/Network	• 2. Configure, monitor, and
Montgomery College	A.S	Information and Network	NW 261	200	77	Knowledege of current industry	Information Systems/Network	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	79	Knowledge of network access,	Identity Management	1.) Configure and manage Cisco
Montgomery College	A.S	Information and Network	NW 261	200	81	Knowledge of network	Infrastructure Design	• 11. Manage Layer 2 security
Montgomery College	A.S	Information and Network	NW 261	200	82	Knowledge of network design	Infrastructure Design	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	87	Knowledge of network traffic	Information Systems/Network	• 6. Design and manage a
Montgomery College	A.S	Information and Network	NW 261	200	88	Knowledge of new and emerging	Technology Awareness	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	93	Knowledge of packetlevel analysis	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	98	Knowledge of policybased and risk	Identity Management	1.) Configure and manage Cisco
Montgomery College	A.S	Information and Network	NW 261	200	100	Knowledge of Privacy Impact Assessments	Personnel Safety and Security	• 6. Design and manage a
Montgomery College	A.S	Information and Network	NW 261	200	106	Knowledge of remote access technology	Information Technology	1.) Configure and manage Cisco
Montgomery College	A.S	Information and Network	NW 261	200	110	Knowledge of security management	Information Assurance	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	111	Knowledge of security system design tools,	Information Systems/Network	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	123	Knowledge of system and application	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	129	Knowledge of systems lifecycle management	Systems Life Cycle	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	138	Knowledge of the computer network	Information Systems/Network	• 6. Design and manage a
Montgomery College	A.S	Information and Network	NW 261	200	139	Knowledge of common networking	Infrastructure Design	• 11. Manage Layer 2 security
Montgomery College	A.S	Information and Network	NW 261	200	148	Knowledge of VPN security.	Encryption	• 6. Design and manage a
Montgomery College	A.S	Information and Network	NW 261	200	149	Knowledge of web services, including	Web Technology	1.) Configure and manage Cisco
Montgomery College	A.S	Information and Network	NW 261	200	150	Knowledge of what constitutes a network	Information Systems/Network	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	154	Skill in analyzing network traffic	Capacity Management	7. Engineer filtering of
Montgomery College	A.S	Information and Network	NW 261	200	157	Skill in applying host/network access	Identity Management	1.) Configure and manage Cisco
Montgomery College	A.S	Information and Network	NW 261	200	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	173	Skill in creating policies that relfect	Information Systems Security	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	175	Skill in developing and deploying signatures	Information Systems/Network	• 6. Design and manage a

Montgomery College	A.S	Information and Network	NW 261	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	179	Skill in designing security controls	Information Assurance	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	183	Skill in determining how a security system	Information Assurance	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	191	Skill in developing and applying security	Identity Management	1.) Configure and manage Cisco
Montgomery College	A.S	Information and Network	NW 261	200	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	205	Skill in implementing, maintaining, and	Information Systems/Network	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	209	Skill in maintaining directory services	Identity Management	• 5. Design and implement trust
Montgomery College	A.S	Information and Network	NW 261	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	231	Skill in using network management tools to	Network Management	7. Engineer filtering of
Montgomery College	A.S	Information and Network	NW 261	200	233	Skill in using protocol analyzers	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	277	Knowledge of defense indepth principles and	Computer Network Defense	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	281	Knowledge of electronic devices	Hardware	1.) Configure and manage Cisco
Montgomery College	A.S	Information and Network	NW 261	200	299	Knowledge of information security	Project Management	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	305	Knowledge of laws that affect cyber	Forensics	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	313	Knowledge of logging services for network	Information Systems/Network	• 6. Design and manage a
Montgomery College	A.S	Information and Network	NW 261	200	320	Knowledge of external organizations	External Awareness	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	321	Knowledge of products and	Technology Awareness	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	326	Knowledge of security hardware and	Information Systems/Network	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	327	Knowledge of security implications of	Information Assurance	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	341	Knowledge of UNIX and Windows systems	Operating Systems	• 2. Configure, monitor, and
Montgomery College	A.S	Information and Network	NW 261	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	886	Skill in wireless network target	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	891	Skill in configuring and utilizing	Configuration Management	• 2. Configure, monitor, and
Montgomery College	A.S	Information and Network	NW 261	200	892	Skill in configuring and utilizing	Configuration Management	• 2. Configure, monitor, and
Montgomery College	A.S	Information and Network	NW 261	200	895	Skill in recognizing and categorizing	Information Assurance	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	915	Knowledge of frontend collection	Information Systems/Network	• 6. Design and manage a
Montgomery College	A.S	Information and Network	NW 261	200	918	Ability to prepare and deliver education and	Teaching Others	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	922	Skill in using network analysis tools to	Vulnerabilities Assessment	• 3. Describe basic security

Montgomery College	A.S	Information and Network	NW 261	200	923	Knowledge of security event correlation	Information Systems/Network	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	952	Knowledge of emerging security	Technology Awareness	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	968	Knowledge of softwarerelated	Information Systems/Network	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	975	Skill in integrating black box security	Quality Assurance	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	981	Knowledge of International Traffic in	Criminal Law	• 6. Design and manage a
Montgomery College	A.S	Information and Network	NW 261	200	985	Skill in configuring and utilizing network	Configuration Management	• 2. Configure, monitor, and
Montgomery College	A.S	Information and Network	NW 261	200	986	Knowledge of organizational	Identity Management	1.) Configure and manage Cisco
Montgomery College	A.S	Information and Network	NW 261	200	1005	Knowledge of functionality, quality,	Contracting/Procurement	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	1011	Knowledge of processes for	Security	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	1033	Knowledge of basic system	Information Systems/Network	• 6. Design and manage a
Montgomery College	A.S	Information and Network	NW 261	200	1034	Knowledge of Personally Identifiable	Security	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	1037	Knowledge of information	Risk Management	• 6. Design and manage a
Montgomery College	A.S	Information and Network	NW 261	200	1054	Knowledge of hardware reverse	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	1056	Knowledge of operations security	Public Safety and Security	• 6. Design and manage a
Montgomery College	A.S	Information and Network	NW 261	200	1062	Knowledge of software reverse	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	1.) Configure and manage Cisco
Montgomery College	A.S	Information and Network	NW 261	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	1.) Configure and manage Cisco
Montgomery College	A.S	Information and Network	NW 261	200	1072	Knowledge of network security	Information Systems/Network	• 4. Describe security
Montgomery College	A.S	Information and Network	NW 261	200	1089	Knowledge of reverse engineering concepts	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	1095	Knowledge of how different file types can	Vulnerabilities Assessment	• 3. Describe basic security
Montgomery College	A.S	Information and Network	NW 261	200	1118	Skill in reading and interpreting	Information Systems/Network	• 6. Design and manage a
Montgomery College	A.S	Information and Network	NW 261	200	1119	Knowledge of signature	Information Systems/Network	• 6. Design and manage a
Montgomery College	A.S	Information and Network	NW 261	200	1121	Knowledge of Windows/Unix ports	Operating Systems	• 11. Manage Layer 2 security
Montgomery College	A.S	Information and Network	NW 263	200	29	Knowledge of data backup, types of	Computer Forensics	(2) Make use of current forensics
Montgomery College	A.S	Information and Network	NW 263	200	114	Knowledge of server diagnostic tools and	Computer Forensics	(2) Make use of current forensics
Montgomery College	A.S	Information and Network	NW 263	200	217	Skill in preserving evidence integrity	Computer Forensics	(3) Perform computer
Montgomery College	A.S	Information and Network	NW 263	200	290	Knowledge of processes for seizing	Forensics	(2) Make use of current computer
Montgomery College	A.S	Information and Network	NW 263	200	302	Knowledge of investigative	Computer Forensics	(1) Handle cell phone and

Montgomery College	A.S	Information and Network	NW 263	200	305	Knowledge of laws that affect cyber	Forensics	?
Montgomery College	A.S	Information and Network	NW 263	200	340	Knowledge of types and collection of	Computer Forensics	(1) Handle cell phone and
Montgomery College	A.S	Information and Network	NW 263	200	346	Knowledge of which system files (e.g. log	Computer Forensics	(2) Make use of current computer
Montgomery College	A.S	Information and Network	NW 263	200	359	Skill in developing and executing technical	Computer Forensics	(2) Make use of current computer
Montgomery College	A.S	Information and Network	NW 263	200	360	Skill in identifying and extracting data of	Computer Forensics	(1) Handle cell phone and
Montgomery College	A.S	Information and Network	NW 263	200	369	Skill in collecting, processing,	Forensics	(3) Perform computer
Montgomery College	A.S	Information and Network	NW 263	200	374	Skill in setting up a forensic workstation	Forensics	(2) Make use of current computer
Montgomery College	A.S	Information and Network	NW 263	200	379	Skill in using common digital forensics tools	Computer Forensics	(1) Handle cell phone and
Montgomery College	A.S	Information and Network	NW 263	200	381	Skill in using forensic tool suites (e.g.	Computer Forensics	(2) Make use of current forensics
Montgomery College	A.S	Information and Network	NW 263	200	888	Knowledge of types of digital forensics data	Computer Forensics	(4) Perform email investigation. (7)
Montgomery College	A.S	Information and Network	NW 263	200	889	Knowledge of deployable forensics	Computer Forensics	(1) Handle cell phone and
Montgomery College	A.S	Information and Network	NW 263	200	890	Skill in conducting forensic analyses in	Computer Forensics	(1) Handle cell phones and
Montgomery College	A.S	Information and Network	NW 263	200	901	Knowledge of the capabilities of	Network Management	.
Montgomery College	A.S	Information and Network	NW 263	200	908	Ability to decrypt digital data collections	Computer Forensics	Make use of current computer
Montgomery College	A.S	Information and Network	NW 263	200	985	Skill in configuring and utilizing network	Configuration Management	.
Montgomery College	A.S	Information and Network	NW 263	200	1044	Skill in identifying forensic footprints	Computer Forensics	(3) Perform computer
Montgomery College	A.S	Information and Network	NW 263	200	1092	Knowledge of antiforensics tactics,	Computer Forensics	(2) Make use of current computer
Montgomery College	A.S	Information and Network	NW 263	200	1093	Knowledge of common forensic tool	Computer Forensics	(2) Make use of current computer
Montgomery College	A.S	Information and Network	NW 263	200	1099	Skill in analyzing volatile data	Computer Forensics	(3) Perform computer
Montgomery College	A.S	Information and Network	NW 275	200	41	Knowledge of organization's Local	Infrastructure Design	1. Analyze Local and Wide Area
Montgomery College	A.S	Information and Network	NW 275	200	72	Knowledge of local area network (LAN)	Infrastructure Design	1. Analyze Local and Wide Area
Montgomery College	A.S	Information and Network	NW 275	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	3. Conduct network
Montgomery College	A.S	Information and Network	NW 275	200	150	Knowledge of what constitutes a network	Information Systems/Network	2. Analyze network
Montgomery College	A.S	Information and Network	NW 275	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	4. Evaluate various network
Montgomery College	A.S	Information and Network	NW 275	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	3. Conduct network
Montgomery College	A.S	Information and Network	NW 275	200	278	Knowledge of different types of	Telecommunicatio ns	1. Analyze Local and Wide Area
Montgomery College	A.S	Information and Network	NW 275	200	902	Knowledge of the range of existing	Network Management	1. Analyze Local and Wide Area
Mercy College	A.S	Information and Network	CISC 335	300	8	Knowledge of access authentication	Identity Management	Endpoint Authn
Mercy College	A.S	Information and Network	CISC 335	300	15	Knowledge of capabilities and	Hardware	Routing principles; HuB.S,
Mercy College	A.S	Information and Network	CISC 335	300	41	Knowledge of organization's Local	Infrastructure Design	configure and troubleshot a LAN

Mercy College	A.S	Information and Network	CISC 335	300	50	Knowledge of how network services and	Infrastructure Design	describe the computer
Mercy College	A.S	Information and Network	CISC 335	300	72	Knowledge of local area network (LAN)	Infrastructure Design	configure and troubleshot a LAN
Mercy College	A.S	Information and Network	CISC 335	300	82	Knowledge of network design	Infrastructure Design	Operational Security
Mercy College	A.S	Information and Network	CISC 335	300	92	Knowledge of how traffic flows across	Infrastructure Design	describe the computer
Mercy College	A.S	Information and Network	CISC 335	300	207	Skill in installing, configuring, and		configure and troubleshot a LAN
Mercy College	A.S	Information and Network	CISC 335	300	322	Knowledge of router and routing	Infrastructure Design	Routing Principles,
Mercy College	A.S	Information and Network	CISC 335	300	387	Skill in verifying the integrity of encrypted	Encryption	Message Integrity
Mercy College	A.S	Information and Network	CISC 335	300	903	Knowledge of Wireless Fidelity	Network Management	Wireless LANs: IEEE 802.11;
Mercy College	A.S	Information and Network	CISC 335	300	1059	Knowledge of networking protocols	Infrastructure Design	describe the computer
Mercy College	A.S	Information and Network	CISC 335	300	1073	Knowledge of network systems	Network Management	What is Network Management?
Mercy College	A.S	Information and Network	CISC 359	300	89	Knowledge of new technological	Technology Awareness	server administration
Mercy College	A.S	Information and Network	CISC 359	300	112	Knowledge of server administration and	Systems Life Cycle	hosting, server administration,
Mercy College	A.S	Information and Network	CISC 359	300	122	Knowledge of system administration	Operating Systems	server administration
Mercy College	A.S	Information and Network	CISC 359	300	127	Knowledge of systems administration	Operating Systems	hosting, server administration,
Mercy College	A.S	Information and Network	CISC 359	300	149	Knowledge of web services, including	Web Technology	Students will learn how to
Mercy College	A.S	Information and Network	CISC 359	300	219	Skill in system administration for	Operating Systems	server administration
Mercy College	A.S	Information and Network	IASP 420	400	8	Knowledge of access authentication	Identity Management	explain in the network security
Mercy College	A.S	Information and Network	IASP 420	400	79	Knowledge of network access,	Identity Management	explain in the network security
Mercy College	A.S	Information and Network	IASP 420	400	82	Knowledge of network design	Infrastructure Design	identify network security
Mercy College	A.S	Information and Network	IASP 420	400	106	Knowledge of remote access technology	Information Technology	explain in the network security
Mercy College	A.S	Information and Network	IASP 420	400	123	Knowledge of system and application	Vulnerabilities Assessment	explain security threat trends like
Mercy College	A.S	Information and Network	IASP 420	400	143	Knowledge of the organization's	Enterprise Architecture	identify network security
Mercy College	A.S	Information and Network	IASP 420	400	150	Knowledge of what constitutes a network	Information Systems/Network	explain security threat trends like
Mercy College	A.S	Information and Network	IASP 420	400	355	Skill in creating plans in support of remote	Requirements Analysis	explain in the network security
Mercy College	A.S	Information and Network	IASP 420	400	895	Skill in recognizing and categorizing	Information Assurance	demonstrate some typical
Mercy College	A.S	Information and Network	IASP 420	400	967	Knowledge of current and emerging	Information Systems/Network	explain security threat trends like
Mercy College	A.S	Information and Network	IASP 420	400	990	Knowledge of common attack	Computer Network Defense	demonstrate some typical
Mercy College	A.S	Information and Network	IASP 420	400	992	Knowledge of different operational	Computer Network Defense	explain security threat trends like
Mercy College	A.S	Information and Network	IASP 420	400	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	demonstrate some typical
Mercy College	A.S	Information and Network	IASP 420	400	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	demonstrate some typical

Mercy College	A.S	Information and Network	IASP 440	400	16	Knowledge of capabilities and	Requirements Analysis	Comprehend critical skills and
Mercy College	A.S	Information and Network	IASP 440	400	126	Knowledge of system software and	Requirements Analysis	Understand security policy,
Mercy College	A.S	Information and Network	IASP 440	400	162	Skill in conducting capabilities and	Requirements Analysis	Comprehend critical skills and
Mercy College	A.S	Information and Network	IASP 440	400	300	Knowledge of intelligence reporting	Organizational Awareness	Comprehend critical skills and
Mercy College	A.S	Information and Network	IASP 440	400	986	Knowledge of organizational	Identity Management	Understand security policy,
Mercy College	A.S	Information and Network	IASP 440	400	1002	Skill in conducting audits or reviews of	Information Technology	realize the purpose of
Mercy College	A.S	Information and Network	IASP 440	400	1004	Knowledge of critical information	Contracting/Procurement	Comprehend critical skills and
Mercy College	A.S	Information and Network	IASP 440	400	1005	Knowledge of functionality, quality,	Contracting/Procurement	Comprehend critical skills and
Mercy College	A.S	Information and Network	IASP 440	400	1038	Knowledge of local specialized system	Infrastructure Design	Comprehend critical skills and
Marymount University	B.S	Information Technology	IT305	300	12	Knowledge of communication	Infrastructure Design	Describe the major features of
Marymount University	B.S	Information Technology	IT305	300	22	Knowledge of computer networking	Infrastructure Design	Describe the major features of
Marymount University	B.S	Information Technology	IT305	300	41	Knowledge of organization's Local	Infrastructure Design	Describe the telecommunicati
Marymount University	B.S	Information Technology	IT305	300	50	Knowledge of how network services and	Infrastructure Design	Define the concepts of
Marymount University	B.S	Information Technology	IT305	300	72	Knowledge of local area network (LAN)	Infrastructure Design	Describe the telecommunicati
Marymount University	B.S	Information Technology	IT305	300	81	Knowledge of network	Infrastructure Design	Define the concepts of
Marymount University	B.S	Information Technology	IT305	300	82	Knowledge of network design	Infrastructure Design	Build and configure a local
Marymount University	B.S	Information Technology	IT305	300	83	Knowledge of network hardware	Hardware	Build and configure a local
Marymount University	B.S	Information Technology	IT305	300	92	Knowledge of how traffic flows across	Infrastructure Design	Define the concepts of
Marymount University	B.S	Information Technology	IT305	300	133	Knowledge of telecommunications	Telecommunications	Describe the telecommunicati
Marymount University	B.S	Information Technology	IT305	300	139	Knowledge of common networking	Infrastructure Design	Define the concepts of
Marymount University	B.S	Information Technology	IT305	300	207	Skill in installing, configuring, and		Build and configure a local
Marymount University	B.S	Information Technology	IT305	300	212	Skill in network mapping and	Infrastructure Design	Build and configure a local
Marymount University	B.S	Information Technology	IT305	300	234	Skill in using subnetting tools	Infrastructure Design	Build and configure a local
Marymount University	B.S	Information Technology	IT305	300	261	Knowledge of basic concepts,	Telecommunications	Describe the telecommunicati
Marymount University	B.S	Information Technology	IT305	300	271	Knowledge of common network	Infrastructure Design	List the common functions of a
Marymount University	B.S	Information Technology	IT305	300	278	Knowledge of different types of	Telecommunications	Describe the technology
Marymount University	B.S	Information Technology	IT305	300	341	Knowledge of UNIX and Windows systems	Operating Systems	List the common functions of a
Marymount University	B.S	Information Technology	IT305	300	357	Skill in determining the effects of various	Configuration Management	Build and configure a local
Marymount University	B.S	Information Technology	IT305	300	902	Knowledge of the range of existing	Network Management	Describe the technology
Marymount University	B.S	Information Technology	IT305	300	989	Knowledge of Voice over Internet Protocol	Telecommunications	Distinguish between analog

Marymount University	B.S	Information Technology	IT305	300	1033	Knowledge of basic system	Information Systems/Network	List the common functions of a
Marymount University	B.S	Information Technology	IT305	300	1052	Knowledge of Global Systems for Mobile	Telecommunications	Distinguish between analog
Marymount University	B.S	Information Technology	IT305	300	1059	Knowledge of networking protocols	Infrastructure Design	Define the concepts of
Marymount University	B.S	Information Technology	IT310	300	23	Knowledge of computer	Object Technology	Discuss objectoriented
Marymount University	B.S	Information Technology	IT310	300	31	Knowledge of data mining and data	Data Management	Explain the problems with
Marymount University	B.S	Information Technology	IT310	300	32	Knowledge of database	Database Management	Write queries for single and
Marymount University	B.S	Information Technology	IT310	300	33	Knowledge of database procedures	Incident Management	Model onetoone, onetomany, and
Marymount University	B.S	Information Technology	IT310	300	34	Knowledge of database systems	Database Management	Define a relational
Marymount University	B.S	Information Technology	IT310	300	104	Knowledge of query languages such as	Database Management	Formulate and execute complex
Marymount University	B.S	Information Technology	IT310	300	120	Knowledge of sources,	Data Management	Describe the increasingly role
Marymount University	B.S	Information Technology	IT310	300	135	Knowledge of the capabilities and	Data Management	Explain the problems with
Marymount University	B.S	Information Technology	IT310	300	166	Skill in conducting queries and	Database Management	Write queries for single and
Marymount University	B.S	Information Technology	IT310	300	178	Skill in designing databases	Database Administration	Model a single entity and define
Marymount University	B.S	Information Technology	IT310	300	187	Skill in developing data models	Modeling and Simulation	List and describe the different data
Marymount University	B.S	Information Technology	IT310	300	201	Skill in generating queries and reports	Database Management	Write queries for single and
Marymount University	B.S	Information Technology	IT310	300	910	Knowledge of database theory	Data Management	List and describe the different data
Marymount University	B.S	Information Technology	IT310	300	1007	Skills in data reduction	Data Management	Recognize different normal
Marymount University	B.S	Information Technology	IT310	300	1120	Ability to interpret and incorporate data	Data Management	Model onetoone, onetomany, and
Marymount University	B.S	Information Technology	IT315	300	90	Knowledge of operating systems	Operating Systems	1. Understand the basic concepts of
Marymount University	B.S	Information Technology	IT315	300	113	Knowledge of server and client operating	Operating Systems	1. Understand the basic concepts of
Marymount University	B.S	Information Technology	IT315	300	137	Knowledge of the characteristics of	Data Management	4. Utilize memory and disk
Marymount University	B.S	Information Technology	IT315	300	174	Skill in creating programs that	Software Testing and Evaluation	5. Write several shell programs.
Marymount University	B.S	Information Technology	IT315	300	286	Knowledge of file extensions (e.g., .dll,	Operating Systems	3. Understand and be able to
Marymount University	B.S	Information Technology	IT315	300	287	Knowledge of file system	Operating Systems	3. Understand and be able to
Marymount University	B.S	Information Technology	IT315	300	342	Knowledge of Unix command line (e.g.,	Computer Languages	
Marymount University	B.S	Information Technology	IT315	300	344	Knowledge of virtualization	Operating Systems	8. Understand and use
Marymount University	B.S	Information Technology	IT315	300	371	Skill in reading, interpreting, writing,	Operating Systems	5. Write several shell programs.
Marymount University	B.S	Information Technology	IT315	300	386	Skill in using virtual machines	Operating Systems	8. Understand and use
Marymount University	B.S	Information Technology	IT315	300	1063	Knowledge of Unix/Linux operating	Operating Systems	2. Understand how the
Marymount University	B.S	Information Technology	IT335	300	4	Ability to identify systemic security	Vulnerabilities Assessment	Discuss examples of security

Marymount University	B.S	Information Technology	IT335	300	12	Knowledge of communication	Infrastructure Design	Describe cryptography and
Marymount University	B.S	Information Technology	IT335	300	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	Describe cryptography and
Marymount University	B.S	Information Technology	IT335	300	27	Knowledge of cryptology	Cryptography	Describe cryptography and
Marymount University	B.S	Information Technology	IT335	300	49	Knowledge of host/network access	Information Systems/Network	Examine techniques for
Marymount University	B.S	Information Technology	IT335	300	59	Knowledge of Intrusion Detection	Computer Network Defense	Examine intrusion response
Marymount University	B.S	Information Technology	IT335	300	66	Knowledge of intrusion detection	Computer Network Defense	Examine intrusion response
Marymount University	B.S	Information Technology	IT335	300	70	Knowledge of information	Information Systems/Network	Describe the major reasons
Marymount University	B.S	Information Technology	IT335	300	81	Knowledge of network	Infrastructure Design	Describe the protocols
Marymount University	B.S	Information Technology	IT335	300	88	Knowledge of new and emerging	Technology Awareness	Describe the major reasons
Marymount University	B.S	Information Technology	IT335	300	92	Knowledge of how traffic flows across	Infrastructure Design	Describe the protocols
Marymount University	B.S	Information Technology	IT335	300	95	Knowledge of penetration testing	Vulnerabilities Assessment	Examine various methods of
Marymount University	B.S	Information Technology	IT335	300	98	Knowledge of policybased and risk	Identity Management	Examine the need for access
Marymount University	B.S	Information Technology	IT335	300	107	Knowledge of resource	Project Management	Review management
Marymount University	B.S	Information Technology	IT335	300	109	Knowledge of secure configuration	Configuration Management	Review management
Marymount University	B.S	Information Technology	IT335	300	110	Knowledge of security management	Information Assurance	Review management
Marymount University	B.S	Information Technology	IT335	300	139	Knowledge of common networking	Infrastructure Design	Describe the protocols
Marymount University	B.S	Information Technology	IT335	300	146	Knowledge of the types of Intrusion	Computer Network Defense	Examine intrusion response
Marymount University	B.S	Information Technology	IT335	300	150	Knowledge of what constitutes a network	Information Systems/Network	Examine various methods of
Marymount University	B.S	Information Technology	IT335	300	284	Knowledge of encryption algorithms	Cryptography	Describe cryptography and
Marymount University	B.S	Information Technology	IT335	300	299	Knowledge of information security	Project Management	Review management
Marymount University	B.S	Information Technology	IT335	300	891	Skill in configuring and utilizing	Configuration Management	Describe the various firewall
Marymount University	B.S	Information Technology	IT335	300	892	Skill in configuring and utilizing	Configuration Management	Examine techniques for
Marymount University	B.S	Information Technology	IT335	300	895	Skill in recognizing and categorizing	Information Assurance	Examine various methods of
Marymount University	B.S	Information Technology	IT335	300	912	Knowledge of collection	Configuration Management	Review management
Marymount University	B.S	Information Technology	IT335	300	986	Knowledge of organizational	Identity Management	Discuss examples of security
Marymount University	B.S	Information Technology	IT335	300	990	Knowledge of common attack	Computer Network Defense	Examine various methods of
Marymount University	B.S	Information Technology	IT335	300	991	Knowledge of different classes of	Computer Network Defense	Examine various methods of
Marymount University	B.S	Information Technology	IT335	300	1029	Knowledge of malware analysis	Computer Network Defense	Examine various methods of
Marymount University	B.S	Information Technology	IT335	300	1033	Knowledge of basic system	Information Systems/Network	Examine techniques for
Marymount University	B.S	Information Technology	IT335	300	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Examine various methods of

Marymount University	B.S	Information Technology	IT335	300	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Examine various methods of
Marymount University	B.S	Information Technology	IT335	300	1114	Knowledge of encryption	Cryptography	Describe cryptography and
Marymount University	B.S	Information Technology	IT355	300	56	Knowledge of information assurance	Information Assurance	e. List and illustrate the
Marymount University	B.S	Information Technology	IT355	300	116	Knowledge of software debugging	Software Development	g. Develop tests scenarios for
Marymount University	B.S	Information Technology	IT355	300	117	Knowledge of software design tools,	Software Development	i. Evaluate tools that are used in
Marymount University	B.S	Information Technology	IT355	300	118	Knowledge of software	Software Engineering	a. Examine the different phases
Marymount University	B.S	Information Technology	IT355	300	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	i. Evaluate tools that are used in
Marymount University	B.S	Information Technology	IT355	300	169	Skill in conducting test events	Systems Testing and Evaluation	g. Develop tests scenarios for
Marymount University	B.S	Information Technology	IT355	300	182	Skill in determining an appropriate level of	Systems Testing and Evaluation	g. Develop tests scenarios for
Marymount University	B.S	Information Technology	IT355	300	239	Skill in writing test plans	Systems Testing and Evaluation	g. Develop tests scenarios for
Marymount University	B.S	Information Technology	IT355	300	950	Skill in evaluating test plans for applicability	Systems Testing and Evaluation	g. Develop tests scenarios for
Marymount University	B.S	Information Technology	IT355	300	976	Knowledge of software quality	Software Engineering	e. List and illustrate the
Marymount University	B.S	Information Technology	IT355	300	1020	Skill in secure test plan deisn (i.e., unit,	Systems Testing and Evaluation	g. Develop tests scenarios for
Marymount University	B.S	Information Technology	IT370	300	24	Knowledge of concepts and	Data Management	6. Digital Evidence Controls
Marymount University	B.S	Information Technology	IT370	300	29	Knowledge of data backup, types of	Computer Forensics	11. Recovering Image Files
Marymount University	B.S	Information Technology	IT370	300	114	Knowledge of server diagnostic tools and	Computer Forensics	4. Current Computer
Marymount University	B.S	Information Technology	IT370	300	217	Skill in preserving evidence integrity	Computer Forensics	6. Digital Evidence Controls
Marymount University	B.S	Information Technology	IT370	300	252	Knowledge of and experience in Insider	Computer Network Defense	2. Understanding Computer
Marymount University	B.S	Information Technology	IT370	300	290	Knowledge of processes for seizing	Forensics	6. Digital Evidence Controls
Marymount University	B.S	Information Technology	IT370	300	302	Knowledge of investigative	Computer Forensics	1. Computer Forensics and
Marymount University	B.S	Information Technology	IT370	300	310	Knowledge of legal governance related to	Criminal Law	14. Becoming an Expert Witness
Marymount University	B.S	Information Technology	IT370	300	313	Knowledge of logging services for network	Information Systems/Network	12. Network Forensics
Marymount University	B.S	Information Technology	IT370	300	316	Knowledge of processes for	Criminal Law	5. Processing Crime and
Marymount University	B.S	Information Technology	IT370	300	340	Knowledge of types and collection of	Computer Forensics	9. Data Acquisition
Marymount University	B.S	Information Technology	IT370	300	346	Knowledge of which system files (e.g. log	Computer Forensics	8. Macintosh and Linux Boot
Marymount University	B.S	Information Technology	IT370	300	360	Skill in identifying and extracting data of	Computer Forensics	9. Data Acquisition
Marymount University	B.S	Information Technology	IT370	300	369	Skill in collecting, processing,	Forensics	6. Digital Evidence Controls
Marymount University	B.S	Information Technology	IT370	300	374	Skill in setting up a forensic workstation	Forensics	3. The Investigator's
Marymount University	B.S	Information Technology	IT370	300	379	Skill in using common digital forensics tools	Computer Forensics	4. Current Computer
Marymount University	B.S	Information Technology	IT370	300	381	Skill in using forensic tool suites (e.g.	Computer Forensics	4. Current Computer

Marymount University	B.S	Information Technology	IT370	300	888	Knowledge of types of digital forensics data	Computer Forensics	10. Computer Forensic Analysis
Marymount University	B.S	Information Technology	IT370	300	889	Knowledge of deployable forensics	Computer Forensics	10. Computer Forensic Analysis
Marymount University	B.S	Information Technology	IT370	300	890	Skill in conducting forensic analyses in	Computer Forensics	10. Computer Forensic Analysis
Marymount University	B.S	Information Technology	IT370	300	908	Ability to decrypt digital data collections	Computer Forensics	10. Computer Forensic Analysis
Marymount University	B.S	Information Technology	IT370	300	978	Knowledge of root cause analysis for	Incident Management	10. Computer Forensic Analysis
Marymount University	B.S	Information Technology	IT370	300	982	Knowledge of electronic evidence	Criminal Law	6. Digital Evidence Controls
Marymount University	B.S	Information Technology	IT370	300	1011	Knowledge of processes for	Security	5. Processing Crime and
Marymount University	B.S	Information Technology	IT370	300	1044	Skill in identifying forensic footprints	Computer Forensics	10. Computer Forensic Analysis
Marymount University	B.S	Information Technology	IT370	300	1086	Knowledge of data carving tools and	Computer Forensics	9. Data Acquisition
Marymount University	B.S	Information Technology	IT370	300	1093	Knowledge of common forensic tool	Computer Forensics	4. Current Computer
Marymount University	B.S	Information Technology	IT390	300	17	Knowledge of certified ethical	Vulnerabilities Assessment	g. Use common attack and defend
Marymount University	B.S	Information Technology	IT390	300	19	Knowledge of Computer Network	Computer Network Defense	g. Use common attack and defend
Marymount University	B.S	Information Technology	IT390	300	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	b. Understand legal, ethical and
Marymount University	B.S	Information Technology	IT390	300	138	Knowledge of the computer network	Information Systems/Network	d. Review the steps involved in
Marymount University	B.S	Information Technology	IT390	300	150	Knowledge of what constitutes a network	Information Systems/Network	a. Recognize common network
Marymount University	B.S	Information Technology	IT390	300	153	Skill in handling malware	Computer Network Defense	g. Use common attack and defend
Marymount University	B.S	Information Technology	IT390	300	181	Skill in detecting host and network based	Computer Network Defense	g. Use common attack and defend
Marymount University	B.S	Information Technology	IT390	300	210	Skill in mimicking threat behaviors	Computer Network Defense	g. Use common attack and defend
Marymount University	B.S	Information Technology	IT390	300	269	Knowledge of CNE/CNA/CNO	Computer Network Defense	g. Use common attack and defend
Marymount University	B.S	Information Technology	IT390	300	274	Knowledge of concepts, principles,	Computer Network Defense	a. Recognize common network
Marymount University	B.S	Information Technology	IT390	300	294	Knowledge of hacking methodologies in	Surveillance	g. Use common attack and defend
Marymount University	B.S	Information Technology	IT390	300	300	Knowledge of intelligence reporting	Organizational Awareness	b. Understand legal, ethical and
Marymount University	B.S	Information Technology	IT390	300	377	Skill in tracking and analyzing technical	Legal, Government and Jurisprudence	b. Understand legal, ethical and
Marymount University	B.S	Information Technology	IT390	300	895	Skill in recognizing and categorizing	Information Assurance	a. Recognize common network
Marymount University	B.S	Information Technology	IT390	300	984	Knowledge of computer network	Computer Network Defense	b. Understand legal, ethical and
Marymount University	B.S	Information Technology	IT390	300	990	Knowledge of common attack	Computer Network Defense	a. Recognize common network
Marymount University	B.S	Information Technology	IT390	300	991	Knowledge of different classes of	Computer Network Defense	a. Recognize common network
Marymount University	B.S	Information Technology	IT390	300	992	Knowledge of different operational	Computer Network Defense	d. Review the steps involved in
Marymount University	B.S	Information Technology	IT390	300	1036	Knowledge of applicable laws (e.g.,	Criminal Law	b. Understand legal, ethical and
Marymount University	B.S	Information Technology	IT390	300	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	c. Evaluate and identify the

Marymount University	B.S	Information Technology	IT390	300	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	c. Evaluate and identify the
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	17. Probe a system for
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	24	Knowledge of concepts and	Data Management	20. Understand basic forensics
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	59	Knowledge of Intrusion Detection	Computer Network Defense	15. Employ intrusion
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	83	Knowledge of network hardware	Hardware	5. Compare network
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	92	Knowledge of how traffic flows across	Infrastructure Design	6. Describe the OSI model of
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	123	Knowledge of system and application	Vulnerabilities Assessment	1. Identify the top threats to a
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	163	Skill in conducting information searches	Computer Skills	19. Search the Web for
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	173	Skill in creating policies that relfect	Information Systems Security	16. Evaluate and improve existing
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	225	Skill in the use of penetration testing	Vulnerabilities Assessment	12. Be familiar with various
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	252	Knowledge of and experience in Insider	Computer Network Defense	9. Understand cyber stalking and
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	353	Skill in collecting data from a variety of	Computer Network Defense	3. Use online resources to
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	967	Knowledge of current and emerging	Information Systems/Network	10. Describe Dos attacks and how
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	1059	Knowledge of networking protocols	Infrastructure Design	4. Identify each of the major
Hagerstown Community	A.S	Technology and Computer	CYB 101	100	1114	Knowledge of encryption	Cryptography	14. Explain the basics of
Hagerstown Community	A.S	Technology and Computer	CYB 201	200	110	Knowledge of security management		3. Apply ethical theories to
Hagerstown Community	A.S	Technology and Computer	CYB 201	200	376	Skill in talking to others to convey	Oral Communication	2. Communicate effectively with
Hagerstown Community	A.S	Technology and Computer	CYB 225	200	17	Knowledge of certified ethical	Vulnerabilities Assessment	3. Review and practice
Hagerstown Community	A.S	Technology and Computer	CYB 225	200	19	Knowledge of Computer Network	Computer Network Defense	7. Install, configure, use
Hagerstown Community	A.S	Technology and Computer	CYB 225	200	82	Knowledge of network design	Infrastructure Design	4. Administer a network
Hagerstown Community	A.S	Technology and Computer	CYB 225	200	88	Knowledge of new and emerging	Technology Awareness	6. Evaluate and implement new
Hagerstown Community	A.S	Technology and Computer	CYB 225	200	156	Skill in applying confidentiality,	Information Assurance	8. Evaluate best practices in
Hagerstown Community	A.S	Technology and Computer	CYB 225	200	207	Skill in installing, configuring, and		5. Troubleshoot problems in an
Hagerstown Community	A.S	Technology and Computer	CYB 225	200	277	Knowledge of defense indepth principles and	Computer Network Defense	9. Design a network defense
Hagerstown Community	A.S	Technology and Computer	CYB 225	200	376	Skill in talking to others to convey	Oral Communication	2. Communicate effectively with
Hagerstown Community	A.S	Technology and Computer	CYB 225	200	985	Skill in configuring and utilizing network	Configuration Management	10. Strategically place and
Hagerstown Community	A.S	Technology and Computer	CYB 240	200	19	Knowledge of Computer Network	Computer Network Defense	12. Describe cyber defense
Hagerstown Community	A.S	Technology and Computer	CYB 240	200	88	Knowledge of new and emerging	Technology Awareness	6. Evaluate and implement new
Hagerstown Community	A.S	Technology and Computer	CYB 240	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	7. Install, configure, use
Hagerstown Community	A.S	Technology and Computer	CYB 240	200	108	Knowledge of risk management	Risk Management	13. Describe appropriate

Hagerstown Community	A.S	Technology and Computer	CYB 240	200	156	Skill in applying confidentiality,	Information Assurance	8. Evaluate best practices in
Hagerstown Community	A.S	Technology and Computer	CYB 240	200	211	Skill in monitoring and optimizing server	Information Technology	9. Use a network monitoring tool
Hagerstown Community	A.S	Technology and Computer	CYB 240	200	212	Skill in network mapping and	Infrastructure Design	10. Use a network mapping
Hagerstown Community	A.S	Technology and Computer	CYB 240	200	294	Knowledge of hacking methodologies in	Surveillance	3. Identify the steps of the
Hagerstown Community	A.S	Technology and Computer	CYB 240	200	368	Skill in navigating mapping tools	Computer Skills	Use a network mapping tool
Hagerstown Community	A.S	Technology and Computer	CYB 240	200	376	Skill in talking to others to convey	Oral Communication	2. Communicate effectively with
Hagerstown Community	A.S	Technology and Computer	CYB 240	200	895	Skill in recognizing and categorizing	Information Assurance	11. Describe potential system
Hagerstown Community	A.S	Technology and Computer	CYB 240	200	920	Knowledge of threat list countries' cyber	External Awareness	14. Identify the bad actors in
Hagerstown Community	A.S	Technology and Computer	CYB 240	200	967	Knowledge of current and emerging	Information Systems/Network	4. List and describe the
Hagerstown Community	A.S	Technology and Computer	CYB 240	200	1072	Knowledge of network security	Information Systems/Network	16. Examine the architecture of a
Hagerstown Community	A.S	Technology and Computer	CYB 245	200	17	Knowledge of certified ethical	Vulnerabilities Assessment	6. Review and practice
Hagerstown Community	A.S	Technology and Computer	CYB 245	200	88	Knowledge of new and emerging	Technology Awareness	7. Evaluate and implement new
Hagerstown Community	A.S	Technology and Computer	CYB 245	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	3. Identify the penetration
Hagerstown Community	A.S	Technology and Computer	CYB 245	200	156	Skill in applying confidentiality,	Information Assurance	9. Evaluate best practices in
Hagerstown Community	A.S	Technology and Computer	CYB 245	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	4. Plan and preform a
Hagerstown Community	A.S	Technology and Computer	CYB 245	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	8. Install, configure, use
Hagerstown Community	A.S	Technology and Computer	CYB 245	200	376	Skill in talking to others to convey	Oral Communication	2. Communicate effectively with
Hagerstown Community	A.S	Technology and Computer	IST 108	100	90	Knowledge of operating systems	Operating Systems	3. Identify the characteristics of
Hagerstown Community	A.S	Technology and Computer	IST 108	100	163	Skill in conducting information searches	Computer Skills	9. Perform advanced
Hagerstown Community	A.S	Technology and Computer	IST 108	100	347	Knowledge of Windows command	Operating Systems	1. Compare the Windows
Hagerstown Community	A.S	Technology and Computer	IST/CSC 109	100	89	Knowledge of new technological	Technology Awareness	3. Research and present
Hagerstown Community	A.S	Technology and Computer	IST/CSC 109	100	342	Knowledge of Unix command line (e.g.,	Computer Languages	1. Choose appropriate
Hagerstown Community	A.S	Technology and Computer	IST/CSC 109	100	371	Skill in reading, interpreting, writing,	Operating Systems	2. Write efficient, effective scripts
Hagerstown Community	A.S	Cybersecurity	IST156	100	81	Knowledge of network	Infrastructure Design	2. Troubleshoot router
Hagerstown Community	A.S	Cybersecurity	IST156	100	92	Knowledge of how traffic flows across	Infrastructure Design	2. Troubleshoot router
Hagerstown Community	A.S	Cybersecurity	IST156	100	139	Knowledge of common networking	Infrastructure Design	1. Using IOS commands and
Hagerstown Community	A.S	Cybersecurity	IST156	100	157	Skill in applying host/network access	Identity Management	3. Provide security for a
Hagerstown Community	A.S	Cybersecurity	IST156	100	191	Skill in developing and applying security	Identity Management	3. Provide security for a
Hagerstown Community	A.S	Cybersecurity	IST154	100	15	Knowledge of capabilities and	Hardware	1. Provide an introduction to
Hagerstown Community	A.S	Cybersecurity	IST154	100	49	Knowledge of host/network access	Information Systems/Network	1.Provide an introduction to

Hagerstown Community	A.S	Cybersecurity	IST154	100	50	Knowledge of how network services and	Infrastructure Design	1. Provide an introduction to
Hagerstown Community	A.S	Cybersecurity	IST154	100	72	Knowledge of local area network (LAN)	Infrastructure Design	1. Provide an introduction to
Hagerstown Community	A.S	Cybersecurity	IST154	100	81	Knowledge of network	Infrastructure Design	1. Provide an introduction to
Hagerstown Community	A.S	Cybersecurity	IST154	100	92	Knowledge of how traffic flows across	Infrastructure Design	1.Provide an introduction to
Hagerstown Community	A.S	Cybersecurity	IST155	100	12	Knowledge of communication	Infrastructure Design	1. Create a physical layer
Hagerstown Community	A.S	Cybersecurity	IST155	100	15	Knowledge of capabilities and	Hardware	1. Create a physical layer
Hagerstown Community	A.S	Cybersecurity	IST155	100	22	Knowledge of computer networking	Infrastructure Design	1. Create a physical layer
Hagerstown Community	A.S	Cybersecurity	IST155	100	50	Knowledge of how network services and	Infrastructure Design	1. Create a physical layer
Hagerstown Community	A.S	Cybersecurity	IST155	100	92	Knowledge of how traffic flows across	Infrastructure Design	2. Develop a logical network
Hagerstown Community	A.S	Cybersecurity	IST155	100	139	Knowledge of common networking	Infrastructure Design	2. Develop a logical network
Hagerstown Community	A.S	Cybersecurity	IST155	100	342	Knowledge of Unix command line (e.g.,	Computer Languages	3. Use a command line
Hagerstown Community	A.S	Cybersecurity	IST155	100	347	Knowledge of Windows command	Operating Systems	3. Use a command line
Hagerstown Community	A.S	Cybersecurity	IST155	100	371	Skill in reading, interpreting, writing,	Operating Systems	3. Use a command line
Hagerstown Community	A.S	Cybersecurity	IST160	100	22	Knowledge of computer networking	Infrastructure Design	1. Fundamentals of network
Hagerstown Community	A.S	Cybersecurity	IST160	100	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	1. Fundamentals of network
Hagerstown Community	A.S	Cybersecurity	IST160	100	49	Knowledge of host/network access	Information Systems/Network	1. Fundamentals of network
Hagerstown Community	A.S	Cybersecurity	IST160	100	58	Knowledge of known vulnerabilities from	Information Systems/Network	1. Fundamentals of network
Hagerstown Community	A.S	Cybersecurity	IST160	100	70	Knowledge of information	Information Systems/Network	1. Fundamentals of network
Hagerstown Community	A.S	Cybersecurity	IST160	100	111	Knowledge of security system design tools,	Information Systems/Network	1. Fundamentals of network
Hagerstown Community	A.S	Cybersecurity	IST160	100	150	Knowledge of what constitutes a network	Information Systems/Network	1. Fundamentals of network
Hagerstown Community	A.S	Cybersecurity	IST160	100	175	Skill in developing and deploying signatures	Information Systems/Network	1. Fundamentals of network
Hagerstown Community	A.S	Cybersecurity	IST255	200	15	Knowledge of capabilities and	Hardware	1. Design and implement a
Hagerstown Community	A.S	Cybersecurity	IST255	200	72	Knowledge of local area network (LAN)	Infrastructure Design	2. Configure a router to support
Hagerstown Community	A.S	Cybersecurity	IST255	200	207	Skill in installing, configuring, and		2. Configure a router to support
Hagerstown Community	A.S	Cybersecurity	IST255	200	278	Knowledge of different types of	Telecommunications	1. Design and implement a
Hagerstown Community	A.S	Cybersecurity	IST261	200	15	Knowledge of capabilities and	Hardware	4. Configuring Network
Hagerstown Community	A.S	Cybersecurity	IST261	200	22	Knowledge of computer networking	Infrastructure Design	4. Configuring Network
Hagerstown Community	A.S	Cybersecurity	IST261	200	107	Knowledge of resource	Project Management	5. Configuring Access to
Hagerstown Community	A.S	Cybersecurity	IST261	200	122	Knowledge of system administration	Operating Systems	1. Installing, Upgrading, and
Hagerstown Community	A.S	Cybersecurity	IST261	200	170	Skill in configuring and optimizing	Software Engineering	3. Configuring Hardware and

Hagerstown Community	A.S	Cybersecurity	IST261	200	341	Knowledge of UNIX and Windows systems	Operating Systems	7. Monitoring and Maintaining
Hagerstown Community	A.S	Cybersecurity	IST261	200	356	Skill in determining installed patches on	Operating Systems	7. Monitoring and Maintaining
Highline Community	A.S	Data Recover / Forensics	CIS 115	100	374	Skill in setting up a forensic workstation	Forensics	Use standard hardware devices
Highline Community	A.S	Data Recover / Forensics	CIS 115	100	379	Skill in using common digital forensics tools	Computer Forensics	Use and evaluate new software
Highline Community	A.S	Data Recover / Forensics	CIS 115	100	381	Skill in using forensic tool suites (e.g.	Computer Forensics	Use standard software
Highline Community	A.S	Data Recover / Forensics	CIS 115	100	1093	Knowledge of common forensic tool	Computer Forensics	Use standard software
Highline Community	A.S	Data Recover / Forensics	CIS 160	100	41	Knowledge of organization's Local	Infrastructure Design	Describe basic configuration of
Highline Community	A.S	Data Recover / Forensics	CIS 160	100	92	Knowledge of how traffic flows across	Infrastructure Design	Explain the functions of each
Highline Community	A.S	Data Recover / Forensics	CIS 160	100	212	Skill in network mapping and	Infrastructure Design	Design basicnetwork
Highline Community	A.S	Data Recover / Forensics	CIS 160	100	322	Knowledge of router and routing	Infrastructure Design	Explain how routing is used in
Highline Community	A.S	Computer Science	CIS 161	100	15	Knowledge of capabilities and	Hardware	Have a basic understanding of
Highline Community	A.S	Computer Science	CIS 161	100	207	Skill in installing, configuring, and		Troubleshoot a network using
Highline Community	A.S	Computer Science	CIS 161	100	278	Knowledge of different types of	Telecommunicatio ns	List and use all components of a
Highline Community	A.S	Computer Science	CIS 161	100	281	Knowledge of electronic devices	Hardware	Install and manage network
Highline Community	A.S	Computer Science	CIS 161	100	322	Knowledge of router and routing	Infrastructure Design	Describe the use of router to
Highline Community	A.S	Computer Science	CIS 161	100	358	Skill in determining tactics, techniques,	Strategic Thinking	Describe the use of router to
Highline Community	A.S	Computer Science	CIS 161	100	902	Knowledge of the range of existing	Network Management	Document network activity.
Highline Community	A.S	Network Specialist	CIS 166	100	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Conduct a vulnerability
Highline Community	A.S	Network Specialist	CIS 166	100	4	Ability to identify systemic security	Vulnerabilities Assessment	Conduct a vulnerability
Highline Community	A.S	Network Specialist	CIS 166	100	37	Knowledge of disaster recovery and	Incident Management	List the elements of an effective
Highline Community	A.S	Network Specialist	CIS 166	100	59	Knowledge of Intrusion Detection	Computer Network Defense	List characteristics of
Highline Community	A.S	Network Specialist	CIS 166	100	79	Knowledge of network access,	Identity Management	Authenicate network access.
Highline Community	A.S	Network Specialist	CIS 166	100	106	Knowledge of remote access technology	Information Technology	List the impacts of VPNs, remote
Highline Community	A.S	Network Specialist	CIS 166	100	146	Knowledge of the types of Intrusion	Computer Network Defense	List characteristics of
Highline Community	A.S	Network Specialist	CIS 166	100	148	Knowledge of VPN security.	Encryption	List the impacts of VPNs, remote
Highline Community	A.S	Network Specialist	CIS 166	100	157	Skill in applying host/network access	Identity Management	Authenicate network access.
Highline Community	A.S	Network Specialist	CIS 166	100	193	Skill in developing, testing, and	Information Assurance	List the elements of an effective
Highline Community	A.S	Network Specialist	CIS 166	100	294	Knowledge of hacking methodologies in	Surveillance	Be able to demonstrate how
Highline Community	A.S	Network Specialist	CIS 166	100	296	Knowledge of how information needs	External Awareness	Identify Internal and External
Highline Community	A.S	Network Specialist	CIS 166	100	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	Conduct a system audit

Highline Community	A.S	Network Specialist	CIS 166	100	356	Skill in determining installed patches on	Operating Systems	Install network patches.
Highline Community	A.S	Network Specialist	CIS 166	100	985	Skill in configuring and utilizing network	Configuration Management	List characteristics of
Highline Community	A.S	Network Specialist	CIS 166	100	1002	Skill in conducting audits or reviews of	Information Technology	Conduct a system audit
Highline Community	A.S	Network Specialist	CIS 166	100	1121	Knowledge of Windows/Unix ports	Operating Systems	List standard ports for
Highline Community	A.S	Computer Science	CIS 210	200	90	Knowledge of operating systems	Operating Systems	Demonstrate the ability to manage
Highline Community	A.S	Computer Science	CIS 210	200	113	Knowledge of server and client operating	Operating Systems	Research, analyze and specify the
Highline Community	A.S	Computer Science	CIS 210	200	314	Knowledge of multiple cognitive	Teaching Others	Demonstrate the ability to and
Highline Community	A.S	Computer Science	CIS 210	200	332	Ability to develop curriculum that	Teaching Others	Describe the pros and cons of the
Highline Community	A.S	Computer Science	CIS 210	200	344	Knowledge of virtualization	Operating Systems	Understand and implement load
Highline Community	A.S	Computer Science	CIS 210	200	386	Skill in using virtual machines	Operating Systems	Be able to describe and
Highline Community	A.S	Computer Science	CIS 210	200	918	Ability to prepare and deliver education and	Teaching Others	Describe the pros and cons of the
Highline Community	A.S	Computer Science	CIS 210	200	1117	Skill in utilizing virtual networks for testing	Operating Systems	Understand and implement load
Highline Community	A.S	Computer Science	CIS 215	200	122	Knowledge of system administration	Operating Systems	Demostrate an overall
Highline Community	A.S	Computer Science	CIS 215	200	219	Skill in system administration for	Operating Systems	Become aquainted with
Highline Community	A.S	Computer Science	CIS 215	200	364	Skill in identifying, modifying, and	Operating Systems	Use the UNIX file system to
Highline Community	A.S	Computer Science	CIS 215	200	1063	Knowledge of Unix/Linux operating	Operating Systems	Use UNIX tools to process data
Highline Community	A.S	Computer Science	CIS 216	200	122	Knowledge of system administration	Operating Systems	Demonstrate overall
Highline Community	A.S	Computer Science	CIS 216	200	342	Knowledge of Unix command line (e.g.,	Computer Languages	Demonstrate overall
Highline Community	A.S	Computer Science	CIS 216	200	371	Skill in reading, interpreting, writing,	Operating Systems	Demostrate an understanding of
Highline Community	A.S	Computer Science	CIS 216	200	1063	Knowledge of Unix/Linux operating	Operating Systems	Use file system monitoring for
Highline Community	A.S	Computer Science	CIS 217	200	122	Knowledge of system administration	Operating Systems	Demostrate knowledge of
Highline Community	A.S	Computer Science	CIS 217	200	219	Skill in system administration for	Operating Systems	Demostrate an understanding of
Highline Community	A.S	Computer Science	CIS 217	200	341	Knowledge of UNIX and Windows systems	Operating Systems	Demostrate an understanding of
Highline Community	A.S	Computer Science	CIS 217	200	342	Knowledge of Unix command line (e.g.,	Computer Languages	Demonstrate a fundamental
Highline Community	A.S	Computer Science	CIS 217	200	364	Skill in identifying, modifying, and	Operating Systems	Demostrate a fundemental
Highline Community	A.S	Computer Science	CIS 217	200	371	Skill in reading, interpreting, writing,	Operating Systems	Demostrate knowledge of
Highline Community	A.S	Computer Science	CIS 217	200	1063	Knowledge of Unix/Linux operating	Operating Systems	Demostrate an understanding of
Highline Community	A.S	Computer Science	CIS 217	200	1121	Knowledge of Windows/Unix ports	Operating Systems	Demonstrate an understanding of
Highline Community	A.S	Web / Database Developer	CIS 230	200	32	Knowledge of database	Database Management	Demonstrate Database Admin.
Highline Community	A.S	Web / Database Developer	CIS 230	200	34	Knowledge of database systems	Database Management	Create a standard database backup

Highline Community	A.S	Web / Database Developer	CIS 230	200	135	Knowledge of the capabilities and	Data Management	Demonstrate Database Admin.
Highline Community	A.S	Web / Database Developer	CIS 230	200	208	Skill in maintaining databases	Database Management	Demonstrate Database Admin.
Highline Community	A.S	Web / Database Developer	CIS 230	200	1114	Knowledge of encryption	Cryptography	Describe and use encryption
Highline Community	A.S	Computer Science	CIS 235	200	114	Knowledge of server diagnostic tools and	Computer Forensics	Analyze forensic data using
Highline Community	A.S	Computer Science	CIS 235	200	219	Skill in system administration for	Operating Systems	Effectively use the command
Highline Community	A.S	Computer Science	CIS 235	200	290	Knowledge of processes for seizing	Forensics	Document processes and
Highline Community	A.S	Computer Science	CIS 235	200	342	Knowledge of Unix command line (e.g.,	Computer Languages	Effectively use the command
Highline Community	A.S	Computer Science	CIS 235	200	359	Skill in developing and executing technical	Computer Forensics	Discuss the issues of digital
Highline Community	A.S	Computer Science	CIS 235	200	363	Skill in identifying gaps in technical	Teaching Others	Discuss the issues of digital
Highline Community	A.S	Computer Science	CIS 235	200	369	Skill in collecting, processing,	Forensics	Document processes and
Highline Community	A.S	Computer Science	CIS 235	200	381	Skill in using forensic tool suites (e.g.	Computer Forensics	Analyze forensic data using
Highline Community	A.S	Computer Science	CIS 235	200	1040	Knowledge of relevant laws,	Criminal Law	Document processes and
Highline Community	A.S	Computer Science	CIS 235	200	1044	Skill in identifying forensic footprints	Computer Forensics	Analyze forensic data using
Highline Community	A.S	Computer Science	CIS 235	200	1086	Knowledge of data carving tools and	Computer Forensics	Conduct indepth data carving and
Highline Community	A.S	Computer Science	CIS 235	200	1093	Knowledge of common forensic tool	Computer Forensics	Analyze forensic data using
Highline Community	A.S	Computer Science	CIS 235	200	1097	Knowledge of virtual machine aware	Computer Network Defense	Utilize electronic discovery tools
Highline Community	A.S	Computer Science	CIS 235	200	1118	Skill in reading and interpreting	Information Systems/Network	Analyze forensic data using
Highline Community	A.S	Data Recover / Forensics	CIS 236	200	29	Knowledge of data backup, types of	Computer Forensics	Demostrate the ability to recover
Highline Community	A.S	Data Recover / Forensics	CIS 236	200	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	Document processes and
Highline Community	A.S	Data Recover / Forensics	CIS 236	200	290	Knowledge of processes for seizing	Forensics	Document processes and
Highline Community	A.S	Data Recover / Forensics	CIS 236	200	300	Knowledge of intelligence reporting	Organizational Awareness	Be able to compose a well
Highline Community	A.S	Data Recover / Forensics	CIS 236	200	358	Skill in determining tactics, techniques,	Strategic Thinking	Be able to compose a well
Highline Community	A.S	Data Recover / Forensics	CIS 236	200	360	Skill in identifying and extracting data of	Computer Forensics	Retrieve ediscovery
Highline Community	A.S	Data Recover / Forensics	CIS 236	200	369	Skill in collecting, processing,	Forensics	Demostrate the ability to recover
Highline Community	A.S	Data Recover / Forensics	CIS 236	200	377	Skill in tracking and analyzing technical	Legal, Government and Jurisprudence	Understand and demostrate
Highline Community	A.S	Data Recover / Forensics	CIS 236	200	379	Skill in using common digital forensics tools	Computer Forensics	Use standard forensics toots
Highline Community	A.S	Data Recover / Forensics	CIS 236	200	381	Skill in using forensic tool suites (e.g.	Computer Forensics	Use standard forensics toots
Highline Community	A.S	Data Recover / Forensics	CIS 236	200	918	Ability to prepare and deliver education and	Teaching Others	Discuss the issues of digital forensic
Highline Community	A.S	Data Recover / Forensics	CIS 236	200	1086	Knowledge of data carving tools and	Computer Forensics	Use standard forensics toots
Prince George's	A.S	Business Management	BMT 2860	200	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	1. Jurisdiction and Venue in

Prince George's	A.S	Business Management	BMT 2860	200	305	Knowledge of laws that affect cyber	Forensics	2. Copyright Law in the Digital
Prince George's	A.S	Business Management	BMT 2860	200	310	Knowledge of legal governance related to	Criminal Law	7. Computer Crimes
Prince George's	A.S	Business Management	BMT 2860	200	316	Knowledge of processes for	Criminal Law	7. Computer Crimes
Prince George's	A.S	Business Management	BMT 2860	200	981	Knowledge of International Traffic in	Criminal Law	7. Computer Crimes
Prince George's	A.S	Business Management	BMT 2860	200	982	Knowledge of electronic evidence	Criminal Law	7. Computer Crimes
Prince George's	A.S	Business Management	BMT 2860	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	2. Copyright Law in the Digital
Prince George's	A.S	Business Management	BMT 2860	200	1040	Knowledge of relevant laws,	Criminal Law	2. Copyright Law in the Digital
Prince George's	A.S	Business Management	BMT 2860	200	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	2. Copyright Law in the Digital
Prince George's	A.S	Business Management	BMT 2880	200	29	Knowledge of data backup, types of	Computer Forensics	9. Preparedness for
Prince George's	A.S	Business Management	BMT 2880	200	37	Knowledge of disaster recovery and	Incident Management	1. Introduction to Emergency
Prince George's	A.S	Business Management	BMT 2880	200	40	Knowledge of organization's	Systems Testing and Evaluation	12. Evaluation
Prince George's	A.S	Business Management	BMT 2880	200	60	Knowledge of incident categories, incident	Incident Management	1. Introduction to Emergency
Prince George's	A.S	Business Management	BMT 2880	200	61	Knowledge of incident response and	Incident Management	1. Introduction to Emergency
Prince George's	A.S	Business Management	BMT 2880	200	108	Knowledge of risk management	Risk Management	6. Hazard, Vulnerability, and
Prince George's	A.S	Business Management	BMT 2880	200	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	12. Evaluation
Prince George's	A.S	Business Management	BMT 2880	200	193	Skill in developing, testing, and	Information Assurance	9. Preparedness for
Prince George's	A.S	Business Management	BMT 2880	200	966	Knowledge of enterprise incident	Incident Management	1. Introduction to Emergency
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	24	Knowledge of concepts and	Data Management	Processing crime and incident
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	217	Skill in preserving evidence integrity	Computer Forensics	Computer forensics and
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	219	Skill in system administration for	Operating Systems	Mactintosh and Linux boot
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	281	Knowledge of electronic devices	Hardware	Computer hardware,
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	287	Knowledge of file system	Operating Systems	Windows operating system
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	290	Knowledge of processes for seizing	Forensics	Processing crime and incident
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	302	Knowledge of investigative	Computer Forensics	The investigator's office and
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	316	Knowledge of processes for	Criminal Law	Identify the terminology used
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	326	Knowledge of security hardware and	Information Systems/Network	Computer hardware,
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	347	Knowledge of Windows command	Operating Systems	Working with Windows, file and
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	359	Skill in developing and executing technical	Computer Forensics	Computer forensics and
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	360	Skill in identifying and extracting data of	Computer Forensics	Acquiring and authentication
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	369	Skill in collecting, processing,	Forensics	First Response Processing crime

Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	374	Skill in setting up a forensic workstation	Forensics	The investigator's office and
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	379	Skill in using common digital forensics tools	Computer Forensics	Current computer forensics tools
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	381	Skill in using forensic tool suites (e.g.	Computer Forensics	Current computer forensics tools
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	888	Knowledge of types of digital forensics data	Computer Forensics	Acquiring and authentication
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	1044	Skill in identifying forensic footprints	Computer Forensics	recovering graphic files
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	1063	Knowledge of Unix/Linux operating	Operating Systems	Macintosh and Linux boot
Prince George's	Certifica	Information Security, Cyber	FOS 2600	200	1097	Knowledge of virtual machine aware	Computer Network Defense	Network Forensics
Prince George's	Certifica	Cyber Crime Investigations	FOS 2610	200	24	Knowledge of concepts and	Data Management	Identify the procedures
Prince George's	Certifica	Cyber Crime Investigations	FOS 2610	200	87	Knowledge of network traffic	Information Systems/Network	Introduction to network analysis
Prince George's	Certifica	Cyber Crime Investigations	FOS 2610	200	93	Knowledge of packetlevel analysis	Vulnerabilities Assessment	Introduction to and installation of
Prince George's	Certifica	Cyber Crime Investigations	FOS 2610	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	Metasploit research
Prince George's	Certifica	Cyber Crime Investigations	FOS 2610	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	Introduction to and installation of
Prince George's	Certifica	Cyber Crime Investigations	FOS 2610	200	294	Knowledge of hacking methodologies in	Surveillance	Describe hacking and other types
Prince George's	Certifica	Cyber Crime Investigations	FOS 2610	200	316	Knowledge of processes for	Criminal Law	Describe network based
Prince George's	Certifica	Cyber Crime Investigations	FOS 2610	200	366	Skill in law enforcement report	Technical Documentation	Preparing cases for court; explain
Prince George's	Certifica	Cyber Crime Investigations	FOS 2610	200	900	Knowledge of web filtering technologies	Web Technology	Filters
Prince George's	Certifica	Cyber Crime Investigations	FOS 2610	200	1029	Knowledge of malware analysis	Computer Network Defense	Malware isolation and infiltration
Prince George's	Certifica	Cyber Crime Investigations	FOS 2610	200	1093	Knowledge of common forensic tool	Computer Forensics	Using Wireshark and analyzing
Prince George's	Certifica	Cyber Crime Investigations	FOS 2610	200	1097	Knowledge of virtual machine aware	Computer Network Defense	Malware isolation and infiltration
Prince George's	A.S	Information Technology,	INT 1010	100	42	Knowledge of electrical engineering	Hardware Engineering	Knowledge of Computer
Prince George's	A.S	Information Technology,	INT 1010	100	68	Knowledge of information	Information Technology	dentify current and emerging
Prince George's	A.S	Information Technology,	INT 1010	100	69	Knowledge of Risk Management	Information Systems Security	Describe risk management
Prince George's	A.S	Information Technology,	INT 1010	100	108	Knowledge of risk management	Risk Management	Describe risk management
Prince George's	A.S	Information Technology,	INT 1010	100	155	Skill in applying and incorporating	Technology Awareness	Identify current and emerging
Prince George's	A.S	Information Technology,	INT 1010	100	264	Knowledge of basic physical computer	Computers and Electronics	computer hardware
Prince George's	A.S	Information Technology,	INT 1010	100	281	Knowledge of electronic devices	Hardware	Various Comptuer hardware and its
Prince George's	A.S	Information Technology,	INT 1010	100	915	Knowledge of frontend collection	Information Systems/Network	Explain data communications
Prince George's	A.S	Information Technology,	INT 1010	100	916	Skill in deconflicting cyber operations and	Political Savvy	Explain why the Internet was
Prince George's	A.S	Information Technology,	INT 1010	100	917	Knowledge of social dynamics of computer	External Awareness	Demonstrate a proficiency in
Prince George's	A.S	Information Technology,Infor	INT 1620	100	8	Knowledge of access authentication	Identity Management	h. Privilege security model

Prince George's	A.S	Information Technology,Infor	INT 1620	100	9	Knowledge of applicable business	Requirements Analysis	16. Management a. Study disaster
Prince George's	A.S	Information Technology,Infor	INT 1620	100	12	Knowledge of communication	Infrastructure Design	6. Communications
Prince George's	A.S	Information Technology,Infor	INT 1620	100	15	Knowledge of capabilities and	Hardware	9. Infrastructure security
Prince George's	A.S	Information Technology,Infor	INT 1620	100	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	6. Communications
Prince George's	A.S	Information Technology,Infor	INT 1620	100	27	Knowledge of cryptology	Cryptography	11. Cryptography a. Exploits and
Prince George's	A.S	Information Technology,Infor	INT 1620	100	28	Knowledge of data administration and	Data Management	16. Management a. Study disaster
Prince George's	A.S	Information Technology,Infor	INT 1620	100	29	Knowledge of data backup, types of	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	37	Knowledge of disaster recovery and	Incident Management	16. Management a. Study disaster
Prince George's	A.S	Information Technology,Infor	INT 1620	100	49	Knowledge of host/network access	Information Systems/Network	h. Privilege security model
Prince George's	A.S	Information Technology,Infor	INT 1620	100	50	Knowledge of how network services and	Infrastructure Design	6. Communications
Prince George's	A.S	Information Technology,Infor	INT 1620	100	59	Knowledge of Intrusion Detection	Computer Network Defense	4. Study tools such as ping,
Prince George's	A.S	Information Technology,Infor	INT 1620	100	60	Knowledge of incident categories, incident	Incident Management	16. Management a. Study disaster
Prince George's	A.S	Information Technology,Infor	INT 1620	100	61	Knowledge of incident response and	Incident Management	16. Management a. Study disaster
Prince George's	A.S	Information Technology,Infor	INT 1620	100	62	Knowledge of industrystandard and	Logical Systems Design	16. Management a. Study disaster
Prince George's	A.S	Information Technology,Infor	INT 1620	100	63	Knowledge of Information	Information Assurance	e. Confidentiality, Integrity and
Prince George's	A.S	Information Technology,Infor	INT 1620	100	66	Knowledge of intrusion detection	Computer Network Defense	4. Study tools such as ping,
Prince George's	A.S	Information Technology,Infor	INT 1620	100	69	Knowledge of Risk Management	Information Systems Security	g. Risk security model
Prince George's	A.S	Information Technology,Infor	INT 1620	100	70	Knowledge of information	Information Systems/Network	General Security Concepts
Prince George's	A.S	Information Technology,Infor	INT 1620	100	77	Knowledege of current industry	Information Systems/Network	13. Look at standards
Prince George's	A.S	Information Technology,Infor	INT 1620	100	79	Knowledge of network access,	Identity Management	12. Public Key Infrastructure
Prince George's	A.S	Information Technology,Infor	INT 1620	100	81	Knowledge of network	Infrastructure Design	1. TCP/IP Concepts and OSI
Prince George's	A.S	Information Technology,Infor	INT 1620	100	92	Knowledge of how traffic flows across	Infrastructure Design	1. TCP/IP Concepts and OSI
Prince George's	A.S	Information Technology,Infor	INT 1620	100	98	Knowledge of policybased and risk	Identity Management	h. Privilege security model
Prince George's	A.S	Information Technology,Infor	INT 1620	100	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	13. Look at standards
Prince George's	A.S	Information Technology,Infor	INT 1620	100	108	Knowledge of risk management	Risk Management	g. Risk security model
Prince George's	A.S	Information Technology,Infor	INT 1620	100	114	Knowledge of server diagnostic tools and	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	126	Knowledge of system software and	Requirements Analysis	13. Look at standards
Prince George's	A.S	Information Technology,Infor	INT 1620	100	133	Knowledge of telecommunications	Telecommunications	6. Communications
Prince George's	A.S	Information Technology,Infor	INT 1620	100	139	Knowledge of common networking	Infrastructure Design	1. TCP/IP Concepts and OSI
Prince George's	A.S	Information Technology,Infor	INT 1620	100	146	Knowledge of the types of Intrusion	Computer Network Defense	4. Study tools such as ping,

Prince George's	A.S	Information Technology,Infor	INT 1620	100	148	Knowledge of VPN security.	Encryption	6. Communications
Prince George's	A.S	Information Technology,Infor	INT 1620	100	149	Knowledge of web services, including	Web Technology	8. Web Security a. HTTP, SHTTP,
Prince George's	A.S	Information Technology,Infor	INT 1620	100	153	Skill in handling malware	Computer Network Defense	3. Malware and Attacks
Prince George's	A.S	Information Technology,Infor	INT 1620	100	156	Skill in applying confidentiality,	Information Assurance	e. Confidentiality, Integrity and
Prince George's	A.S	Information Technology,Infor	INT 1620	100	157	Skill in applying host/network access	Identity Management	h. Privilege security model
Prince George's	A.S	Information Technology,Infor	INT 1620	100	177	Skill in designing countermeasures to	Vulnerabilities Assessment	d. Study host countermeasures
Prince George's	A.S	Information Technology,Infor	INT 1620	100	181	Skill in detecting host and network based	Computer Network Defense	4. Study tools such as ping,
Prince George's	A.S	Information Technology,Infor	INT 1620	100	185	Skill in developing applications that can	Software Development	c. Logging and Auditing
Prince George's	A.S	Information Technology,Infor	INT 1620	100	191	Skill in developing and applying security	Identity Management	h. Privilege security model
Prince George's	A.S	Information Technology,Infor	INT 1620	100	212	Skill in network mapping and	Infrastructure Design	9. Infrastructure security
Prince George's	A.S	Information Technology,Infor	INT 1620	100	217	Skill in preserving evidence integrity	Computer Forensics	13. Look at standards
Prince George's	A.S	Information Technology,Infor	INT 1620	100	237	Skill in using Virtual Private Network	Encryption	6. Communications
Prince George's	A.S	Information Technology,Infor	INT 1620	100	261	Knowledge of basic concepts,	Telecommunicatio ns	6. Communications
Prince George's	A.S	Information Technology,Infor	INT 1620	100	271	Knowledge of common network	Infrastructure Design	4. Study tools such as ping,
Prince George's	A.S	Information Technology,Infor	INT 1620	100	277	Knowledge of defense indepth principles and	Computer Network Defense	b. Defenseindepth
Prince George's	A.S	Information Technology,Infor	INT 1620	100	284	Knowledge of encryption algorithms	Cryptography	11. Cryptography a. Exploits and
Prince George's	A.S	Information Technology,Infor	INT 1620	100	290	Knowledge of processes for seizing	Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	300	Knowledge of intelligence reporting	Organizational Awareness	13. Look at standards
Prince George's	A.S	Information Technology,Infor	INT 1620	100	302	Knowledge of investigative	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	305	Knowledge of laws that affect cyber	Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	310	Knowledge of legal governance related to	Criminal Law	13. Look at standards
Prince George's	A.S	Information Technology,Infor	INT 1620	100	313	Knowledge of logging services for network	Information Systems/Network	c. Logging and Auditing
Prince George's	A.S	Information Technology,Infor	INT 1620	100	316	Knowledge of processes for	Criminal Law	14. Study physical security
Prince George's	A.S	Information Technology,Infor	INT 1620	100	329	Knowledge of surveillance detection	Surveillance	d. Study host countermeasures
Prince George's	A.S	Information Technology,Infor	INT 1620	100	341	Knowledge of UNIX and Windows systems	Operating Systems	4. Study tools such as ping,
Prince George's	A.S	Information Technology,Infor	INT 1620	100	345	Knowledge of web mail collection,	Web Technology	8. Web Security a. HTTP, SHTTP,
Prince George's	A.S	Information Technology,Infor	INT 1620	100	346	Knowledge of which system files (e.g. log	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	348	Knowledge of wireless network collection	Cryptography	11. Cryptography a. Exploits and
Prince George's	A.S	Information Technology,Infor	INT 1620	100	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	c. Logging and Auditing
Prince George's	A.S	Information Technology,Infor	INT 1620	100	359	Skill in developing and executing technical	Computer Forensics	15. Forensics a. Study

Prince George's	A.S	Information Technology,Infor	INT 1620	100	360	Skill in identifying and extracting data of	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	369	Skill in collecting, processing,	Forensics	14. Study physical security
Prince George's	A.S	Information Technology,Infor	INT 1620	100	374	Skill in setting up a forensic workstation	Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	377	Skill in tracking and analyzing technical	Legal, Government and Jurisprudence	13. Look at standards
Prince George's	A.S	Information Technology,Infor	INT 1620	100	379	Skill in using common digital forensics tools	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	381	Skill in using forensic tool suites (e.g.	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	385	Skill in using traceroute analysis	Network Management	4. Study tools such as ping,
Prince George's	A.S	Information Technology,Infor	INT 1620	100	888	Knowledge of types of digital forensics data	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	889	Knowledge of deployable forensics	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	890	Skill in conducting forensic analyses in	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	891	Skill in configuring and utilizing	Configuration Management	4. Study tools such as ping,
Prince George's	A.S	Information Technology,Infor	INT 1620	100	892	Skill in configuring and utilizing	Configuration Management	4. Study tools such as ping,
Prince George's	A.S	Information Technology,Infor	INT 1620	100	893	Skill in securing network	Information Assurance	6. Communications
Prince George's	A.S	Information Technology,Infor	INT 1620	100	895	Skill in recognizing and categorizing	Information Assurance	3. Malware and Attacks
Prince George's	A.S	Information Technology,Infor	INT 1620	100	896	Skill in protecting a network against	Computer Network Defense	3. Malware and Attacks
Prince George's	A.S	Information Technology,Infor	INT 1620	100	900	Knowledge of web filtering technologies	Web Technology	8. Web Security a. HTTP, SHTTP,
Prince George's	A.S	Information Technology,Infor	INT 1620	100	901	Knowledge of the capabilities of	Network Management	6. Communications
Prince George's	A.S	Information Technology,Infor	INT 1620	100	908	Ability to decrypt digital data collections	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	942	Knowledge of the organization's core	Organizational Awareness	16. Management a. Study disaster
Prince George's	A.S	Information Technology,Infor	INT 1620	100	965	Knowledge of organization's risk	Risk Management	g. Risk security model16.
Prince George's	A.S	Information Technology,Infor	INT 1620	100	966	Knowledge of enterprise incident	Incident Management	16. Management a. Study disaster
Prince George's	A.S	Information Technology,Infor	INT 1620	100	968	Knowledge of softwarerelated	Information Systems/Network	General Security Concepts
Prince George's	A.S	Information Technology,Infor	INT 1620	100	979	Knowledge of supply chain risk	Risk Management	16. Management a. Study disaster
Prince George's	A.S	Information Technology,Infor	INT 1620	100	984	Knowledge of computer network	Computer Network Defense	16. Management a. Study disaster
Prince George's	A.S	Information Technology,Infor	INT 1620	100	985	Skill in configuring and utilizing network	Configuration Management	4. Study tools such as ping,
Prince George's	A.S	Information Technology,Infor	INT 1620	100	986	Knowledge of organizational	Identity Management	a. Study security principles
Prince George's	A.S	Information Technology,Infor	INT 1620	100	991	Knowledge of different classes of	Computer Network Defense	3. Malware and Attacks
Prince George's	A.S	Information Technology,Infor	INT 1620	100	993	Knowledge of the methods, standards,	Enterprise Architecture	13. Look at standards
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1021	Knowledge of threat assessment	Risk Management	16. Management a. Study disaster
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1029	Knowledge of malware analysis	Computer Network Defense	3. Malware and Attacks

Prince George's	A.S	Information Technology,Infor	INT 1620	100	1036	Knowledge of applicable laws (e.g.,	Criminal Law	13. Look at standards
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1037	Knowledge of information	Risk Management	g. Risk security model
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1044	Skill in identifying forensic footprints	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1059	Knowledge of networking protocols	Infrastructure Design	6. Communications
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	4. Study tools such as ping,
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	13. Look at standards
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1072	Knowledge of network security	Information Systems/Network	b. Defenseindepth
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1086	Knowledge of data carving tools and	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1087	Skill in deep analysis of captured malicious	Computer Network Defense	3. Malware and Attacks
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1092	Knowledge of antiforensics tactics,	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1093	Knowledge of common forensic tool	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1096	Knowledge of malware analysis	Computer Network Defense	3. Malware and Attacks
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1097	Knowledge of virtual machine aware	Computer Network Defense	3. Malware and Attacks
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1099	Skill in analyzing volatile data	Computer Forensics	15. Forensics a. Study
Prince George's	A.S	Information Technology,Infor	INT 1620	100	1114	Knowledge of encryption	Cryptography	11. Cryptography a. Exploits and
Prince George's	A.S	Information Security	INT 1680	100	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	hacking overview hacking phases
Prince George's	A.S	Information Security	INT 1680	100	59	Knowledge of Intrusion Detection	Computer Network Defense	Understand the fundamentals of
Prince George's	A.S	Information Security	INT 1680	100	70	Knowledge of information	Information Systems/Network	Understand the fundamentals of
Prince George's	A.S	Information Security	INT 1680	100	81	Knowledge of network	Infrastructure Design	Understand the fundamentals of
Prince George's	A.S	Information Security	INT 1680	100	92	Knowledge of how traffic flows across	Infrastructure Design	understand the funda
Prince George's	A.S	Information Security	INT 1680	100	139	Knowledge of common networking	Infrastructure Design	Understand the fundamentals of
Prince George's	A.S	Information Security	INT 1680	100	141	Knowledge of the enterprise	Information Technology	supernetting and the TCP life cycle
Prince George's	A.S	Information Security	INT 1680	100	146	Knowledge of the types of Intrusion	Computer Network Defense	Understand the fundamentals of
Prince George's	A.S	Information Security	INT 1680	100	148	Knowledge of VPN security.	Encryption	Understand the fundamentals of
Prince George's	A.S	Information Security	INT 1680	100	226	Skill in the use of social engineering	Human Factors	Explore social engineering
Prince George's	A.S	Information Security	INT 1680	100	237	Skill in using Virtual Private Network	Encryption	Understand the fundamentals of
Prince George's	A.S	Information Security	INT 1680	100	294	Knowledge of hacking methodologies in	Surveillance	Ethical hacking overiew
Prince George's	A.S	Information Security	INT 1680	100	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	Penetration Methodology
Prince George's	A.S	Information Security	INT 1680	100	891	Skill in configuring and utilizing	Configuration Management	Understand the fundamentals of
Prince George's	A.S	Information Security	INT 1680	100	892	Skill in configuring and utilizing	Configuration Management	Understand the fundamentals of

Prince George's	A.S	Information Security	INT 1680	100	899	Skill in gathering information from	Information Management	Social engineering
Prince George's	A.S	Information Security	INT 1680	100	917	Knowledge of social dynamics of computer	External Awareness	Introduction to Social
Prince George's	A.S	Information Security	INT 1680	100	985	Skill in configuring and utilizing network	Configuration Management	Understand the fundamentals of
Prince George's	A.S	Information Security	INT 1680	100	986	Knowledge of organizational	Identity Management	Password types and cracking
Prince George's	A.S	Information Security	INT 1680	100	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Practice using the tools for
Prince George's	A.S	Information Security	INT 1680	100	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Practice using the tools for
Prince George's	A.S	Information Security	INT 1680	100	1121	Knowledge of Windows/Unix ports	Operating Systems	port scanning for vulnearability
Prince George's	A.S	Computer Service	INT 1700	100	347	Knowledge of Windows command	Operating Systems	Demonstrate the ability to perform
Prince George's	A.S	Information Technology,	INT 2300	200	29	Knowledge of data backup, types of	Computer Forensics	Configure backup and recovery –
Prince George's	A.S	Information Technology,	INT 2300	200	37	Knowledge of disaster recovery and	Incident Management	Configure backup and recovery –
Prince George's	A.S	Information Technology,	INT 2300	200	55	Knowledge of Information	Information Assurance	Managing and working with disk
Prince George's	A.S	Information Technology,	INT 2300	200	77	Knowledege of current industry	Information Systems/Network	Monitoring and maintaining
Prince George's	A.S	Information Technology,	INT 2300	200	137	Knowledge of the characteristics of	Data Management	Managing and working with disk
Prince George's	A.S	Information Technology,	INT 2300	200	170	Skill in configuring and optimizing	Software Engineering	Configure hardware and
Prince George's	A.S	Information Technology,	INT 2300	200	193	Skill in developing, testing, and	Information Assurance	Configure backup and recovery –
Prince George's	A.S	Information Technology,	INT 2300	200	207	Skill in installing, configuring, and		Configure network
Prince George's	A.S	Information Technology,	INT 2300	200	221	Skill in testing and configuring network	Network Management	Configure hardware and
Prince George's	A.S	Information Technology,	INT 2300	200	264	Knowledge of basic physical computer	Computers and Electronics	Managing and working with disk
Prince George's	A.S	Information Technology,	INT 2300	200	281	Knowledge of electronic devices	Hardware	Managing and working with disk
Prince George's	A.S	Information Technology,	INT 2300	200	322	Knowledge of router and routing	Infrastructure Design	Configure network
Prince George's	A.S	Information Technology,	INT 2300	200	327	Knowledge of security implications of	Information Assurance	Configure hardware and
Prince George's	A.S	Information Technology,	INT 2300	200	347	Knowledge of Windows command	Operating Systems	Overview of Windows
Prince George's	A.S	Information Technology,	INT 2300	200	357	Skill in determining the effects of various	Configuration Management	Configure network
Prince George's	A.S	Information Technology,	INT 2300	200	364	Skill in identifying, modifying, and	Operating Systems	Managing users and group
Prince George's	A.S	Information Technology,	INT 2300	200	891	Skill in configuring and utilizing	Configuration Management	Configure hardware and
Prince George's	A.S	Information Technology,	INT 2300	200	892	Skill in configuring and utilizing	Configuration Management	Managing Windows
Prince George's	A.S	Information Technology,	INT 2300	200	985	Skill in configuring and utilizing network	Configuration Management	Configure hardware and
Prince George's	A.S	Information Technology,	INT 2300	200	986	Knowledge of organizational	Identity Management	Managing users and group
Prince George's	A.S	Information Technology,	INT 2300	200	1073	Knowledge of network systems	Network Management	Monitoring and maintaining
Prince George's	A.S	Information Technology,	INT 2300	200	1121	Knowledge of Windows/Unix ports	Operating Systems	Overview of Windows

Prince George's	A.S	Information Security	INT 2680	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Explain techniques to
Prince George's	A.S	Information Security	INT 2680	200	4	Ability to identify systemic security	Vulnerabilities Assessment	Explain techniques to
Prince George's	A.S	Information Security	INT 2680	200	8	Knowledge of access authentication	Identity Management	Understanding Authentication
Prince George's	A.S	Information Security	INT 2680	200	23	Knowledge of computer	Object Technology	Programming for Security
Prince George's	A.S	Information Security	INT 2680	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	Cryptography
Prince George's	A.S	Information Security	INT 2680	200	27	Knowledge of cryptology	Cryptography	Cryptography
Prince George's	A.S	Information Security	INT 2680	200	43	Knowledge of embedded systems	Embedded Computers	Embedded Oss
Prince George's	A.S	Information Security	INT 2680	200	79	Knowledge of network access,	Identity Management	Understanding Public Key
Prince George's	A.S	Information Security	INT 2680	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	Explore the use advanced of
Prince George's	A.S	Information Security	INT 2680	200	123	Knowledge of system and application	Vulnerabilities Assessment	Desktop and Server OS
Prince George's	A.S	Information Security	INT 2680	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	Explore the use advanced of
Prince George's	A.S	Information Security	INT 2680	200	261	Knowledge of basic concepts,	Telecommunications	Describe wireless hacking and tools
Prince George's	A.S	Information Security	INT 2680	200	278	Knowledge of different types of	Telecommunications	Describe wireless hacking and tools
Prince George's	A.S	Information Security	INT 2680	200	348	Knowledge of wireless network collection	Cryptography	Describe wireless hacking and tools
Prince George's	A.S	Information Security	INT 2680	200	371	Skill in reading, interpreting, writing,	Operating Systems	Programming for Security
Prince George's	A.S	Information Security	INT 2680	200	886	Skill in wireless network target	Vulnerabilities Assessment	Understanding Wireless Hacking
Prince George's	A.S	Information Security	INT 2680	200	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	Explore the use advanced of
Prince George's	A.S	Information Security	INT 2680	200	1114	Knowledge of encryption	Cryptography	Cryptography
Prince George's	A.S	Information Security	INT 2690	200	4	Ability to identify systemic security	Vulnerabilities Assessment	Risk Analysis Risk Analysis
Prince George's	A.S	Information Security	INT 2690	200	5	Ability to match the appropriate	Knowledge Management	Security Definitions
Prince George's	A.S	Information Security	INT 2690	200	8	Knowledge of access authentication	Identity Management	Identification, Authentication,
Prince George's	A.S	Information Security	INT 2690	200	10	Knowledge of application	Vulnerabilities Assessment	Applications Security
Prince George's	A.S	Information Security	INT 2690	200	12	Knowledge of communication	Infrastructure Design	Cryptography History of
Prince George's	A.S	Information Security	INT 2690	200	17	Knowledge of certified ethical	Vulnerabilities Assessment	Hacking and Attacking
Prince George's	A.S	Information Security	INT 2690	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	Cryptography Cryptography
Prince George's	A.S	Information Security	INT 2690	200	27	Knowledge of cryptology	Cryptography	Cryptography History of
Prince George's	A.S	Information Security	INT 2690	200	28	Knowledge of data administration and	Data Management	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	29	Knowledge of data backup, types of	Computer Forensics	Back ups
Prince George's	A.S	Information Security	INT 2690	200	31	Knowledge of data mining and data	Data Management	Data Warehousing and
Prince George's	A.S	Information Security	INT 2690	200	32	Knowledge of database	Database Management	Database Management

Prince George's	A.S	Information Security	INT 2690	200	33	Knowledge of database procedures	Incident Management	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	34	Knowledge of database systems	Database Management	Database Management
Prince George's	A.S	Information Security	INT 2690	200	37	Knowledge of disaster recovery and	Incident Management	Business Continuity
Prince George's	A.S	Information Security	INT 2690	200	38	Knowledge of organization's	Information Assurance	Organizational Security Model
Prince George's	A.S	Information Security	INT 2690	200	40	Knowledge of organization's	Systems Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	41	Knowledge of organization's Local	Infrastructure Design	Wide Area Network
Prince George's	A.S	Information Security	INT 2690	200	44	Knowledge of enterprise messaging	Enterprise Architecture	Security Architecture and
Prince George's	A.S	Information Security	INT 2690	200	49	Knowledge of host/network access	Information Systems/Network	Access Controls Access Controls
Prince George's	A.S	Information Security	INT 2690	200	50	Knowledge of how network services and	Infrastructure Design	Networking Services and
Prince George's	A.S	Information Security	INT 2690	200	55	Knowledge of Information	Information Assurance	Fundamental Principles of
Prince George's	A.S	Information Security	INT 2690	200	56	Knowledge of information assurance	Information Assurance	Fundamental Principles of
Prince George's	A.S	Information Security	INT 2690	200	62	Knowledge of industrystandard and	Logical Systems Design	Fundamental Principles of
Prince George's	A.S	Information Security	INT 2690	200	63	Knowledge of Information	Information Assurance	Fundamental Principles of
Prince George's	A.S	Information Security	INT 2690	200	64	Knowledge of information security	Information Systems/ Network	Fundamental Principles of
Prince George's	A.S	Information Security	INT 2690	200	68	Knowledge of information	Information Technology	An architectural View
Prince George's	A.S	Information Security	INT 2690	200	69	Knowledge of Risk Management	Information Systems Security	Information Security and Risk
Prince George's	A.S	Information Security	INT 2690	200	70	Knowledge of information	Information Systems/Network	Fundamental Principles of
Prince George's	A.S	Information Security	INT 2690	200	72	Knowledge of local area network (LAN)	Infrastructure Design	Wide Area Network
Prince George's	A.S	Information Security	INT 2690	200	76	Knowledge of measures or	Information Technology	Network and Resource
Prince George's	A.S	Information Security	INT 2690	200	77	Knowledege of current industry	Information Systems/Network	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	79	Knowledge of network access,	Identity Management	Identity Management
Prince George's	A.S	Information Security	INT 2690	200	81	Knowledge of network	Infrastructure Design	TCP/IP Networking
Prince George's	A.S	Information Security	INT 2690	200	83	Knowledge of network hardware	Hardware	Networking Devices
Prince George's	A.S	Information Security	INT 2690	200	92	Knowledge of how traffic flows across	Infrastructure Design	The OSI Reference Model
Prince George's	A.S	Information Security	INT 2690	200	94	Knowledge of parallel and distributed	Information Technology	Security Architecture and
Prince George's	A.S	Information Security	INT 2690	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	Penetration Testing
Prince George's	A.S	Information Security	INT 2690	200	98	Knowledge of policybased and risk	Identity Management	Access Controls Access Controls
Prince George's	A.S	Information Security	INT 2690	200	104	Knowledge of query languages such as	Database Management	Database Management
Prince George's	A.S	Information Security	INT 2690	200	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	Keystroke Monitoring
Prince George's	A.S	Information Security	INT 2690	200	106	Knowledge of remote access technology	Information Technology	Remote Access

Prince George's	A.S	Information Security	INT 2690	200	108	Knowledge of risk management	Risk Management	Information Security and Risk
Prince George's	A.S	Information Security	INT 2690	200	109	Knowledge of secure configuration	Configuration Management	Configuration management
Prince George's	A.S	Information Security	INT 2690	200	110	Knowledge of security management	Information Assurance	Security Management
Prince George's	A.S	Information Security	INT 2690	200	111	Knowledge of security system design tools,	Information Systems/Network	System Development
Prince George's	A.S	Information Security	INT 2690	200	112	Knowledge of server administration and	Systems Life Cycle	Security Administration
Prince George's	A.S	Information Security	INT 2690	200	122	Knowledge of system administration	Operating Systems	Security Administration
Prince George's	A.S	Information Security	INT 2690	200	123	Knowledge of system and application	Vulnerabilities Assessment	Threats to Security Models
Prince George's	A.S	Information Security	INT 2690	200	124	Knowledge of system design tools,	Logical Systems Design	System Development
Prince George's	A.S	Information Security	INT 2690	200	126	Knowledge of system software and	Requirements Analysis	Organizational Security Model
Prince George's	A.S	Information Security	INT 2690	200	127	Knowledge of systems administration	Operating Systems	Security Administration
Prince George's	A.S	Information Security	INT 2690	200	128	Knowledge of systems diagnostic tools and	Systems Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	129	Knowledge of systems lifecycle management	Systems Life Cycle	Fundamental Principles of
Prince George's	A.S	Information Security	INT 2690	200	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	133	Knowledge of telecommunications	Telecommunicatio ns	Telecommunicati ons and
Prince George's	A.S	Information Security	INT 2690	200	139	Knowledge of common networking	Infrastructure Design	TCP/IP Networking
Prince George's	A.S	Information Security	INT 2690	200	141	Knowledge of the enterprise	Information Technology	An architectural View
Prince George's	A.S	Information Security	INT 2690	200	149	Knowledge of web services, including	Web Technology	Internet and Web Activities
Prince George's	A.S	Information Security	INT 2690	200	150	Knowledge of what constitutes a network	Information Systems/Network	Hacking and Attacking
Prince George's	A.S	Information Security	INT 2690	200	156	Skill in applying confidentiality,	Information Assurance	Fundamental Principles of
Prince George's	A.S	Information Security	INT 2690	200	157	Skill in applying host/network access	Identity Management	Access Controls Access Controls
Prince George's	A.S	Information Security	INT 2690	200	158	Skill in applying organizationspecific	Systems Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	166	Skill in conducting queries and	Database Management	Database Management
Prince George's	A.S	Information Security	INT 2690	200	169	Skill in conducting test events	Systems Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	173	Skill in creating policies that relfect	Information Systems Security	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	174	Skill in creating programs that	Software Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	176	Skill in designing a data analysis	Systems Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	Countermeasure Selection
Prince George's	A.S	Information Security	INT 2690	200	179	Skill in designing security controls	Information Assurance	Fundamental Principles of
Prince George's	A.S	Information Security	INT 2690	200	182	Skill in determining an appropriate level of	Systems Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	183	Skill in determining how a security system	Information Assurance	Security Modes of Operation

Prince George's	A.S	Information Security	INT 2690	200	185	Skill in developing applications that can	Software Development	Application Development
Prince George's	A.S	Information Security	INT 2690	200	187	Skill in developing data models	Modeling and Simulation	Database Models
Prince George's	A.S	Information Security	INT 2690	200	190	Skill in developing operationsbased	Systems Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	191	Skill in developing and applying security	Identity Management	Access Controls Access Controls
Prince George's	A.S	Information Security	INT 2690	200	193	Skill in developing, testing, and	Information Assurance	Business Continuity
Prince George's	A.S	Information Security	INT 2690	200	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	Protection Mechanisms
Prince George's	A.S	Information Security	INT 2690	200	201	Skill in generating queries and reports	Database Management	Database Management
Prince George's	A.S	Information Security	INT 2690	200	202	Skill in identifying and anticipating server	Information Technology	Network and Resource
Prince George's	A.S	Information Security	INT 2690	200	204	Skill in identifying possible causes of	Systems Life Cycle	Network and Resource
Prince George's	A.S	Information Security	INT 2690	200	207	Skill in installing, configuring, and		Wide Area Network
Prince George's	A.S	Information Security	INT 2690	200	208	Skill in maintaining databases	Database Management	Database Management
Prince George's	A.S	Information Security	INT 2690	200	212	Skill in network mapping and	Infrastructure Design	Network topologies
Prince George's	A.S	Information Security	INT 2690	200	217	Skill in preserving evidence integrity	Computer Forensics	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	219	Skill in system administration for	Operating Systems	Security Administration
Prince George's	A.S	Information Security	INT 2690	200	220	Skill in systems integration testing	Systems Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	Penetration Testing
Prince George's	A.S	Information Security	INT 2690	200	231	Skill in using network management tools to	Network Management	Networking Services and
Prince George's	A.S	Information Security	INT 2690	200	237	Skill in using Virtual Private Network	Encryption	Networking Devices
Prince George's	A.S	Information Security	INT 2690	200	239	Skill in writing test plans	Systems Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	252	Knowledge of and experience in Insider	Computer Network Defense	Politics and Laws Regulations and
Prince George's	A.S	Information Security	INT 2690	200	261	Knowledge of basic concepts,	Telecommunicatio ns	Telecommunicati ons and
Prince George's	A.S	Information Security	INT 2690	200	264	Knowledge of basic physical computer	Computers and Electronics	Security Architecture and
Prince George's	A.S	Information Security	INT 2690	200	270	Knowledge of common adversary	Computer Network Defense	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	277	Knowledge of defense indepth principles and	Computer Network Defense	A Layered Approach
Prince George's	A.S	Information Security	INT 2690	200	278	Knowledge of different types of	Telecommunicatio ns	Telecommunicati ons and
Prince George's	A.S	Information Security	INT 2690	200	281	Knowledge of electronic devices	Hardware	Networking Devices
Prince George's	A.S	Information Security	INT 2690	200	284	Knowledge of encryption algorithms	Cryptography	Cryptography
Prince George's	A.S	Information Security	INT 2690	200	294	Knowledge of hacking methodologies in	Surveillance	Hacking and Attacking
Prince George's	A.S	Information Security	INT 2690	200	300	Knowledge of intelligence reporting	Organizational Awareness	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	305	Knowledge of laws that affect cyber	Forensics	Politics and Laws Regulations and

Prince George's	A.S	Information Security	INT 2690	200	310	Knowledge of legal governance related to	Criminal Law	Regulations and Compliance
Prince George's	A.S	Information Security	INT 2690	200	313	Knowledge of logging services for network	Information Systems/Network	Networking Devices
Prince George's	A.S	Information Security	INT 2690	200	316	Knowledge of processes for	Criminal Law	Regulations and Compliance
Prince George's	A.S	Information Security	INT 2690	200	322	Knowledge of router and routing	Infrastructure Design	Routing Protocols Networking
Prince George's	A.S	Information Security	INT 2690	200	325	Knowledge of secure acquisitions (e.g.,	Contracting/Procurement	Information Security and Risk
Prince George's	A.S	Information Security	INT 2690	200	327	Knowledge of security implications of	Information Assurance	Software Importance
Prince George's	A.S	Information Security	INT 2690	200	329	Knowledge of surveillance detection	Surveillance	Countermeasure Selection
Prince George's	A.S	Information Security	INT 2690	200	336	Knowledge of the nature and function	Telecommunications	Telecommunications and
Prince George's	A.S	Information Security	INT 2690	200	338	Knowledge of the principal methods,	Reasoning	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	341	Knowledge of UNIX and Windows systems	Operating Systems	Identification, Authentication,
Prince George's	A.S	Information Security	INT 2690	200	345	Knowledge of web mail collection,	Web Technology	Internet and Web Activities
Prince George's	A.S	Information Security	INT 2690	200	348	Knowledge of wireless network collection	Cryptography	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	Hacking and Attacking
Prince George's	A.S	Information Security	INT 2690	200	357	Skill in determining the effects of various	Configuration Management	Configuration management
Prince George's	A.S	Information Security	INT 2690	200	358	Skill in determining tactics, techniques,	Strategic Thinking	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	359	Skill in developing and executing technical	Computer Forensics	Security Awareness
Prince George's	A.S	Information Security	INT 2690	200	364	Skill in identifying, modifying, and	Operating Systems	Password Management
Prince George's	A.S	Information Security	INT 2690	200	366	Skill in law enforcement report	Technical Documentation	Regulations and Compliance
Prince George's	A.S	Information Security	INT 2690	200	375	Skill in survey, collection, and	Network Management	Wireless Technologies
Prince George's	A.S	Information Security	INT 2690	200	886	Skill in wireless network target	Vulnerabilities Assessment	Wireless Technologies
Prince George's	A.S	Information Security	INT 2690	200	891	Skill in configuring and utilizing	Configuration Management	Protection Mechanisms
Prince George's	A.S	Information Security	INT 2690	200	892	Skill in configuring and utilizing	Configuration Management	Protection Mechanisms
Prince George's	A.S	Information Security	INT 2690	200	895	Skill in recognizing and categorizing	Information Assurance	Hacking and Attacking
Prince George's	A.S	Information Security	INT 2690	200	900	Knowledge of web filtering technologies	Web Technology	Internet and Web Activities
Prince George's	A.S	Information Security	INT 2690	200	901	Knowledge of the capabilities of	Network Management	Internet and Web Activities
Prince George's	A.S	Information Security	INT 2690	200	902	Knowledge of the range of existing	Network Management	Wide Area Network
Prince George's	A.S	Information Security	INT 2690	200	903	Knowledge of Wireless Fidelity	Network Management	Wireless Technologies
Prince George's	A.S	Information Security	INT 2690	200	907	Skill in data mining techniques	Data Management	Data Warehousing and
Prince George's	A.S	Information Security	INT 2690	200	910	Knowledge of database theory	Data Management	Database Security Issues
Prince George's	A.S	Information Security	INT 2690	200	912	Knowledge of collection	Configuration Management	Configuration management

Prince George's	A.S	Information Security	INT 2690	200	917	Knowledge of social dynamics of computer	External Awareness	Hacking and Attacking
Prince George's	A.S	Information Security	INT 2690	200	918	Ability to prepare and deliver education and	Teaching Others	Education Policies,
Prince George's	A.S	Information Security	INT 2690	200	950	Skill in evaluating test plans for applicability	Systems Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	965	Knowledge of organization's risk	Risk Management	Information Security and Risk
Prince George's	A.S	Information Security	INT 2690	200	966	Knowledge of enterprise incident	Incident Management	Layers of Responsibility
Prince George's	A.S	Information Security	INT 2690	200	968	Knowledge of softwarerelated	Information Systems/Network	A Layered Approach
Prince George's	A.S	Information Security	INT 2690	200	974	Ability to tailor code analysis for	Software Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	978	Knowledge of root cause analysis for	Incident Management	Risk Analysis Risk Analysis
Prince George's	A.S	Information Security	INT 2690	200	979	Knowledge of supply chain risk	Risk Management	Information Security and Risk
Prince George's	A.S	Information Security	INT 2690	200	980	Skill in performing root cause analysis for	Incident Management	Risk Analysis Risk Analysis
Prince George's	A.S	Information Security	INT 2690	200	981	Knowledge of International Traffic in	Criminal Law	Regulations and Compliance
Prince George's	A.S	Information Security	INT 2690	200	982	Knowledge of electronic evidence	Criminal Law	Regulations and Compliance
Prince George's	A.S	Information Security	INT 2690	200	984	Knowledge of computer network	Computer Network Defense	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	985	Skill in configuring and utilizing network	Configuration Management	Protection Mechanisms
Prince George's	A.S	Information Security	INT 2690	200	986	Knowledge of organizational	Identity Management	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	989	Knowledge of Voice over Internet Protocol	Telecommunicatio ns	Telecommunicati ons and
Prince George's	A.S	Information Security	INT 2690	200	990	Knowledge of common attack	Computer Network Defense	Hacking and Attacking
Prince George's	A.S	Information Security	INT 2690	200	991	Knowledge of different classes of	Computer Network Defense	Hacking and Attacking
Prince George's	A.S	Information Security	INT 2690	200	992	Knowledge of different operational	Computer Network Defense	Different Environments
Prince George's	A.S	Information Security	INT 2690	200	993	Knowledge of the methods, standards,	Enterprise Architecture	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	1002	Skill in conducting audits or reviews of	Information Technology	Review of Audit Information
Prince George's	A.S	Information Security	INT 2690	200	1005	Knowledge of functionality, quality,	Contracting/Procur ement	Complexity of Functionality
Prince George's	A.S	Information Security	INT 2690	200	1020	Skill in secure test plan deisn (i.e., unit,	Systems Testing and Evaluation	Systems Evaluation
Prince George's	A.S	Information Security	INT 2690	200	1021	Knowledge of threat assessment	Risk Management	Information Security and Risk
Prince George's	A.S	Information Security	INT 2690	200	1022	Knowledge of the nature and function	Enterprise Architecture	Security Architecture and
Prince George's	A.S	Information Security	INT 2690	200	1033	Knowledge of basic system	Information Systems/Network	Security Administration
Prince George's	A.S	Information Security	INT 2690	200	1034	Knowledge of Personally Identifiable	Security	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	Politics and Laws Policies,
Prince George's	A.S	Information Security	INT 2690	200	1037	Knowledge of information	Risk Management	Information Security and Risk
Prince George's	A.S	Information Security	INT 2690	200	1040	Knowledge of relevant laws,	Criminal Law	Politics and Laws Policies,

Prince George's	A.S	Information Security	INT 2690	200	1047	Skill in writing kernel level applications	Software Development	Application Development
Prince George's	A.S	Information Security	INT 2690	200	1052	Knowledge of Global Systems for Mobile	Telecommunications	Telecommunications and
Prince George's	A.S	Information Security	INT 2690	200	1056	Knowledge of operations security	Public Safety and Security	Operations Security
Prince George's	A.S	Information Security	INT 2690	200	1059	Knowledge of networking protocols	Infrastructure Design	Networking Services and
Prince George's	A.S	Information Security	INT 2690	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Hacking and Attacking
Prince George's	A.S	Information Security	INT 2690	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Hacking and Attacking
Prince George's	A.S	Information Security	INT 2690	200	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	Politics and Laws Policies,
Prince George's	A.S	Information Security	INT 2690	200	1071	Knowledge of secure software deployment	Software Engineering	Software Importance
Prince George's	A.S	Information Security	INT 2690	200	1072	Knowledge of network security	Information Systems/Network	A Layered Approach
Prince George's	A.S	Information Security	INT 2690	200	1073	Knowledge of network systems	Network Management	Security Management
Prince George's	A.S	Information Security	INT 2690	200	1074	Knowledge of transmission records	Telecommunications	Telecommunications and
Prince George's	A.S	Information Security	INT 2690	200	1091	Skill in one way hash functions (e.g., Secure	Data Management	Cryptography Cryptography
Prince George's	A.S	Information Security	INT 2690	200	1092	Knowledge of antiforensics tactics,	Computer Forensics	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	1094	Knowledge of debugging procedures	Software Development	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	1101	Skill in interpreting results of debugger to	Computer Network Defense	Policies, Standards,
Prince George's	A.S	Information Security	INT 2690	200	1114	Knowledge of encryption	Cryptography	Cryptography Cryptography
Prince George's	A.S	Information Technology	INT2721	200	90	Knowledge of operating systems	Operating Systems	Linux Operating System
Prince George's	A.S	Information Technology	INT2721	200	113	Knowledge of server and client operating	Operating Systems	Linux Operating System
Prince George's	A.S	Information Technology	INT2721	200	122	Knowledge of system administration	Operating Systems	Linux Operating System
Prince George's	A.S	Information Technology	INT2721	200	127	Knowledge of systems administration	Operating Systems	Exploring Linux commands
Prince George's	A.S	Information Technology	INT2721	200	219	Skill in system administration for	Operating Systems	Security features and scripting in
Prince George's	A.S	Information Technology	INT2721	200	341	Knowledge of UNIX and Windows systems	Operating Systems	Security features and scripting in
Prince George's	A.S	Information Technology	INT2721	200	342	Knowledge of Unix command line (e.g.,	Computer Languages	Use appropriate commands like ls,
Prince George's	A.S	Information Technology	INT2721	200	364	Skill in identifying, modifying, and	Operating Systems	Describe the structure of the
Prince George's	A.S	Information Technology	INT2721	200	371	Skill in reading, interpreting, writing,	Operating Systems	Linux scripting commands
Prince George's	A.S	Information Technology	INT2721	200	1033	Knowledge of basic system	Information Systems/Network	Linux scripting commands
Prince George's	A.S	Information Technology	INT2721	200	1063	Knowledge of Unix/Linux operating	Operating Systems	Describe the structure of the
Prince George's	A.S	Information Technology	INT2721	200	1121	Knowledge of Windows/Unix ports	Operating Systems	Linux files system and controlling
Prince George's	A.S	Information Technology	INT2760	200	104	Knowledge of query languages such as	Database Management	Writing Scripts, Configuring
Prince George's	A.S	Information Technology	INT2760	200	122	Knowledge of system administration	Operating Systems	Administer the system to include

Prince George's	A.S	Information Technology	INT2760	200	219	Skill in system administration for	Operating Systems	Explain the responsibilities of
Prince George's	A.S	Information Technology	INT2760	200	364	Skill in identifying, modifying, and	Operating Systems	Write shell scripts involving loops,
Prince George's	A.S	Information Technology	INT2760	200	371	Skill in reading, interpreting, writing,	Operating Systems	Write shell scripts involving loops,
Prince George's	A.S	Information Technology	INT2760	200	1063	Knowledge of Unix/Linux operating	Operating Systems	describe the X Window system
Rochester Institute of	N/A	Elective	GCCISCSEC3	300	8	Knowledge of access authentication	Identity Management	Explain methods of user and
Rochester Institute of	N/A	Elective	GCCISCSEC3	300	148	Knowledge of VPN security.	Encryption	Identify major applications of
Rochester Institute of	N/A	Elective	GCCISCSEC3	300	237	Skill in using Virtual Private Network	Encryption	Demonstrate authentication
Rochester Institute of	N/A	Elective	GCCISCSEC3	300	1114	Knowledge of encryption	Cryptography	Describe the foundations and
Rochester Institute of	N/A	Elective	CSEC461	400	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Describe common
Rochester Institute of	N/A	Elective	CSEC461	400	10	Knowledge of application	Vulnerabilities Assessment	Describe common
Rochester Institute of	N/A	Elective	CSEC461	400	19	Knowledge of Computer Network	Computer Network Defense	Describe and discuss various
Rochester Institute of	N/A	Elective	CSEC461	400	59	Knowledge of Intrusion Detection	Computer Network Defense	Describe and discuss various
Rochester Institute of	N/A	Elective	CSEC461	400	123	Knowledge of system and application	Vulnerabilities Assessment	Describe common
Rochester Institute of	N/A	Elective	CSEC461	400	146	Knowledge of the types of Intrusion	Computer Network Defense	Describe and discuss various
Rochester Institute of	N/A	Elective	CSEC461	400	150	Knowledge of what constitutes a network	Information Systems/Network	Recognize and discuss the
Rochester Institute of	N/A	Elective	CSEC461	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	Describe and discuss various
Rochester Institute of	N/A	Elective	CSEC461	400	181	Skill in detecting host and network based	Computer Network Defense	Describe and discuss various
Rochester Institute of	N/A	Elective	CSEC461	400	210	Skill in mimicking threat behaviors	Computer Network Defense	Describe and discuss various
Rochester Institute of	N/A	Elective	CSEC461	400	225	Skill in the use of penetration testing	Vulnerabilities Assessment	Describe and discuss various
Rochester Institute of	N/A	Elective	CSEC461	400	274	Knowledge of concepts, principles,	Computer Network Defense	Describe and discuss various
Rochester Institute of	N/A	Elective	CSEC461	400	285	Knowledge of evasion strategies and	Computer Network Defense	Describe and discuss various
Rochester Institute of	N/A	Elective	CSEC461	400	321	Knowledge of products and	Technology Awareness	Describe common
Rochester Institute of	N/A	Elective	CSEC461	400	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	Describe and discuss various
Rochester Institute of	N/A	Elective	CSEC461	400	895	Skill in recognizing and categorizing	Information Assurance	Describe common
Rochester Institute of	N/A	Elective	CSEC461	400	952	Knowledge of emerging security	Technology Awareness	Describe common
Rochester Institute of	N/A	Elective	CSEC461	400	990	Knowledge of common attack	Computer Network Defense	Describe common
Rochester Institute of	N/A	Elective	CSEC461	400	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	Describe common
Rochester Institute of	N/A	Elective	CSEC461	400	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Recognize and discuss the
Rochester Institute of	N/A	Elective	CSEC461	400	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Recognize and discuss the
Rochester Institute of	N/A	Elective	GCCISCSEC4	400	890	Skill in conducting forensic analyses in	Computer Forensics	Discuss the fundamental

Rochester Institute of	B.S.	Networking and Systems	CSEC 464	400	19	Knowledge of Computer Network	Computer Network Defense	7.3 Demonstrate ability to identify
Rochester Institute of	B.S.	Networking and Systems	CSEC 464	400	59	Knowledge of Intrusion Detection	Computer Network Defense	7.3 Demonstrate ability to identify
Rochester Institute of	B.S.	Networking and Systems	CSEC 464	400	60	Knowledge of incident categories, incident	Incident Management	7.4 Describe the basic procedures
Rochester Institute of	B.S.	Networking and Systems	CSEC 464	400	61	Knowledge of incident response and	Incident Management	7.4 Describe the basic procedures
Rochester Institute of	B.S.	Networking and Systems	CSEC 464	400	379	Skill in using common digital forensics tools	Computer Forensics	7.1 Discuss the fundamental
Rochester Institute of	B.S.	Networking and Systems	CSEC 464	400	381	Skill in using forensic tool suites (e.g.	Computer Forensics	7.5 Utilize available forensic
Rochester Institute of	B.S.	Networking and Systems	CSEC 464	400	966	Knowledge of enterprise incident	Incident Management	7.4 Describe the basic procedures
Rochester Institute of	B.S.	Networking and Systems	CSEC 464	400	1093	Knowledge of common forensic tool	Computer Forensics	7.5 Utilize available forensic
Rochester Institute of	B.S.	Networking and Systems	CSEC 465	400	70	Knowledge of information	Information Systems/Network	7.2 Describe the basic design and
Rochester Institute of	B.S.	Networking and Systems	CSEC 465	400	95	Knowledge of penetration testing	Vulnerabilities Assessment	7.4 Utilize available tools to
Rochester Institute of	B.S.	Networking and Systems	CSEC 465	400	225	Skill in the use of penetration testing	Vulnerabilities Assessment	7.4 Utilize available tools to
Rochester Institute of	B.S.	Networking and Systems	CSEC 465	400	322	Knowledge of router and routing	Infrastructure Design	7.2 Describe the basic design and
Rochester Institute of	B.S.	Networking and Systems	CSEC 465	400	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	7.1 Explain the fundamental
Rochester Institute of	B.S.	Networking and Systems	CSEC 465	400	892	Skill in configuring and utilizing	Configuration Management	7.2 Describe the basic design and
Rochester Institute of	B.S.	Networking and Systems	CSEC 465	400	985	Skill in configuring and utilizing network	Configuration Management	7.2 Describe the basic design and
Rochester Institute of	B.S.	Networking and Systems	CSEC 465	400	1002	Skill in conducting audits or reviews of	Information Technology	7.1 Explain the fundamental
Rochester Institute of	B.S.	Networking and Systems	CSEC 465	400	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	7.4 Utilize available tools to
Rochester Institute of	B.S.	Networking and Systems	CSEC 466	400	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	7.6 Explain various
Rochester Institute of	B.S.	Networking and Systems	CSEC 466	400	274	Knowledge of concepts, principles,	Computer Network Defense	7.6 Explain various
Rochester Institute of	B.S.	Networking and Systems	CSEC 466	400	892	Skill in configuring and utilizing	Configuration Management	7.2 Compare different types
Rochester Institute of	B.S.	Computing Security	NSSA 242	200	72	Knowledge of local area network (LAN)	Infrastructure Design	Demonstrate understanding of
Rochester Institute of	B.S.	Computing Security	NSSA 242	200	98	Knowledge of policybased and risk	Identity Management	maybe knowledge?
Rochester Institute of	B.S.	Computing Security	NSSA 242	200	278	Knowledge of different types of	Telecommunicatio ns	1. Explain theoretical
Rochester Institute of	B.S.	Computing Security	NSSA 242	200	903	Knowledge of Wireless Fidelity	Network Management	1. Explain theoretical
Rochester Institute of	B.S.	Computing Security	CSCI 250	200	42	Knowledge of electrical engineering	Hardware Engineering	The student will be able to outline
Rochester Institute of	B.S.	Computing Security	CSCI 250	200	68	Knowledge of information	Information Technology	The student will be able to outline
Rochester Institute of	B.S.	Computing Security	CSCI 250	200	74	Knowledge of low level computer	Computer Languages	The student will be able to design,
Rochester Institute of	B.S.	Computing Security	CSCI 250	200	141	Knowledge of the enterprise	Information Technology	The student will be able to outline
Rochester Institute of	B.S.	Computing Security	CSCI 250	200	264	Knowledge of basic physical computer	Computers and Electronics	The student will be able to outline
Rochester Institute of	B.S.	Computing Security	GCCISCSEC3	300	37	Knowledge of disaster recovery and	Incident Management	Identify the major components of a

Rochester Institute of	B.S.	Computing Security	GCCISCSEC3	300	60	Knowledge of incident categories, incident	Incident Management	Explain the composition of an
Rochester Institute of	B.S.	Computing Security	GCCISCSEC3	300	61	Knowledge of incident response and	Incident Management	Explain the composition of an
Rochester Institute of	B.S.	Computing Security	GCCISCSEC3	300	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	Perform a security policy
Rochester Institute of	B.S.	Computing Security	GCCISCSEC3	300	305	Knowledge of laws that affect cyber	Forensics	Develop an electronic
Rochester Institute of	B.S.	Computing Security	GCCISCSEC3	300	901	Knowledge of the capabilities of	Network Management	Develop an electronic
Rochester Institute of	B.S.	Computing Security	GCCISCSEC3	300	966	Knowledge of enterprise incident	Incident Management	Explain the composition of an
Rochester Institute of	B.S.	Computing Security	GCCISCSEC3	300	1034	Knowledge of Personally Identifiable	Security	Explain different security
Rochester Institute of	B.S.	Computing Security	GCCISCSEC4	400	8	Knowledge of access authentication	Identity Management	7.2 Identify standards as they
Rochester Institute of	B.S.	Computing Security	GCCISCSEC4	400	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	7.3 Identify major applications of
Rochester Institute of	B.S.	Computing Security	GCCISCSEC4	400	35	Knowledge of digital rights management	Encryption	7.2 Identify standards as they
Rochester Institute of	B.S.	Computing Security	GCCISCSEC4	400	284	Knowledge of encryption algorithms	Cryptography	7.1 Describe the foundations and
Rochester Institute of	B.S.	Computing Security	GCCISCSEC4	400	1114	Knowledge of encryption	Cryptography	7.1 Describe the foundations and
Rochester Institute of	B.S.	Computing Security	ISTE 230	200	32	Knowledge of database	Database Management	7.1 Read and interpret an
Rochester Institute of	B.S.	Computing Security	ISTE 230	200	34	Knowledge of database systems	Database Management	7.1 Read and interpret an
Rochester Institute of	B.S.	Computing Security	ISTE 230	200	104	Knowledge of query languages such as	Database Management	7.3 Implement a relational model
Rochester Institute of	B.S.	Computing Security	ISTE 230	200	166	Skill in conducting queries and	Database Management	7.4 Apply relational algebra
Rochester Institute of	N/A	Elective	CSEC462	400	19	Knowledge of Computer Network	Computer Network Defense	Employ various tools to assess
Rochester Institute of	N/A	Elective	CSEC462	400	38	Knowledge of organization's	Information Assurance	Recognize and discuss network
Rochester Institute of	N/A	Elective	CSEC462	400	59	Knowledge of Intrusion Detection	Computer Network Defense	Employ various tools to assess
Rochester Institute of	N/A	Elective	CSEC462	400	66	Knowledge of intrusion detection	Computer Network Defense	Describe the attributes
Rochester Institute of	N/A	Elective	CSEC462	400	111	Knowledge of security system design tools,	Information Systems/Network	Describe the attributes
Rochester Institute of	N/A	Elective	CSEC462	400	146	Knowledge of the types of Intrusion	Computer Network Defense	Describe the attributes
Rochester Institute of	N/A	Elective	CSEC462	400	225	Skill in the use of penetration testing	Vulnerabilities Assessment	Employ various tools to assess
Rochester Institute of	N/A	Elective	CSEC462	400	231	Skill in using network management tools to	Network Management	Employ various tools to assess
Rochester Institute of	N/A	Elective	CSEC462	400	271	Knowledge of common network	Infrastructure Design	Employ various tools to assess
Rochester Institute of	N/A	Elective	CSEC462	400	274	Knowledge of concepts, principles,	Computer Network Defense	Describe the attributes
Rochester Institute of	N/A	Elective	CSEC462	400	277	Knowledge of defense indepth principles and	Computer Network Defense	Recognize and discuss network
Rochester Institute of	N/A	Elective	CSEC462	400	892	Skill in configuring and utilizing	Configuration Management	Employ various tools to assess
Rochester Institute of	N/A	Elective	CSEC462	400	922	Skill in using network analysis tools to	Vulnerabilities Assessment	Employ various tools to assess
Rochester Institute of	N/A	Elective	CSEC462	400	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	Employ various tools to assess

Rochester Institute of	N/A	Elective	CSEC462	400	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	Employ various tools to assess
Rochester Institute of	N/A	Elective	CSEC462	400	1096	Knowledge of malware analysis	Computer Network Defense	Employ various tools to assess
Rochester Institute of	B.S.	Computing Security	CSCI 141	100	20	Knowledge of complex data	Object Technology	7.2 The student will describe and
Rochester Institute of	B.S.	Computing Security	CSCI 141	100	21	Knowledge of computer algorithms	Mathematical Reasoning	7.2 The student will describe and
Rochester Institute of	B.S.	Computing Security	CSCI 141	100	23	Knowledge of computer	Object Technology	7.3 The student will describe the
Rochester Institute of	B.S.	Computing Security	CSCI 141	100	102	Knowledge of programming	Computer Languages	7.3 The student will describe the
Rochester Institute of	B.S.	Computing Security	CSCI 141	100	383	Skill in using scientific rules and methods to	Reasoning	7.1 The student will describe and
Rochester Institute of	B.S.	Computing Security	CSCI 243	200	21	Knowledge of computer algorithms	Mathematical Reasoning	7.1 The student will be able to
Rochester Institute of	B.S.	Computing Security	CSCI 243	200	23	Knowledge of computer	Object Technology	7.1 The student will be able to
Rochester Institute of	B.S.	Computing Security	CSCI 243	200	102	Knowledge of programming	Computer Languages	7.1 The student will be able to
Rochester Institute of	B.S.	Computing Security	CSEC 101	100	66	Knowledge of intrusion detection	Computer Network Defense	7.3 Describe the attributes
Rochester Institute of	B.S.	Computing Security	CSEC 101	100	274	Knowledge of concepts, principles,	Computer Network Defense	7.1 Recognize and discuss the
Rochester Institute of	B.S.	Computing Security	CSEC 101	100	282	Knowledge of emerging	Technology Awareness	7.1 Recognize and discuss the
Rochester Institute of	B.S.	Networking and Systems	CSEC 210	200	19	Knowledge of Computer Network	Computer Network Defense	7.6 Describe how to prepare and
Rochester Institute of	B.S.	Networking and Systems	CSEC 210	200	55	Knowledge of Information	Information Assurance	7.3 Identify the risks associated
Rochester Institute of	B.S.	Networking and Systems	CSEC 210	200	60	Knowledge of incident categories, incident	Incident Management	7.7 Explain the appropriate
Rochester Institute of	B.S.	Networking and Systems	CSEC 210	200	61	Knowledge of incident response and	Incident Management	7.7 Explain the appropriate
Rochester Institute of	B.S.	Networking and Systems	CSEC 210	200	108	Knowledge of risk management	Risk Management	7.3 Identify the risks associated
Rochester Institute of	B.S.	Networking and Systems	CSEC 210	200	285	Knowledge of evasion strategies and	Computer Network Defense	7.6 Describe how to prepare and
Rochester Institute of	B.S.	Networking and Systems	CSEC 210	200	302	Knowledge of investigative	Computer Forensics	7.1 discuss the history and
Rochester Institute of	B.S.	Networking and Systems	CSEC 210	200	305	Knowledge of laws that affect cyber	Forensics	7.1 discuss the history and
Rochester Institute of	B.S.	Networking and Systems	CSEC 210	200	896	Skill in protecting a network against	Computer Network Defense	7.6 Describe how to prepare and
Rochester Institute of	B.S.	Networking and Systems	CSEC 210	200	917	Knowledge of social dynamics of computer	External Awareness	7.4 Describe the potential
Rochester Institute of	B.S.	Networking and Systems	CSEC 210	200	966	Knowledge of enterprise incident	Incident Management	7.7 Explain the appropriate
Rochester Institute of	B.S.	Computing Security, B.S.	NSSA 221	200	8	Knowledge of access authentication	Identity Management	7.4 Discuss service
Rochester Institute of	B.S.	Computing Security, B.S.	NSSA 221	200	63	Knowledge of Information	Information Assurance	7.4 Discuss service
Rochester Institute of	B.S.	Computing Security, B.S.	NSSA 221	200	287	Knowledge of file system	Operating Systems	7.2 Describe the following as they
Rochester Institute of	B.S.	Computing Security, B.S.	NSSA 221	200	341	Knowledge of UNIX and Windows systems	Operating Systems	7.4 Discuss service
Rochester Institute of	B.S.	Computing Security	NSSA 241	200	12	Knowledge of communication	Infrastructure Design	3. Be able to explain the basic
Rochester Institute of	B.S.	Computing Security	NSSA 241	200	15	Knowledge of capabilities and	Hardware	3. Be able to explain the basic

Rochester Institute of	B.S.	Computing Security	NSSA 241	200	81	Knowledge of network	Infrastructure Design	Be able to explain the operation and
Rochester Institute of	B.S.	Computing Security	NSSA 241	200	92	Knowledge of how traffic flows across	Infrastructure Design	Be able to explain the operation and
Rochester Institute of	B.S.	Computing Security	NSSA 241	200	139	Knowledge of common networking	Infrastructure Design	Be able to explain the operation and
Rochester Institute of	B.S.	Computing Security	NSSA 241	200	198	Skill in establishing a routing schema	Infrastructure Design	2.Be able to explain the
Rochester Institute of	B.S.	Computing Security	NSSA 241	200	322	Knowledge of router and routing	Infrastructure Design	2.Be able to explain the
Rochester Institute of	B.S.	Computing Security	NSSA 241	200	1121	Knowledge of Windows/Unix ports	Operating Systems	5. Explain the Spanning Tree
Rose State College	Certifica	Information Security Program	CIT2513	200	10	Knowledge of application	Vulnerabilities Assessment	Hardware, software, input,
Rose State College	Certifica	Information Security Program	CIT2513	200	37	Knowledge of disaster recovery and	Incident Management	Contingency planning and
Rose State College	Certifica	Information Security Program	CIT2513	200	49	Knowledge of host/network access	Information Systems/Network	Discretionary, mandatory and
Rose State College	Certifica	Information Security Program	CIT2513	200	79	Knowledge of network access,	Identity Management	Public Key Infrastructure
Rose State College	Certifica	Information Security Program	CIT2513	200	98	Knowledge of policybased and risk	Identity Management	Policy creation, enforcement and
Rose State College	Certifica	Information Security Program	CIT2513	200	108	Knowledge of risk management	Risk Management	Risk management and assessment
Rose State College	Certifica	Information Security Program	CIT2513	200	123	Knowledge of system and application	Vulnerabilities Assessment	Hardware, software, input,
Rose State College	Certifica	Information Security Program	CIT2513	200	137	Knowledge of the characteristics of	Data Management	Concurrent access to storage
Rose State College	Certifica	Information Security Program	CIT2513	200	145	Knowledge of the type and frequency of	Systems Life Cycle	system development and
Rose State College	Certifica	Information Security Program	CIT2513	200	150	Knowledge of what constitutes a network	Information Systems/Network	Threat identification,
Rose State College	Certifica	Information Security Program	CIT2513	200	157	Skill in applying host/network access	Identity Management	Discretionary, mandatory and
Rose State College	Certifica	Information Security Program	CIT2513	200	305	Knowledge of laws that affect cyber	Forensics	Cyber Law and ethics;Uniform
Rose State College	Certifica	Information Security Program	CIT2513	200	967	Knowledge of current and emerging	Information Systems/Network	Threat identification,
Rose State College	Certifica	Information Security Program	CIT2513	200	986	Knowledge of organizational	Identity Management	Discretionary, mandatory and
Rose State College	Certifica	Information Security Program	CIT2513	200	1021	Knowledge of threat assessment	Risk Management	Threat identification,
Rose State College	Certifica	Information Security Program	CIT2513	200	1061	Knowledge of the lifecycle process	Systems Life Cycle	System life cycles, trusts and modes
Rose State College	Certifica	Information Security Program	CIT2523	200	37	Knowledge of disaster recovery and	Incident Management	Contingency planning;
Rose State College	Certifica	Information Security Program	CIT2523	200	60	Knowledge of incident categories, incident	Incident Management	Contingency planning;
Rose State College	Certifica	Information Security Program	CIT2523	200	61	Knowledge of incident response and	Incident Management	Contingency planning;
Rose State College	Certifica	Information Security Program	CIT2523	200	966	Knowledge of enterprise incident	Incident Management	Contingency planning;
Rose State College	Certifica	Information Security Program	CIT 2533	200	9	Knowledge of applicable business	Requirements Analysis	describe business issues in
Rose State College	Certifica	Information Security Program	CIT 2533	200	252	Knowledge of and experience in Insider	Computer Network Defense	describe ebusiness and
Rose State College	Certifica	Information Security Program	CIT 2533	200	305	Knowledge of laws that affect cyber	Forensics	describe ebusiness and
Rose State College	Certifica	Information Security Program	CIT 2533	200	310	Knowledge of legal governance related to	Criminal Law	identify internet and computer

Rose State College	Certifica	Information Security Program	CIT 2533	200	316	Knowledge of processes for	Criminal Law	describe ebusiness and
Rose State College	Certifica	Information Security Program	CIT 2533	200	981	Knowledge of International Traffic in	Criminal Law	describe ebusiness and
Rose State College	Certifica	Information Security Program	CIT 2533	200	982	Knowledge of electronic evidence	Criminal Law	describe ebusiness and
Rose State College	Certifica	Information Security Program	CIT 2533	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	describe ebusiness and
Rose State College	Certifica	Information Security Program	CIT 2533	200	1040	Knowledge of relevant laws,	Criminal Law	describe ebusiness and
Rose State College	Certifica	Information Security Program	CIT 2533	200	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	describe ebusiness and
Rose State College	Certifica	Information Security Program	CIT 2543	200	8	Knowledge of access authentication	Identity Management	identify access controls to
Rose State College	Certifica	Information Security Program	CIT 2543	200	32	Knowledge of database	Database Management	Disucss media handling,
Rose State College	Certifica	Information Security Program	CIT 2543	200	35	Knowledge of digital rights management	Encryption	describe ethical issues including
Rose State College	Certifica	Information Security Program	CIT 2543	200	55	Knowledge of Information	Information Assurance	discuss transmission
Rose State College	Certifica	Information Security Program	CIT 2543	200	56	Knowledge of information assurance	Information Assurance	discuss software security
Rose State College	Certifica	Information Security Program	CIT 2543	200	60	Knowledge of incident categories, incident	Incident Management	discuss incident identification and
Rose State College	Certifica	Information Security Program	CIT 2543	200	61	Knowledge of incident response and	Incident Management	discuss incident identification and
Rose State College	Certifica	Information Security Program	CIT 2543	200	63	Knowledge of Information	Information Assurance	discuss confidentiality,
Rose State College	Certifica	Information Security Program	CIT 2543	200	77	Knowledege of current industry	Information Systems/Network	evaluate assurance and
Rose State College	Certifica	Information Security Program	CIT 2543	200	98	Knowledge of policybased and risk	Identity Management	identify access controls to
Rose State College	Certifica	Information Security Program	CIT 2543	200	110	Knowledge of security management	Information Assurance	Security Management
Rose State College	Certifica	Information Security Program	CIT 2543	200	129	Knowledge of systems lifecycle management	Systems Life Cycle	discuss software security
Rose State College	Certifica	Information Security Program	CIT 2543	200	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	Security Testing and evaluation.
Rose State College	Certifica	Information Security Program	CIT 2543	200	205	Skill in implementing, maintaining, and	Information Systems/Network	Records Management to
Rose State College	Certifica	Information Security Program	CIT 2543	200	229	Skill in using incident handling	Incident Management	discuss incident identification and
Rose State College	Certifica	Information Security Program	CIT 2543	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	evaluate auditing and monitoring
Rose State College	Certifica	Information Security Program	CIT 2543	200	950	Skill in evaluating test plans for applicability	Systems Testing and Evaluation	Security Testing and evaluation.
Rose State College	Certifica	Information Security Program	CIT 2543	200	978	Knowledge of root cause analysis for	Incident Management	discuss incident identification and
Rose State College	Certifica	Information Security Program	CIT 2543	200	980	Skill in performing root cause analysis for	Incident Management	discuss incident identification and
Rose State College	Certifica	Information Security Program	CIT 2543	200	986	Knowledge of organizational	Identity Management	identify access controls to
Rose State College	Certifica	Information Security Program	CIT 2543	200	1011	Knowledge of processes for	Security	
Rose State College	Certifica	Information Security Program	CIT 2543	200	1087	Skill in deep analysis of captured malicious	Computer Network Defense	identify malicious logic
Rose State College	Certifica	Information Security Program	CIT 2553	200	20	Knowledge of complex data	Object Technology	data structures
Rose State College	Certifica	Information Security Program	CIT 2553	200	29	Knowledge of data backup, types of	Computer Forensics	data recovery

Rose State College	Certifica	Information Security Program	CIT 2553	200	166	Skill in conducting queries and	Database Management	data structures
Rose State College	Certifica	Information Security Program	CIT 2553	200	217	Skill in preserving evidence integrity	Computer Forensics	identify digital evidence
Rose State College	Certifica	Information Security Program	CIT 2553	200	287	Knowledge of file system	Operating Systems	identify file systems.
Rose State College	Certifica	Information Security Program	CIT 2553	200	290	Knowledge of processes for seizing	Forensics	identify digital evidence
Rose State College	Certifica	Information Security Program	CIT 2553	200	294	Knowledge of hacking methodologies in	Surveillance	Windows security measures
Rose State College	Certifica	Information Security Program	CIT 2553	200	302	Knowledge of investigative	Computer Forensics	describe computer
Rose State College	Certifica	Information Security Program	CIT 2553	200	310	Knowledge of legal governance related to	Criminal Law	identify digital evidence
Rose State College	Certifica	Information Security Program	CIT 2553	200	316	Knowledge of processes for	Criminal Law	identify digital evidence
Rose State College	Certifica	Information Security Program	CIT 2553	200	346	Knowledge of which system files (e.g. log	Computer Forensics	Windows security measures
Rose State College	Certifica	Information Security Program	CIT 2553	200	347	Knowledge of Windows command	Operating Systems	Windows Security Measures
Rose State College	Certifica	Information Security Program	CIT 2553	200	381	Skill in using forensic tool suites (e.g.	Computer Forensics	identify digital evidence
Rose State College	Certifica	Information Security Program	CIT 2553	200	888	Knowledge of types of digital forensics data	Computer Forensics	identify digital evidence
Rose State College	Certifica	Information Security Program	CIT 2553	200	889	Knowledge of deployable forensics	Computer Forensics	describe investigation
Rose State College	Certifica	Information Security Program	CIT 2553	200	986	Knowledge of organizational	Identity Management	password protection/exploi
Rose State College	Certifica	Information Security Program	CIT 2553	200	1121	Knowledge of Windows/Unix ports	Operating Systems	Linux/Unix security
Rose State College	Certifica	Information Security Program	CIT2563	200	27	Knowledge of cryptology	Cryptography	examine cryptography
Rose State College	Certifica	Information Security Program	CIT2563	200	49	Knowledge of host/network access	Information Systems/Network	verify contents of user registries
Rose State College	Certifica	Information Security Program	CIT2563	200	66	Knowledge of intrusion detection	Computer Network Defense	intrusion methods and
Rose State College	Certifica	Information Security Program	CIT2563	200	70	Knowledge of information	Information Systems/Network	define security Commuication
Rose State College	Certifica	Information Security Program	CIT2563	200	79	Knowledge of network access,	Identity Management	discuss key management as it
Rose State College	Certifica	Information Security Program	CIT2563	200	98	Knowledge of policybased and risk	Identity Management	policy management and
Rose State College	Certifica	Information Security Program	CIT2563	200	123	Knowledge of system and application	Vulnerabilities Assessment	identify threats, vulnerabilities,
Rose State College	Certifica	Information Security Program	CIT2563	200	129	Knowledge of systems lifecycle management	Systems Life Cycle	life cycles, trusts, modes, and
Rose State College	Certifica	Information Security Program	CIT2563	200	277	Knowledge of defense indepth principles and	Computer Network Defense	describe methods of
Rose State College	Certifica	Information Security Program	CIT2563	200	966	Knowledge of enterprise incident	Incident Management	personnel roles and
Rose State College	Certifica	Information Security Program	CIT2563	200	1061	Knowledge of the lifecycle process	Systems Life Cycle	life cycles, trusts, modes, and
Rose State College	Certifica	Information Security Program	CIT2563	200	1114	Knowledge of encryption	Cryptography	examine encryption and
Rose State College	Certifica	Information Security Program	CIT 2573	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Performance of vulnerability
Rose State College	Certifica	Information Security Program	CIT 2573	200	4	Ability to identify systemic security	Vulnerabilities Assessment	Performance of vulnerability
Rose State College	Certifica	Information Security Program	CIT 2573	200	8	Knowledge of access authentication	Identity Management	Discuss Availability/Integr

Rose State College	Certifica	Information Security Program	CIT 2573	200	10	Knowledge of application	Vulnerabilities Assessment	Performance of vulnerability
Rose State College	Certifica	Information Security Program	CIT 2573	200	38	Knowledge of organization's	Information Assurance	Define Security Architecture
Rose State College	Certifica	Information Security Program	CIT 2573	200	40	Knowledge of organization's	Systems Testing and Evaluation	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	41	Knowledge of organization's Local	Infrastructure Design	WAN security policies
Rose State College	Certifica	Information Security Program	CIT 2573	200	51	Knowledge of how system components	Systems Integration	system development and
Rose State College	Certifica	Information Security Program	CIT 2573	200	62	Knowledge of industrystandard and	Logical Systems Design	discuss skills need to perform
Rose State College	Certifica	Information Security Program	CIT 2573	200	63	Knowledge of Information	Information Assurance	Discuss Availability/Integr
Rose State College	Certifica	Information Security Program	CIT 2573	200	70	Knowledge of information	Information Systems/Network	evaluate deploying
Rose State College	Certifica	Information Security Program	CIT 2573	200	72	Knowledge of local area network (LAN)	Infrastructure Design	WAN security policies
Rose State College	Certifica	Information Security Program	CIT 2573	200	76	Knowledge of measures or	Information Technology	system development and
Rose State College	Certifica	Information Security Program	CIT 2573	200	77	Knowledege of current industry	Information Systems/Network	explain security implementations
Rose State College	Certifica	Information Security Program	CIT 2573	200	87	Knowledge of network traffic	Information Systems/Network	discuss skills need to perform
Rose State College	Certifica	Information Security Program	CIT 2573	200	93	Knowledge of packetlevel analysis	Vulnerabilities Assessment	discuss skills need to perform
Rose State College	Certifica	Information Security Program	CIT 2573	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	108	Knowledge of risk management	Risk Management	describe risk management and
Rose State College	Certifica	Information Security Program	CIT 2573	200	111	Knowledge of security system design tools,	Information Systems/Network	system development and
Rose State College	Certifica	Information Security Program	CIT 2573	200	121	Knowledge of structured analysis	Logical Systems Design	discuss skills need to perform
Rose State College	Certifica	Information Security Program	CIT 2573	200	123	Knowledge of system and application	Vulnerabilities Assessment	Performance of vulnerability
Rose State College	Certifica	Information Security Program	CIT 2573	200	124	Knowledge of system design tools,	Logical Systems Design	system development and
Rose State College	Certifica	Information Security Program	CIT 2573	200	126	Knowledge of system software and	Requirements Analysis	system development and
Rose State College	Certifica	Information Security Program	CIT 2573	200	128	Knowledge of systems diagnostic tools and	Systems Testing and Evaluation	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	133	Knowledge of telecommunications	Telecommunicatio ns	describe policy requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	142	Knowledge of the operations and	Systems Life Cycle	system development and
Rose State College	Certifica	Information Security Program	CIT 2573	200	150	Knowledge of what constitutes a network	Information Systems/Network	Performance of vulnerability
Rose State College	Certifica	Information Security Program	CIT 2573	200	156	Skill in applying confidentiality,	Information Assurance	Discuss Availability/Integr
Rose State College	Certifica	Information Security Program	CIT 2573	200	158	Skill in applying organizationspecific	Systems Testing and Evaluation	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	Performance of vulnerability
Rose State College	Certifica	Information Security Program	CIT 2573	200	169	Skill in conducting test events	Systems Testing and Evaluation	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	Performance of vulnerability

Rose State College	Certifica	Information Security Program	CIT 2573	200	182	Skill in determining an appropriate level of	Systems Testing and Evaluation	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	183	Skill in determining how a security system	Information Assurance	system development and
Rose State College	Certifica	Information Security Program	CIT 2573	200	190	Skill in developing operationsbased	Systems Testing and Evaluation	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	191	Skill in developing and applying security	Identity Management	system development and
Rose State College	Certifica	Information Security Program	CIT 2573	200	193	Skill in developing, testing, and	Information Assurance	explain security implementations
Rose State College	Certifica	Information Security Program	CIT 2573	200	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	Performance of vulnerability
Rose State College	Certifica	Information Security Program	CIT 2573	200	202	Skill in identifying and anticipating server	Information Technology	Discuss Availability/Integr
Rose State College	Certifica	Information Security Program	CIT 2573	200	203	Skill in identifying measures or	Information Technology	system development and
Rose State College	Certifica	Information Security Program	CIT 2573	200	204	Skill in identifying possible causes of	Systems Life Cycle	system development and
Rose State College	Certifica	Information Security Program	CIT 2573	200	205	Skill in implementing, maintaining, and	Information Systems/Network	describe security practices
Rose State College	Certifica	Information Security Program	CIT 2573	200	207	Skill in installing, configuring, and		WAN security policies
Rose State College	Certifica	Information Security Program	CIT 2573	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	discuss skills need to perform
Rose State College	Certifica	Information Security Program	CIT 2573	200	217	Skill in preserving evidence integrity	Computer Forensics	Discuss Availability/Integr
Rose State College	Certifica	Information Security Program	CIT 2573	200	220	Skill in systems integration testing	Systems Testing and Evaluation	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	221	Skill in testing and configuring network	Network Management	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	239	Skill in writing test plans	Systems Testing and Evaluation	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	261	Knowledge of basic concepts,	Telecommunicatio ns	describe policy requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	277	Knowledge of defense indepth principles and	Computer Network Defense	Define Security Architecture
Rose State College	Certifica	Information Security Program	CIT 2573	200	278	Knowledge of different types of	Telecommunicatio ns	describe policy requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	300	Knowledge of intelligence reporting	Organizational Awareness	identify national COMSEC policy
Rose State College	Certifica	Information Security Program	CIT 2573	200	321	Knowledge of products and	Technology Awareness	discuss vendor cooperation
Rose State College	Certifica	Information Security Program	CIT 2573	200	341	Knowledge of UNIX and Windows systems	Operating Systems	evaluate deploying
Rose State College	Certifica	Information Security Program	CIT 2573	200	348	Knowledge of wireless network collection	Cryptography	Wireless security Policy
Rose State College	Certifica	Information Security Program	CIT 2573	200	357	Skill in determining the effects of various	Configuration Management	WAN security policies
Rose State College	Certifica	Information Security Program	CIT 2573	200	359	Skill in developing and executing technical	Computer Forensics	Education, Training and
Rose State College	Certifica	Information Security Program	CIT 2573	200	360	Skill in identifying and extracting data of	Computer Forensics	Performance of vulnerability
Rose State College	Certifica	Information Security Program	CIT 2573	200	375	Skill in survey, collection, and	Network Management	discuss skills need to perform
Rose State College	Certifica	Information Security Program	CIT 2573	200	385	Skill in using traceroute analysis	Network Management	discuss skills need to perform
Rose State College	Certifica	Information Security Program	CIT 2573	200	387	Skill in verifying the integrity of encrypted	Encryption	Discuss Availability/Integr

Rose State College	Certifica	Information Security Program	CIT 2573	200	886	Skill in wireless network target	Vulnerabilities Assessment	Performance of vulnerability
Rose State College	Certifica	Information Security Program	CIT 2573	200	891	Skill in configuring and utilizing	Configuration Management	evaluate deploying
Rose State College	Certifica	Information Security Program	CIT 2573	200	892	Skill in configuring and utilizing	Configuration Management	evaluate deploying
Rose State College	Certifica	Information Security Program	CIT 2573	200	895	Skill in recognizing and categorizing	Information Assurance	Performance of vulnerability
Rose State College	Certifica	Information Security Program	CIT 2573	200	902	Knowledge of the range of existing	Network Management	WAN security policies
Rose State College	Certifica	Information Security Program	CIT 2573	200	918	Ability to prepare and deliver education and	Teaching Others	Network Security Policies
Rose State College	Certifica	Information Security Program	CIT 2573	200	922	Skill in using network analysis tools to	Vulnerabilities Assessment	discuss skills need to perform
Rose State College	Certifica	Information Security Program	CIT 2573	200	950	Skill in evaluating test plans for applicability	Systems Testing and Evaluation	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	952	Knowledge of emerging security	Technology Awareness	Performance of vulnerability
Rose State College	Certifica	Information Security Program	CIT 2573	200	965	Knowledge of organization's risk	Risk Management	describe risk management and
Rose State College	Certifica	Information Security Program	CIT 2573	200	966	Knowledge of enterprise incident	Incident Management	discuss roles and responsibilities
Rose State College	Certifica	Information Security Program	CIT 2573	200	975	Skill in integrating black box security	Quality Assurance	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	978	Knowledge of root cause analysis for	Incident Management	discuss skills need to perform
Rose State College	Certifica	Information Security Program	CIT 2573	200	979	Knowledge of supply chain risk	Risk Management	describe risk management and
Rose State College	Certifica	Information Security Program	CIT 2573	200	980	Skill in performing root cause analysis for	Incident Management	discuss skills need to perform
Rose State College	Certifica	Information Security Program	CIT 2573	200	985	Skill in configuring and utilizing network	Configuration Management	evaluate deploying
Rose State College	Certifica	Information Security Program	CIT 2573	200	986	Knowledge of organizational	Identity Management	identify national COMSEC policy
Rose State College	Certifica	Information Security Program	CIT 2573	200	989	Knowledge of Voice over Internet Protocol	Telecommunications	describe policy requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	993	Knowledge of the methods, standards,	Enterprise Architecture	discuss appraising the maintenance
Rose State College	Certifica	Information Security Program	CIT 2573	200	1020	Skill in secure test plan deisn (i.e., unit,	Systems Testing and Evaluation	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	1021	Knowledge of threat assessment	Risk Management	describe risk management and
Rose State College	Certifica	Information Security Program	CIT 2573	200	1029	Knowledge of malware analysis	Computer Network Defense	discuss skills need to perform
Rose State College	Certifica	Information Security Program	CIT 2573	200	1033	Knowledge of basic system	Information Systems/Network	system development and
Rose State College	Certifica	Information Security Program	CIT 2573	200	1037	Knowledge of information	Risk Management	describe risk management and
Rose State College	Certifica	Information Security Program	CIT 2573	200	1040	Knowledge of relevant laws,	Criminal Law	identify national COMSEC policy
Rose State College	Certifica	Information Security Program	CIT 2573	200	1052	Knowledge of Global Systems for Mobile	Telecommunications	describe policy requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	discuss skills need to perform
Rose State College	Certifica	Information Security Program	CIT 2573	200	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	identify national COMSEC policy
Rose State College	Certifica	Information Security Program	CIT 2573	200	1072	Knowledge of network security	Information Systems/Network	Define Security Architecture

Rose State College	Certifica	Information Security Program	CIT 2573	200	1074	Knowledge of transmission records	Telecommunicatio ns	describe policy requirements for
Rose State College	Certifica	Information Security Program	CIT 2573	200	1117	Skill in utilizing virtual networks for testing	Operating Systems	explain security requirements for
Rose State College	Certifica	Information Security Program	CIT 2603	200	59	Knowledge of Intrusion Detection	Computer Network Defense	Perimeter Defense / IDSs
Rose State College	Certifica	Information Security Program	CIT 2603	200	60	Knowledge of incident categories, incident	Incident Management	Incident Respond / Reconstruction
Rose State College	Certifica	Information Security Program	CIT 2603	200	61	Knowledge of incident response and	Incident Management	Incident Respond / Reconstruction
Rose State College	Certifica	Information Security Program	CIT 2603	200	66	Knowledge of intrusion detection	Computer Network Defense	Detect and defend against
Rose State College	Certifica	Information Security Program	CIT 2603	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	Penetration testing tools and
Rose State College	Certifica	Information Security Program	CIT 2603	200	146	Knowledge of the types of Intrusion	Computer Network Defense	Perimeter Defense / IDSs
Rose State College	Certifica	Information Security Program	CIT 2603	200	181	Skill in detecting host and network based	Computer Network Defense	Detect and defend against
Rose State College	Certifica	Information Security Program	CIT 2603	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	Penetration testing tools and
Rose State College	Certifica	Information Security Program	CIT 2603	200	348	Knowledge of wireless network collection	Cryptography	Wireless network analysis
Rose State College	Certifica	Information Security Program	CIT 2603	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	Security Auditing Tools and
Rose State College	Certifica	Information Security Program	CIT 2603	200	375	Skill in survey, collection, and	Network Management	Wireless network analysis
Rose State College	Certifica	Information Security Program	CIT 2603	200	922	Skill in using network analysis tools to	Vulnerabilities Assessment	Wireless network analysis
Rose State College	Certifica	Information Security Program	CIT 2603	200	966	Knowledge of enterprise incident	Incident Management	Incident Respond / Reconstruction
Rose State College	Certifica	Information Security Program	CIT 2603	200	985	Skill in configuring and utilizing network	Configuration Management	Perimeter Defense / IDSs
Rose State College	Certifica	Information Security Program	CIT 2603	200	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	penetration testing tools and
Rose State College	Certifica	Information Security Program	CIT 2603	200	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	
Rose State College	Certifica	Information Security Program	CIT 2603	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Port Scanning assessment
Rose State College	Certifica	Information Security Program	CIT 2603	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Port Scanning assessment
Rose State College	Certifica	Information Security Program	CIT 2323	200	12	Knowledge of communication	Infrastructure Design	Different Encryption
Rose State College	Certifica	Information Security Program	CIT 2323	200	22	Knowledge of computer networking	Infrastructure Design	Demonstrate the ability to design
Rose State College	Certifica	Information Security Program	CIT 2323	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	Identify and fingerprint
Rose State College	Certifica	Information Security Program	CIT 2323	200	27	Knowledge of cryptology	Cryptography	Different Encryption
Rose State College	Certifica	Information Security Program	CIT 2323	200	49	Knowledge of host/network access	Information Systems/Network	Configure access control lists
Rose State College	Certifica	Information Security Program	CIT 2323	200	50	Knowledge of how network services and	Infrastructure Design	Demonstrate the ability to design
Rose State College	Certifica	Information Security Program	CIT 2323	200	59	Knowledge of Intrusion Detection	Computer Network Defense	Configure and evaluate various
Rose State College	Certifica	Information Security Program	CIT 2323	200	61	Knowledge of incident response and	Incident Management	Demonstrate the ability to analyze
Rose State College	Certifica	Information Security Program	CIT 2323	200	62	Knowledge of industrystandard and	Logical Systems Design	Demonstrate the ability to design
Rose State College	Certifica	Information Security Program	CIT 2323	200	66	Knowledge of intrusion detection	Computer Network Defense	Configure and evaluate various

Rose State College	Certifica	Information Security Program	CIT 2323	200	70	Knowledge of information	Information Systems/Network	Configure and evaluate Firewalls
Rose State College	Certifica	Information Security Program	CIT 2323	200	81	Knowledge of network	Infrastructure Design	Identify and fingerprint
Rose State College	Certifica	Information Security Program	CIT 2323	200	82	Knowledge of network design	Infrastructure Design	Demonstrate the ability to design
Rose State College	Certifica	Information Security Program	CIT 2323	200	87	Knowledge of network traffic	Information Systems/Network	Analyze network traffic
Rose State College	Certifica	Information Security Program	CIT 2323	200	92	Knowledge of how traffic flows across	Infrastructure Design	Demonstrate the ability to design
Rose State College	Certifica	Information Security Program	CIT 2323	200	111	Knowledge of security system design tools,	Information Systems/Network	Demonstrate the ability to design
Rose State College	Certifica	Information Security Program	CIT 2323	200	121	Knowledge of structured analysis	Logical Systems Design	Demonstrate the ability to design
Rose State College	Certifica	Information Security Program	CIT 2323	200	124	Knowledge of system design tools,	Logical Systems Design	Demonstrate the ability to design
Rose State College	Certifica	Information Security Program	CIT 2323	200	126	Knowledge of system software and	Requirements Analysis	Demonstrate the ability to design
Rose State College	Certifica	Information Security Program	CIT 2323	200	139	Knowledge of common networking	Infrastructure Design	Identify and fingerprint
Rose State College	Certifica	Information Security Program	CIT 2323	200	146	Knowledge of the types of Intrusion	Computer Network Defense	Configure and evaluate various
Rose State College	Certifica	Information Security Program	CIT 2323	200	148	Knowledge of VPN security.	Encryption	Configure and evaluate Virtual
Rose State College	Certifica	Information Security Program	CIT 2323	200	154	Skill in analyzing network traffic	Capacity Management	Analyze network traffic
Rose State College	Certifica	Information Security Program	CIT 2323	200	157	Skill in applying host/network access	Identity Management	Configure access control lists
Rose State College	Certifica	Information Security Program	CIT 2323	200	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	Demonstrate the ability to design
Rose State College	Certifica	Information Security Program	CIT 2323	200	173	Skill in creating policies that relfect	Information Systems Security	Configure security policies
Rose State College	Certifica	Information Security Program	CIT 2323	200	179	Skill in designing security controls	Information Assurance	Demonstrate the ability to design
Rose State College	Certifica	Information Security Program	CIT 2323	200	181	Skill in detecting host and network based	Computer Network Defense	Configure and evaluate various
Rose State College	Certifica	Information Security Program	CIT 2323	200	205	Skill in implementing, maintaining, and	Information Systems/Network	Demonstrate the ability to design
Rose State College	Certifica	Information Security Program	CIT 2323	200	229	Skill in using incident handling	Incident Management	Demonstrate the ability to analyze
Rose State College	Certifica	Information Security Program	CIT 2323	200	231	Skill in using network management tools to	Network Management	Analyze network traffic
Rose State College	Certifica	Information Security Program	CIT 2323	200	237	Skill in using Virtual Private Network	Encryption	Configure and evaluate Virtual
Rose State College	Certifica	Information Security Program	CIT 2323	200	277	Knowledge of defense indepth principles and	Computer Network Defense	Demonstrate a basic knowledge
Rose State College	Certifica	Information Security Program	CIT 2323	200	300	Knowledge of intelligence reporting	Organizational Awareness	Configure security policies
Rose State College	Certifica	Information Security Program	CIT 2323	200	322	Knowledge of router and routing	Infrastructure Design	Demonstrate the ability to design
Rose State College	Certifica	Information Security Program	CIT 2323	200	341	Knowledge of UNIX and Windows systems	Operating Systems	Configure and evaluate Firewalls
Rose State College	Certifica	Information Security Program	CIT 2323	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	Secure audit trails from
Rose State College	Certifica	Information Security Program	CIT 2323	200	891	Skill in configuring and utilizing	Configuration Management	Configure and evaluate Firewalls
Rose State College	Certifica	Information Security Program	CIT 2323	200	892	Skill in configuring and utilizing	Configuration Management	Configure and evaluate Firewalls
Rose State College	Certifica	Information Security Program	CIT 2323	200	915	Knowledge of frontend collection	Information Systems/Network	Analyze network traffic

Rose State College	Certifica	Information Security Program	CIT 2323	200	922	Skill in using network analysis tools to	Vulnerabilities Assessment	Demonstrate the ability to analyze
Rose State College	Certifica	Information Security Program	CIT 2323	200	978	Knowledge of root cause analysis for	Incident Management	Demonstrate the ability to analyze
Rose State College	Certifica	Information Security Program	CIT 2323	200	980	Skill in performing root cause analysis for	Incident Management	Demonstrate the ability to analyze
Rose State College	Certifica	Information Security Program	CIT 2323	200	985	Skill in configuring and utilizing network	Configuration Management	Configure and evaluate Virtual
Rose State College	Certifica	Information Security Program	CIT 2323	200	993	Knowledge of the methods, standards,	Enterprise Architecture	Discuss documenting
Rose State College	Certifica	Information Security Program	CIT 2323	200	1033	Knowledge of basic system	Information Systems/Network	Demonstrate proper host
Rose State College	Certifica	Information Security Program	CIT 2323	200	1059	Knowledge of networking protocols	Infrastructure Design	Identify and fingerprint
Rose State College	Certifica	Information Security Program	CIT 2323	200	1072	Knowledge of network security	Information Systems/Network	Demonstrate a basic knowledge
Rose State College	Certifica	Information Security Program	CIT 2323	200	1114	Knowledge of encryption	Cryptography	Different Encryption
Capella University	B.S	Information Assurance and	IT 4070	400	7	Knowledge of “knowledge base”	Knowledge Management	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	8	Knowledge of access authentication	Identity Management	(2) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	12	Knowledge of communication	Infrastructure Design	(3) Develop solutions to allow
Capella University	B.S	Information Assurance and	IT 4070	400	38	Knowledge of organization's	Information Assurance	(5) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	44	Knowledge of enterprise messaging	Enterprise Architecture	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	50	Knowledge of how network services and	Infrastructure Design	(3) Develop solutions to allow
Capella University	B.S	Information Assurance and	IT 4070	400	55	Knowledge of Information	Information Assurance	(3) Develop solutions to allow
Capella University	B.S	Information Assurance and	IT 4070	400	81	Knowledge of network	Infrastructure Design	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	82	Knowledge of network design	Infrastructure Design	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	92	Knowledge of how traffic flows across	Infrastructure Design	(2) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	134	Knowledge of the capabilities and	Technology Awareness	(3) Develop solutions to allow
Capella University	B.S	Information Assurance and	IT 4070	400	136	Knowledge of the capabilities and	Technology Awareness	(3) Develop solutions to allow
Capella University	B.S	Information Assurance and	IT 4070	400	139	Knowledge of common networking	Infrastructure Design	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	198	Skill in establishing a routing schema	Infrastructure Design	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	261	Knowledge of basic concepts,	Telecommunications	(3) Develop solutions to allow
Capella University	B.S	Information Assurance and	IT 4070	400	322	Knowledge of router and routing	Infrastructure Design	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	336	Knowledge of the nature and function	Telecommunications	(5) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	899	Skill in gathering information from	Information Management	(3) Develop solutions to allow
Capella University	B.S	Information Assurance and	IT 4070	400	901	Knowledge of the capabilities of	Network Management	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	902	Knowledge of the range of existing	Network Management	(4) Identify solutions for

Capella University	B.S	Information Assurance and	IT 4070	400	1036	Knowledge of applicable laws (e.g.,	Criminal Law	(6) Describe legal and ethical
Capella University	B.S	Information Assurance and	IT 4070	400	1038	Knowledge of local specialized system	Infrastructure Design	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4070	400	1040	Knowledge of relevant laws,	Criminal Law	(6) Describe legal and ethical
Capella University	B.S	Information Assurance and	IT 4070	400	1052	Knowledge of Global Systems for Mobile	Telecommunications	(7) Communicate effectively
Capella University	B.S	Information Assurance and	IT 4070	400	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	(6) Describe legal and ethical
Capella University	B.S	Information Assurance and	IT 4070	400	1074	Knowledge of transmission records	Telecommunications	(3) Develop solutions to allow
Capella University	B.S	Information Assurance and	IT 4071	400	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	(1) Perform ethical hacking
Capella University	B.S	Information Assurance and	IT 4071	400	4	Ability to identify systemic security	Vulnerabilities Assessment	(1) Perform ethical hacking
Capella University	B.S	Information Assurance and	IT 4071	400	10	Knowledge of application	Vulnerabilities Assessment	(4) Identify the vulnerabilities of
Capella University	B.S	Information Assurance and	IT 4071	400	12	Knowledge of communication	Infrastructure Design	(4) Identify the vulnerabilities of
Capella University	B.S	Information Assurance and	IT 4071	400	17	Knowledge of certified ethical	Vulnerabilities Assessment	(1) Perform ethical hacking
Capella University	B.S	Information Assurance and	IT 4071	400	50	Knowledge of how network services and	Infrastructure Design	(4) Identify the vulnerabilities of
Capella University	B.S	Information Assurance and	IT 4071	400	59	Knowledge of Intrusion Detection	Computer Network Defense	(1) Perform ethical hacking
Capella University	B.S	Information Assurance and	IT 4071	400	66	Knowledge of intrusion detection	Computer Network Defense	(2) Describe the role of social
Capella University	B.S	Information Assurance and	IT 4071	400	95	Knowledge of penetration testing	Vulnerabilities Assessment	(1) Perform ethical hacking
Capella University	B.S	Information Assurance and	IT 4071	400	123	Knowledge of system and application	Vulnerabilities Assessment	(1) Perform ethical hacking
Capella University	B.S	Information Assurance and	IT 4071	400	146	Knowledge of the types of Intrusion	Computer Network Defense	(5) Design a plan for intrusion
Capella University	B.S	Information Assurance and	IT 4071	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	(4) identify the vulnerabilities of
Capella University	B.S	Information Assurance and	IT 4071	400	181	Skill in detecting host and network based	Computer Network Defense	(1) Perform ethical hacking
Capella University	B.S	Information Assurance and	IT 4071	400	193	Skill in developing, testing, and	Information Assurance	(5) Design a plan for intrusion
Capella University	B.S	Information Assurance and	IT 4071	400	225	Skill in the use of penetration testing	Vulnerabilities Assessment	(1) Perform ethical hacking
Capella University	B.S	Information Assurance and	IT 4071	400	226	Skill in the use of social engineering	Human Factors	(2) Describe the role of social
Capella University	B.S	Information Assurance and	IT 4071	400	233	Skill in using protocol analyzers	Vulnerabilities Assessment	(4) Identify the vulnerabilities of
Capella University	B.S	Information Assurance and	IT 4071	400	261	Knowledge of basic concepts,	Telecommunications	(6) Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4071	400	278	Knowledge of different types of	Telecommunications	(6) Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4071	400	294	Knowledge of hacking methodologies in	Surveillance	(1) Perform ethical hacking
Capella University	B.S	Information Assurance and	IT 4071	400	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	(1) Perform ethical hacking
Capella University	B.S	Information Assurance and	IT 4071	400	376	Skill in talking to others to convey	Oral Communication	(2) Describe the role of social
Capella University	B.S	Information Assurance and	IT 4071	400	886	Skill in wireless network target	Vulnerabilities Assessment	(3) Perform sniffing on
Capella University	B.S	Information Assurance and	IT 4071	400	922	Skill in using network analysis tools to	Vulnerabilities Assessment	(4) Identify the vulnerabilities of

Capella University	B.S	Information Assurance and	IT 4071	400	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	(1) Perform ethical hacking
Capella University	B.S	Information Assurance and	IT 4071	400	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	(3) Perform sniffing on
Capella University	B.S	Information Assurance and	IT 4071	400	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	(4) Identify the vulnerabilities of
Capella University	B.S	Information Assurance and	IT 4071	400	1117	Skill in utilizing virtual networks for testing	Operating Systems	(2) Describe the role of social
Capella University	B.S	Information Assurance and	IT 4071	400	1121	Knowledge of Windows/Unix ports	Operating Systems	(2) Describe the role of social
Capella University	B.S	Information Assurance and	IT 4072	400	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	8	Knowledge of access authentication	Identity Management	(3) Describe the vulnerabilities of
Capella University	B.S	Information Assurance and	IT 4072	400	90	Knowledge of operating systems	Operating Systems	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	113	Knowledge of server and client operating	Operating Systems	(2) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	122	Knowledge of system administration	Operating Systems	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	127	Knowledge of systems administration	Operating Systems	(3) Describe the vulnerabilities of
Capella University	B.S	Information Assurance and	IT 4072	400	219	Skill in system administration for	Operating Systems	(2) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	286	Knowledge of file extensions (e.g., .dll,	Operating Systems	(2) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	287	Knowledge of file system	Operating Systems	(3) Describe the vulnerabilities of
Capella University	B.S	Information Assurance and	IT 4072	400	294	Knowledge of hacking methodologies in	Surveillance	(2) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	302	Knowledge of investigative	Computer Forensics	(2) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	341	Knowledge of UNIX and Windows systems	Operating Systems	(2) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	344	Knowledge of virtualization	Operating Systems	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	347	Knowledge of Windows command	Operating Systems	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	(2) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	356	Skill in determining installed patches on	Operating Systems	(2) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	364	Skill in identifying, modifying, and	Operating Systems	(2) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	371	Skill in reading, interpreting, writing,	Operating Systems	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	386	Skill in using virtual machines	Operating Systems	(5) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	1002	Skill in conducting audits or reviews of	Information Technology	(5) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	1008	Knowledge of how to troubleshoot basic	Operating Systems	(2) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	1011	Knowledge of processes for	Security	(5) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	1033	Knowledge of basic system	Information Systems/Network	(1) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	1056	Knowledge of operations security	Public Safety and Security	(5) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	1063	Knowledge of Unix/Linux operating	Operating Systems	(2) Develop recommendation

Capella University	B.S	Information Assurance and	IT 4072	400	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	(5) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	1117	Skill in utilizing virtual networks for testing	Operating Systems	(5) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4072	400	1121	Knowledge of Windows/Unix ports	Operating Systems	(2) Develop recommendation
Capella University	B.S	Information Assurance and	IT 4073	400	8	Knowledge of access authentication	Identity Management	2. Develop recommendation
Capella University	B.S	Information Assurance and	IT 4073	400	109	Knowledge of secure configuration	Configuration Management	4. Review the security life cycle
Capella University	B.S	Information Assurance and	IT 4073	400	918	Ability to prepare and deliver education and	Teaching Others	3. Develop recommendation
Capella University	B.S	Information Assurance and	IT 4074	400	10	Knowledge of application	Vulnerabilities Assessment	2. Identify malicious code
Capella University	B.S	Information Assurance and	IT 4074	400	123	Knowledge of system and application	Vulnerabilities Assessment	2. Identify malicious code
Capella University	B.S	Information Assurance and	IT 4074	400	1120	Ability to interpret and incorporate data	Data Management	1. Develop recommendation
Capella University	B.S	Information Assurance and	IT 4074	400	1121	Knowledge of Windows/Unix ports	Operating Systems	5. Develop recommendation
Capella University	B.S	Information Assurance and	IT 4075	400	12	Knowledge of communication	Infrastructure Design	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	29	Knowledge of data backup, types of	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	33	Knowledge of database procedures	Incident Management	2. Develop an incident response
Capella University	B.S	Information Assurance and	IT 4075	400	37	Knowledge of disaster recovery and	Incident Management	2. Develop an incident response
Capella University	B.S	Information Assurance and	IT 4075	400	50	Knowledge of how network services and	Infrastructure Design	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	60	Knowledge of incident categories, incident	Incident Management	2. Develop an incident response
Capella University	B.S	Information Assurance and	IT 4075	400	61	Knowledge of incident response and	Incident Management	2. Develop an incident response
Capella University	B.S	Information Assurance and	IT 4075	400	81	Knowledge of network	Infrastructure Design	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	4. Identify legal issues related to
Capella University	B.S	Information Assurance and	IT 4075	400	114	Knowledge of server diagnostic tools and	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	133	Knowledge of telecommunications	Telecommunicatio ns	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	137	Knowledge of the characteristics of	Data Management	1. Develop recommendation
Capella University	B.S	Information Assurance and	IT 4075	400	139	Knowledge of common networking	Infrastructure Design	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	171	Skill in correcting physical and technical	Network Management	1. Develop recommendation
Capella University	B.S	Information Assurance and	IT 4075	400	216	Skill in recovering failed servers	Incident Management	2. Develop an incident response
Capella University	B.S	Information Assurance and	IT 4075	400	217	Skill in preserving evidence integrity	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	229	Skill in using incident handling	Incident Management	2. Develop an incident response
Capella University	B.S	Information Assurance and	IT 4075	400	252	Knowledge of and experience in Insider	Computer Network Defense	3. Identify how law enforcement
Capella University	B.S	Information Assurance and	IT 4075	400	261	Knowledge of basic concepts,	Telecommunicatio ns	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	264	Knowledge of basic physical computer	Computers and Electronics	1. Develop recommendation

Capella University	B.S	Information Assurance and	IT 4075	400	278	Knowledge of different types of	Telecommunications	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	300	Knowledge of intelligence reporting	Organizational Awareness	4. Identify legal issues related to
Capella University	B.S	Information Assurance and	IT 4075	400	302	Knowledge of investigative	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	305	Knowledge of laws that affect cyber	Forensics	3. Identify how law enforcement
Capella University	B.S	Information Assurance and	IT 4075	400	310	Knowledge of legal governance related to	Criminal Law	3. Identify how law enforcement
Capella University	B.S	Information Assurance and	IT 4075	400	316	Knowledge of processes for	Criminal Law	1. Develop recommendation
Capella University	B.S	Information Assurance and	IT 4075	400	336	Knowledge of the nature and function	Telecommunications	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	340	Knowledge of types and collection of	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	346	Knowledge of which system files (e.g. log	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	359	Skill in developing and executing technical	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	360	Skill in identifying and extracting data of	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	366	Skill in law enforcement report	Technical Documentation	3. Identify how law enforcement
Capella University	B.S	Information Assurance and	IT 4075	400	369	Skill in collecting, processing,	Forensics	1. Develop recommendation
Capella University	B.S	Information Assurance and	IT 4075	400	376	Skill in talking to others to convey	Oral Communication	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	377	Skill in tracking and analyzing technical	Legal, Government and Jurisprudence	4. Identify legal issues related to
Capella University	B.S	Information Assurance and	IT 4075	400	379	Skill in using common digital forensics tools	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	381	Skill in using forensic tool suites (e.g.	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	389	Skill in physically disassembling	Computers and Electronics	1. Develop recommendation
Capella University	B.S	Information Assurance and	IT 4075	400	888	Knowledge of types of digital forensics data	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	889	Knowledge of deployable forensics	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	890	Skill in conducting forensic analyses in	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	893	Skill in securing network	Information Assurance	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	901	Knowledge of the capabilities of	Network Management	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	908	Ability to decrypt digital data collections	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	966	Knowledge of enterprise incident	Incident Management	2. Develop an incident response
Capella University	B.S	Information Assurance and	IT 4075	400	978	Knowledge of root cause analysis for	Incident Management	2. Develop an incident response
Capella University	B.S	Information Assurance and	IT 4075	400	980	Skill in performing root cause analysis for	Incident Management	2. Develop an incident response
Capella University	B.S	Information Assurance and	IT 4075	400	981	Knowledge of International Traffic in	Criminal Law	3. Identify how law enforcement
Capella University	B.S	Information Assurance and	IT 4075	400	982	Knowledge of electronic evidence	Criminal Law	3. Identify how law enforcement
Capella University	B.S	Information Assurance and	IT 4075	400	989	Knowledge of Voice over Internet Protocol	Telecommunications	6. Communicate effectively.

Capella University	B.S	Information Assurance and	IT 4075	400	1011	Knowledge of processes for	Security	2. Develop an incident response
Capella University	B.S	Information Assurance and	IT 4075	400	1036	Knowledge of applicable laws (e.g.,	Criminal Law	3. Identify how law enforcement
Capella University	B.S	Information Assurance and	IT 4075	400	1040	Knowledge of relevant laws,	Criminal Law	3. Identify how law enforcement
Capella University	B.S	Information Assurance and	IT 4075	400	1044	Skill in identifying forensic footprints	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	1052	Knowledge of Global Systems for Mobile	Telecommunications	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	3. Identify how law enforcement
Capella University	B.S	Information Assurance and	IT 4075	400	1074	Knowledge of transmission records	Telecommunications	6. Communicate effectively.
Capella University	B.S	Information Assurance and	IT 4075	400	1086	Knowledge of data carving tools and	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	1092	Knowledge of antiforensics tactics,	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	1093	Knowledge of common forensic tool	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4075	400	1099	Skill in analyzing volatile data	Computer Forensics	5. Use a computer
Capella University	B.S	Information Assurance and	IT 4076	400	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	4	Ability to identify systemic security	Vulnerabilities Assessment	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	38	Knowledge of organization's	Information Assurance	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	49	Knowledge of host/network access	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	53	Knowledge of the Security Assessment	Information Assurance	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	55	Knowledge of Information	Information Assurance	1. Quantify risk. 2. Assess risk of
Capella University	B.S	Information Assurance and	IT 4076	400	58	Knowledge of known vulnerabilities from	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	64	Knowledge of information security	Information Systems/ Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	69	Knowledge of Risk Management	Information Systems Security	1. Quantify risk. 2. Assess risk of
Capella University	B.S	Information Assurance and	IT 4076	400	70	Knowledge of information	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	77	Knowledege of current industry	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	82	Knowledge of network design	Infrastructure Design	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	87	Knowledge of network traffic	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	88	Knowledge of new and emerging	Technology Awareness	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	98	Knowledge of policybased and risk	Identity Management	1. Quantify risk. 2. Assess risk of
Capella University	B.S	Information Assurance and	IT 4076	400	100	Knowledge of Privacy Impact Assessments	Personnel Safety and Security	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	108	Knowledge of risk management	Risk Management	1. Quantify risk. 2. Assess risk of
Capella University	B.S	Information Assurance and	IT 4076	400	110	Knowledge of security management	Information Assurance	3. Create appropriate

Capella University	B.S	Information Assurance and	IT 4076	400	111	Knowledge of security system design tools,	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	123	Knowledge of system and application	Vulnerabilities Assessment	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	129	Knowledge of systems lifecycle management	Systems Life Cycle	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	138	Knowledge of the computer network	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	148	Knowledge of VPN security.	Encryption	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	150	Knowledge of what constitutes a network	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	173	Skill in creating policies that relfect	Information Systems Security	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	175	Skill in developing and deploying signatures	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	1. Quantify risk. 2. Assess risk of
Capella University	B.S	Information Assurance and	IT 4076	400	179	Skill in designing security controls	Information Assurance	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	183	Skill in determining how a security system	Information Assurance	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	191	Skill in developing and applying security	Identity Management	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	205	Skill in implementing, maintaining, and	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	277	Knowledge of defense indepth principles and	Computer Network Defense	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	299	Knowledge of information security	Project Management	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	305	Knowledge of laws that affect cyber	Forensics	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	313	Knowledge of logging services for network	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	320	Knowledge of external organizations	External Awareness	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	321	Knowledge of products and	Technology Awareness	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	325	Knowledge of secure acquisitions (e.g.,	Contracting/Procurement	1. Quantify risk. 2. Assess risk of
Capella University	B.S	Information Assurance and	IT 4076	400	326	Knowledge of security hardware and	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	327	Knowledge of security implications of	Information Assurance	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	915	Knowledge of frontend collection	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	918	Ability to prepare and deliver education and	Teaching Others	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	923	Knowledge of security event correlation	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	952	Knowledge of emerging security	Technology Awareness	1. Quantify risk. 2. Assess risk of

Capella University	B.S	Information Assurance and	IT 4076	400	954	Knowledge of Export Control regulations	Contracting/Procurement	1. Quantify risk. 2. Assess risk of
Capella University	B.S	Information Assurance and	IT 4076	400	965	Knowledge of organization's risk	Risk Management	1. Quantify risk. 2. Assess risk of
Capella University	B.S	Information Assurance and	IT 4076	400	967	Knowledge of current and emerging	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	968	Knowledge of softwarerelated	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	975	Skill in integrating black box security	Quality Assurance	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	979	Knowledge of supply chain risk	Risk Management	1. Quantify risk. 2. Assess risk of
Capella University	B.S	Information Assurance and	IT 4076	400	981	Knowledge of International Traffic in	Criminal Law	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	986	Knowledge of organizational	Identity Management	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	1005	Knowledge of functionality, quality,	Contracting/Procurement	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	1011	Knowledge of processes for	Security	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	1021	Knowledge of threat assessment	Risk Management	1. Quantify risk. 2. Assess risk of
Capella University	B.S	Information Assurance and	IT 4076	400	1033	Knowledge of basic system	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	1034	Knowledge of Personally Identifiable	Security	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	1037	Knowledge of information	Risk Management	1. Quantify risk. 2. Assess risk of
Capella University	B.S	Information Assurance and	IT 4076	400	1056	Knowledge of operations security	Public Safety and Security	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	1072	Knowledge of network security	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	1118	Skill in reading and interpreting	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4076	400	1119	Knowledge of signature	Information Systems/Network	3. Create appropriate
Capella University	B.S	Information Assurance and	IT 4803	400	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	2. Identify security threats
Capella University	B.S	Information Assurance and	IT 4803	400	4	Ability to identify systemic security	Vulnerabilities Assessment	6. Describe the relationship
Capella University	B.S	Information Assurance and	IT 4803	400	37	Knowledge of disaster recovery and	Incident Management	3. Develop a security plan.
Capella University	B.S	Information Assurance and	IT 4803	400	123	Knowledge of system and application	Information Assurance	1. Identify general
Capella University	B.S	Information Assurance and	IT 4803	400	191	Skill in developing and applying security	Vulnerabilities Assessment	2. Identify security threats
St. Leo University	B.S	Computer Science,	COM416	400	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Technology Safeguards: IDS,
St. Leo University	B.S	Computer Science,	COM416	400	4	Ability to identify systemic security	Vulnerabilities Assessment	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	5	Ability to match the appropriate	Knowledge Management	Describe and explain the key
St. Leo University	B.S	Computer Science,	COM416	400	8	Knowledge of access authentication	Identity Management	Balance of security and
St. Leo University	B.S	Computer Science,	COM416	400	9	Knowledge of applicable business	Requirements Analysis	Describe and explain the logical
St. Leo University	B.S	Computer Science,	COM416	400	12	Knowledge of communication	Infrastructure Design	Describe and explain the logical
St. Leo University	B.S	Computer Science,	COM416	400	17	Knowledge of certified ethical	Vulnerabilities Assessment	Explain the need for security and

St. Leo University	B.S	Computer Science,	COM416	400	27	Knowledge of cryptology	Cryptography	Technology Safeguard:
St. Leo University	B.S	Computer Science,	COM416	400	28	Knowledge of data administration and	Data Management	Education and Policy Safeguards
St. Leo University	B.S	Computer Science,	COM416	400	55	Knowledge of Information	Information Assurance	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	62	Knowledge of industrystandard and	Logical Systems Design	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	70	Knowledge of information	Information Systems/Network	Technology Safeguards:
St. Leo University	B.S	Computer Science,	COM416	400	77	Knowledege of current industry	Information Systems/Network	Top Down Implementation
St. Leo University	B.S	Computer Science,	COM416	400	82	Knowledge of network design	Infrastructure Design	Describe and explain the logical
St. Leo University	B.S	Computer Science,	COM416	400	98	Knowledge of policybased and risk	Identity Management	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	Legal, Ethical, and Privacy Issues
St. Leo University	B.S	Computer Science,	COM416	400	108	Knowledge of risk management	Risk Management	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	111	Knowledge of security system design tools,	Information Systems/Network	Describe and explain the logical
St. Leo University	B.S	Computer Science,	COM416	400	117	Knowledge of software design tools,	Software Development	Describe and explain the logical
St. Leo University	B.S	Computer Science,	COM416	400	121	Knowledge of structured analysis	Logical Systems Design	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	123	Knowledge of system and application	Vulnerabilities Assessment	Threats, Attacks
St. Leo University	B.S	Computer Science,	COM416	400	124	Knowledge of system design tools,	Logical Systems Design	Describe and explain the logical
St. Leo University	B.S	Computer Science,	COM416	400	126	Knowledge of system software and	Requirements Analysis	Describe and explain the logical
St. Leo University	B.S	Computer Science,	COM416	400	129	Knowledge of systems lifecycle management	Systems Life Cycle	Secure Systems Development
St. Leo University	B.S	Computer Science,	COM416	400	145	Knowledge of the type and frequency of	Systems Life Cycle	Implementing, Maintenance
St. Leo University	B.S	Computer Science,	COM416	400	148	Knowledge of VPN security.	Encryption	Technology Safeguards:
St. Leo University	B.S	Computer Science,	COM416	400	150	Knowledge of what constitutes a network	Information Systems/Network	Threats, Attacks
St. Leo University	B.S	Computer Science,	COM416	400	158	Skill in applying organizationspecific	Systems Testing and Evaluation	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	Describe and explain the logical
St. Leo University	B.S	Computer Science,	COM416	400	167	Skill in conducting server planning,	Network Management	Describe and explain the logical
St. Leo University	B.S	Computer Science,	COM416	400	173	Skill in creating policies that relfect	Information Systems Security	Education and Policy Safeguards
St. Leo University	B.S	Computer Science,	COM416	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	193	Skill in developing, testing, and	Information Assurance	Top Down Implementation
St. Leo University	B.S	Computer Science,	COM416	400	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	Describe and explain the logical
St. Leo University	B.S	Computer Science,	COM416	400	205	Skill in implementing, maintaining, and	Information Systems/Network	Top Down Implementation
St. Leo University	B.S	Computer Science,	COM416	400	237	Skill in using Virtual Private Network	Encryption	Technology Safeguards:
St. Leo University	B.S	Computer Science,	COM416	400	284	Knowledge of encryption algorithms	Cryptography	Technology Safeguard:

St. Leo University	B.S	Computer Science,	COM416	400	299	Knowledge of information security	Project Management	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	300	Knowledge of intelligence reporting	Organizational Awareness	Education and Policy Safeguards
St. Leo University	B.S	Computer Science,	COM416	400	310	Knowledge of legal governance related to	Criminal Law	Legal, Ethical, and Privacy Issues
St. Leo University	B.S	Computer Science,	COM416	400	325	Knowledge of secure acquisitions (e.g.,	Contracting/Procurement	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	341	Knowledge of UNIX and Windows systems	Operating Systems	Technology Safeguards:
St. Leo University	B.S	Computer Science,	COM416	400	344	Knowledge of virtualization	Operating Systems	Implementing, Maintenance
St. Leo University	B.S	Computer Science,	COM416	400	348	Knowledge of wireless network collection	Cryptography	Technology Safeguard:
St. Leo University	B.S	Computer Science,	COM416	400	377	Skill in tracking and analyzing technical	Legal, Government and Jurisprudence	Legal, Ethical, and Privacy Issues
St. Leo University	B.S	Computer Science,	COM416	400	387	Skill in verifying the integrity of encrypted	Encryption	Technology Safeguard:
St. Leo University	B.S	Computer Science,	COM416	400	891	Skill in configuring and utilizing	Configuration Management	Technology Safeguards:
St. Leo University	B.S	Computer Science,	COM416	400	892	Skill in configuring and utilizing	Configuration Management	Technology Safeguards:
St. Leo University	B.S	Computer Science,	COM416	400	918	Ability to prepare and deliver education and	Teaching Others	Education and Policy Safeguards
St. Leo University	B.S	Computer Science,	COM416	400	942	Knowledge of the organization's core	Organizational Awareness	Describe and explain the logical
St. Leo University	B.S	Computer Science,	COM416	400	952	Knowledge of emerging security	Technology Awareness	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	965	Knowledge of organization's risk	Risk Management	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	967	Knowledge of current and emerging	Information Systems/Network	Threats, Attacks
St. Leo University	B.S	Computer Science,	COM416	400	979	Knowledge of supply chain risk	Risk Management	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	985	Skill in configuring and utilizing network	Configuration Management	Technology Safeguards:
St. Leo University	B.S	Computer Science,	COM416	400	986	Knowledge of organizational	Identity Management	Education and Policy Safeguards
St. Leo University	B.S	Computer Science,	COM416	400	1021	Knowledge of threat assessment	Risk Management	Risk Management Describe and
St. Leo University	B.S	Computer Science,	COM416	400	1036	Knowledge of applicable laws (e.g.,	Criminal Law	Legal, Ethical, and Privacy Issues
St. Leo University	B.S	Computer Science,	COM416	400	1037	Knowledge of information	Risk Management	Describe and explain the
St. Leo University	B.S	Computer Science,	COM416	400	1038	Knowledge of local specialized system	Infrastructure Design	Describe and explain the logical
St. Leo University	B.S	Computer Science,	COM416	400	1061	Knowledge of the lifecycle process	Systems Life Cycle	Secure Systems Development
St. Leo University	B.S	Computer Science,	COM416	400	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	Legal, Ethical, and Privacy Issues
St. Leo University	B.S	Computer Science,	COM416	400	1114	Knowledge of encryption	Cryptography	Describe and explain the logical
St. Leo University	Certifica	Information Security	COM 470	400	70	Knowledge of information	Information Systems/Network	Access control approaches,
St. Leo University	Certifica	Information Security	COM 470	400	98	Knowledge of policybased and risk	Identity Management	Explain and develop policies,
St. Leo University	Certifica	Information Security	COM 470	400	107	Knowledge of resource	Project Management	Describe and explain the
St. Leo University	Certifica	Information Security	COM 470	400	108	Knowledge of risk management	Risk Management	Explain and develop

St. Leo University	Certifica	Information Security	COM 470	400	110	Knowledge of security management	Information Assurance	Describe and explain the
St. Leo University	Certifica	Information Security	COM 470	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	Risk management and its role in the
St. Leo University	Certifica	Information Security	COM 470	400	179	Skill in designing security controls	Information Assurance	Explain and develop
St. Leo University	Certifica	Information Security	COM 470	400	252	Knowledge of and experience in Insider	Computer Network Defense	Distinguish between law and
St. Leo University	Certifica	Information Security	COM 470	400	325	Knowledge of secure acquisitions (e.g.,	Contracting/Procurement	Risk management and its role in the
St. Leo University	Certifica	Information Security	COM 470	400	341	Knowledge of UNIX and Windows systems	Operating Systems	Access control approaches,
St. Leo University	Certifica	Information Security	COM 470	400	891	Skill in configuring and utilizing	Configuration Management	Access control approaches,
St. Leo University	Certifica	Information Security	COM 470	400	892	Skill in configuring and utilizing	Configuration Management	Access control approaches,
St. Leo University	Certifica	Information Security	COM 470	400	985	Skill in configuring and utilizing network	Configuration Management	Access control approaches,
St. Leo University	Speciali	Information Assurance	COM 475	400	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	4	Ability to identify systemic security	Vulnerabilities Assessment	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	10	Knowledge of application	Vulnerabilities Assessment	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	17	Knowledge of certified ethical	Vulnerabilities Assessment	Emphasize and explain the
St. Leo University	Speciali	Information Assurance	COM 475	400	58	Knowledge of known vulnerabilities from	Information Systems/Network	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	93	Knowledge of packetlevel analysis	Vulnerabilities Assessment	1. Demonstrate
St. Leo University	Speciali	Information Assurance	COM 475	400	95	Knowledge of penetration testing	Vulnerabilities Assessment	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	123	Knowledge of system and application	Vulnerabilities Assessment	Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	150	Knowledge of what constitutes a network	Information Systems/Network	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	Demonstrate packet analyzers
St. Leo University	Speciali	Information Assurance	COM 475	400	225	Skill in the use of penetration testing	Vulnerabilities Assessment	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	229	Skill in using incident handling	Incident Management	Compare and contrast incident
St. Leo University	Speciali	Information Assurance	COM 475	400	233	Skill in using protocol analyzers	Vulnerabilities Assessment	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	294	Knowledge of hacking methodologies in	Surveillance	1. Describe techniques used
St. Leo University	Speciali	Information Assurance	COM 475	400	321	Knowledge of products and	Technology Awareness	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	Describe and evaluate threat
St. Leo University	Speciali	Information Assurance	COM 475	400	364	Skill in identifying, modifying, and	Operating Systems	Encryption and Password
St. Leo University	Speciali	Information Assurance	COM 475	400	886	Skill in wireless network target	Vulnerabilities Assessment	1. Summarize operating system

St. Leo University	Speciali	Information Assurance	COM 475	400	895	Skill in recognizing and categorizing	Information Assurance	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	986	Knowledge of organizational	Identity Management	Encryption and Password
St. Leo University	Speciali	Information Assurance	COM 475	400	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	1. Demonstrate
St. Leo University	Speciali	Information Assurance	COM 475	400	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Describe and evaluate threat
St. Leo University	Speciali	Information Assurance	COM 475	400	1089	Knowledge of reverse engineering concepts	Vulnerabilities Assessment	1. Summarize operating system
St. Leo University	Speciali	Information Assurance	COM 475	400	1095	Knowledge of how different file types can	Vulnerabilities Assessment	1. Summarize operating system
Southern PolyTech	B.S.	Information Technology	IT 4533	400	1036	Knowledge of applicable laws (e.g.,	Criminal Law	1, Understand the concepts of
Southern PolyTech	B.S.	Information Technology	IT 4533	400	1037	Knowledge of information	Risk Management	3. Discuss the components
Southern PolyTech	B.S.	Information Technology	IT 4823	400	4	Ability to identify systemic security	Vulnerabilities Assessment	2. Describe the threats to and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	10	Knowledge of application	Vulnerabilities Assessment	2. Describe the threats to and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	55	Knowledge of Information	Information Assurance	5. Analyze critically
Southern PolyTech	B.S.	Information Technology	IT 4823	400	63	Knowledge of Information	Information Assurance	3. • Demonstrate a working
Southern PolyTech	B.S.	Information Technology	IT 4823	400	88	Knowledge of new and emerging	Technology Awareness	3. • Demonstrate a working
Southern PolyTech	B.S.	Information Technology	IT 4823	400	98	Knowledge of policybased and risk	Identity Management	4. Design, execute, and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	108	Knowledge of risk management	Risk Management	5. Analyze critically
Southern PolyTech	B.S.	Information Technology	IT 4823	400	123	Knowledge of system and application	Vulnerabilities Assessment	2. • Describe the threats to and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	126	Knowledge of system software and	Requirements Analysis	4. Design, execute, and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	150	Knowledge of what constitutes a network	Information Systems/Network	2. • Describe the threats to and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	173	Skill in creating policies that relfect	Information Systems Security	4. Design, execute, and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	5. Analyze critically
Southern PolyTech	B.S.	Information Technology	IT 4823	400	205	Skill in implementing, maintaining, and	Information Systems/Network	3. Demonstrate a working
Southern PolyTech	B.S.	Information Technology	IT 4823	400	299	Knowledge of information security	Project Management	3. • Demonstrate a working
Southern PolyTech	B.S.	Information Technology	IT 4823	400	300	Knowledge of intelligence reporting	Organizational Awareness	4. Design, execute, and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	917	Knowledge of social dynamics of computer	External Awareness	1. • Describe the importance of
Southern PolyTech	B.S.	Information Technology	IT 4823	400	918	Ability to prepare and deliver education and	Teaching Others	4. Design, execute, and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	920	Knowledge of threat list countries' cyber	External Awareness	2. • Describe the threats to and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	921	Ability to identify possible threat actor	Technology Awareness	2. Describe the threats to and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	952	Knowledge of emerging security	Technology Awareness	5. Analyze critically
Southern PolyTech	B.S.	Information Technology	IT 4823	400	965	Knowledge of organization's risk	Risk Management	5. Analyze critically
Southern PolyTech	B.S.	Information Technology	IT 4823	400	967	Knowledge of current and emerging	Information Systems/Network	2. • Describe the threats to and

Southern PolyTech	B.S.	Information Technology	IT 4823	400	984	Knowledge of computer network	Computer Network Defense	4. Design, execute, and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	986	Knowledge of organizational	Identity Management	4. Design, execute, and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	992	Knowledge of different operational	Computer Network Defense	2. • Describe the threats to and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	1021	Knowledge of threat assessment	Risk Management	2. • Describe the threats to and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	1040	Knowledge of relevant laws,	Criminal Law	4. Design, execute, and
Southern PolyTech	B.S.	Information Technology	IT 4823	400	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	4. Design, execute, and
Southern PolyTech	B.S.	Information Technology	IT 4833	400	12	Knowledge of communication	Infrastructure Design	2?
Southern PolyTech	B.S.	Information Technology	IT 4833	400	41	Knowledge of organization's Local	Infrastructure Design	2. Build or reinforce the
Southern PolyTech	B.S.	Information Technology	IT 4833	400	42	Knowledge of electrical engineering	Hardware Engineering	
Southern PolyTech	B.S.	Information Technology	IT 4833	400	72	Knowledge of local area network (LAN)	Infrastructure Design	2. Build or reinforce the
Southern PolyTech	B.S.	Information Technology	IT 4833	400	82	Knowledge of network design	Infrastructure Design	2. Build or reinforce the
Southern PolyTech	B.S.	Information Technology	IT 4833	400	111	Knowledge of security system design tools,	Information Systems/Network	2. Build or reinforce the
Southern PolyTech	B.S.	Information Technology	IT 4833	400	261	Knowledge of basic concepts,	Telecommunications	5. Enhance the skills of enabling
Southern PolyTech	B.S.	Information Technology	IT 4833	400	278	Knowledge of different types of	Telecommunications	5. Enhance the skills of enabling
Southern PolyTech	B.S.	Information Technology	IT 4833	400	348	Knowledge of wireless network collection	Cryptography	2. Build or reinforce the
Southern PolyTech	B.S.	Information Technology	IT 4833	400	375	Skill in survey, collection, and	Network Management	4. Master to learn at least one of
Southern PolyTech	B.S.	Information Technology	IT 4833	400	886	Skill in wireless network target	Vulnerabilities Assessment	4. Master to learn at least one of
Southern PolyTech	B.S.	Information Technology	IT 4833	400	903	Knowledge of Wireless Fidelity	Network Management	1. Describe the differences
Southern PolyTech	B.S.	Information Technology	IT 4833	400	1086	Knowledge of data carving tools and	Computer Forensics	1. Describe the differences
Southern PolyTech	B.S.	Information Technology	IT 4843	400	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	2. Identify security threats
Southern PolyTech	B.S.	Information Technology	IT 4843	400	4	Ability to identify systemic security	Vulnerabilities Assessment	2. Identify security threats
Southern PolyTech	B.S.	Information Technology	IT 4843	400	10	Knowledge of application	Vulnerabilities Assessment	2. Identify security threats
Southern PolyTech	B.S.	Information Technology	IT 4843	400	12	Knowledge of communication	Infrastructure Design	5. Describe possible attacks
Southern PolyTech	B.S.	Information Technology	IT 4843	400	17	Knowledge of certified ethical	Vulnerabilities Assessment	1. Identify what an ethical hacker
Southern PolyTech	B.S.	Information Technology	IT 4843	400	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	5. Describe possible attacks
Southern PolyTech	B.S.	Information Technology	IT 4843	400	27	Knowledge of cryptology	Cryptography	5. Describe possible attacks
Southern PolyTech	B.S.	Information Technology	IT 4843	400	49		Information Systems/Network	6. Describe network security
Southern PolyTech	B.S.	Information Technology	IT 4843	400	58	Knowledge of known vulnerabilities from	Information Systems/Network	2. Identify security threats
Southern PolyTech	B.S.	Information Technology	IT 4843	400	90	Knowledge of operating systems	Operating Systems	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	95	Knowledge of penetration testing	Vulnerabilities Assessment	2. Identify security threats

Southern PolyTech	B.S.	Information Technology	IT 4843	400	98	Knowledge of policybased and risk	Identity Management	6.Describe network security
Southern PolyTech	B.S.	Information Technology	IT 4843	400	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	1. Identify what an ethical hacker
Southern PolyTech	B.S.	Information Technology	IT 4843	400	113	Knowledge of server and client operating	Operating Systems	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	122	Knowledge of system administration	Operating Systems	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	123	Knowledge of system and application	Vulnerabilities Assessment	2. Identify security threats
Southern PolyTech	B.S.	Information Technology	IT 4843	400	150	Knowledge of what constitutes a network	Information Systems/Network	2. Identify security threats
Southern PolyTech	B.S.	Information Technology	IT 4843	400	157	Skill in applying host/network access	Identity Management	6.Describe network security
Southern PolyTech	B.S.	Information Technology	IT 4843	400	179	Skill in designing security controls	Information Assurance	6.Describe network security
Southern PolyTech	B.S.	Information Technology	IT 4843	400	191	Skill in developing and applying security	Identity Management	6.Describe network security
Southern PolyTech	B.S.	Information Technology	IT 4843	400	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	6.Describe network security
Southern PolyTech	B.S.	Information Technology	IT 4843	400	204	Skill in identifying possible causes of	Systems Life Cycle	3. Use hacking tools to locate
Southern PolyTech	B.S.	Information Technology	IT 4843	400	205	Skill in implementing, maintaining, and	Information Systems/Network	3. Use hacking tools to locate
Southern PolyTech	B.S.	Information Technology	IT 4843	400	210	Skill in mimicking threat behaviors	Computer Network Defense	2. Identify security threats
Southern PolyTech	B.S.	Information Technology	IT 4843	400	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	3. Use hacking tools to locate
Southern PolyTech	B.S.	Information Technology	IT 4843	400	219	Skill in system administration for	Operating Systems	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	225	Skill in the use of penetration testing	Vulnerabilities Assessment	2. Identify security threats
Southern PolyTech	B.S.	Information Technology	IT 4843	400	271	Knowledge of common network	Infrastructure Design	3. Use hacking tools to locate
Southern PolyTech	B.S.	Information Technology	IT 4843	400	284	Knowledge of encryption algorithms	Cryptography	5. Describe possible attacks
Southern PolyTech	B.S.	Information Technology	IT 4843	400	286	Knowledge of file extensions (e.g., .dll,	Operating Systems	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	287	Knowledge of file system	Operating Systems	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	300	Knowledge of intelligence reporting	Organizational Awareness	1. Identify what an ethical hacker
Southern PolyTech	B.S.	Information Technology	IT 4843	400	302	Knowledge of investigative	Computer Forensics	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	341	Knowledge of UNIX and Windows systems	Operating Systems	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	345	Knowledge of web mail collection,	Web Technology	2. Identify security threats
Southern PolyTech	B.S.	Information Technology	IT 4843	400	347	Knowledge of Windows command	Operating Systems	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	348	Knowledge of wireless network collection	Cryptography	5. Describe possible attacks
Southern PolyTech	B.S.	Information Technology	IT 4843	400	356	Skill in determining installed patches on	Operating Systems	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	364	Skill in identifying, modifying, and	Operating Systems	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	371	Skill in reading, interpreting, writing,	Operating Systems	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	377	Skill in tracking and analyzing technical	Legal, Government and Jurisprudence	1. Identify what an ethical hacker

Southern PolyTech	B.S.	Information Technology	IT 4843	400	921	Ability to identify possible threat actor	Technology Awareness	2. Identify security threats
Southern PolyTech	B.S.	Information Technology	IT 4843	400	967	Knowledge of current and emerging	Information Systems/Network	2. Identify security threats
Southern PolyTech	B.S.	Information Technology	IT 4843	400	986	Knowledge of organizational	Identity Management	6.Describe network security
Southern PolyTech	B.S.	Information Technology	IT 4843	400	992	Knowledge of different operational	Computer Network Defense	2. Identify security threats
Southern PolyTech	B.S.	Information Technology	IT 4843	400	1008	Knowledge of how to troubleshoot basic	Operating Systems	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	1033	Knowledge of basic system	Information Systems/Network	3.Use hacking tools to locate
Southern PolyTech	B.S.	Information Technology	IT 4843	400	1036	Knowledge of applicable laws (e.g.,	Criminal Law	1. Identify what an ethical hacker
Southern PolyTech	B.S.	Information Technology	IT 4843	400	1063	Knowledge of Unix/Linux operating	Operating Systems	4. Identify operating
Southern PolyTech	B.S.	Information Technology	IT 4843	400	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	1. Identify what an ethical hacker
Southern PolyTech	B.S.	Information Technology	IT 4843	400	1114	Knowledge of encryption	Cryptography	5. Describe possible attacks
Southern PolyTech	B.S.	Information Technology	IT 4853	400	24	Knowledge of concepts and	Data Management	4. Organize and present
Southern PolyTech	B.S.	Information Technology	IT 4853	400	60	Knowledge of incident categories, incident	Incident Management	1. Define and explain the role
Southern PolyTech	B.S.	Information Technology	IT 4853	400	61	Knowledge of incident response and	Incident Management	1. Define and explain the role
Southern PolyTech	B.S.	Information Technology	IT 4853	400	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	4. Organize and present
Southern PolyTech	B.S.	Information Technology	IT 4853	400	217	Skill in preserving evidence integrity	Computer Forensics	2. Identify the requirements for
Southern PolyTech	B.S.	Information Technology	IT 4853	400	252	Knowledge of and experience in Insider	Computer Network Defense	1. Define and explain the role
Southern PolyTech	B.S.	Information Technology	IT 4853	400	290	Knowledge of processes for seizing	Forensics	2. Identify the requirements for
Southern PolyTech	B.S.	Information Technology	IT 4853	400	302	Knowledge of investigative	Computer Forensics	1. Define and explain the role
Southern PolyTech	B.S.	Information Technology	IT 4853	400	305	Knowledge of laws that affect cyber	Forensics	1. Define and explain the role
Southern PolyTech	B.S.	Information Technology	IT 4853	400	310	Knowledge of legal governance related to	Criminal Law	4. Organize and present
Southern PolyTech	B.S.	Information Technology	IT 4853	400	316	Knowledge of processes for	Criminal Law	2. Identify the requirements for
Southern PolyTech	B.S.	Information Technology	IT 4853	400	340	Knowledge of types and collection of	Computer Forensics	3. Identify the requirements for
Southern PolyTech	B.S.	Information Technology	IT 4853	400	369	Skill in collecting, processing,	Forensics	3. Identify and explain basic
Southern PolyTech	B.S.	Information Technology	IT 4853	400	379	Skill in using common digital forensics tools	Computer Forensics	3. Identify and explain basic
Southern PolyTech	B.S.	Information Technology	IT 4853	400	381	Skill in using forensic tool suites (e.g.	Computer Forensics	3. Identify and explain basic
Southern PolyTech	B.S.	Information Technology	IT 4853	400	888	Knowledge of types of digital forensics data	Computer Forensics	1. Define and explain the role
Southern PolyTech	B.S.	Information Technology	IT 4853	400	908	Ability to decrypt digital data collections	Computer Forensics	3. Identify and explain basic
Southern PolyTech	B.S.	Information Technology	IT 4853	400	909	Skill in processing collected data for	Computer Skills	3. Identify and explain basic
Southern PolyTech	B.S.	Information Technology	IT 4853	400	966	Knowledge of enterprise incident	Incident Management	1. Define and explain the role
Southern PolyTech	B.S.	Information Technology	IT 4853	400	982	Knowledge of electronic evidence	Criminal Law	4. Organize and present

Southern PolyTech	B.S.	Information Technology	IT 4853	400	1036	Knowledge of applicable laws (e.g.,	Criminal Law	4. Organize and present
Southern PolyTech	B.S.	Information Technology	IT 4853	400	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	4. Organize and present
Southern PolyTech	B.S.	Information Technology	IT 4853	400	1092	Knowledge of antiforensics tactics,	Computer Forensics	1. Define and explain the role
Southern PolyTech	B.S.	Information Technology	IT 4853	400	1093	Knowledge of common forensic tool	Computer Forensics	3. Identify and explain basic
Southern PolyTech	B.S.	Information Technology	IT 4903	400	10	Knowledge of application	Vulnerabilities Assessment	1. Define the overall process of
Southern PolyTech	B.S.	Information Technology	IT 4903	400	33	Knowledge of database procedures	Incident Management	5. Explain the goals and content
Southern PolyTech	B.S.	Information Technology	IT 4903	400	55	Knowledge of Information	Information Assurance	1. Define the overall process of
Southern PolyTech	B.S.	Information Technology	IT 4903	400	77	Knowledege of current industry	Information Systems/Network	1. Define the overall process of
Southern PolyTech	B.S.	Information Technology	IT 4903	400	95	Knowledge of penetration testing	Vulnerabilities Assessment	2. Identify the goals of a
Southern PolyTech	B.S.	Information Technology	IT 4903	400	100	Knowledge of Privacy Impact Assessments	Personnel Safety and Security	1. Define the overall process of
Southern PolyTech	B.S.	Information Technology	IT 4903	400	108	Knowledge of risk management	Risk Management	1. Define the overall process of
Southern PolyTech	B.S.	Information Technology	IT 4903	400	123	Knowledge of system and application	Vulnerabilities Assessment	1. Define the overall process of
Southern PolyTech	B.S.	Information Technology	IT 4903	400	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	2.Identify the goals of a
Southern PolyTech	B.S.	Information Technology	IT 4903	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	4. Identify and explain the
Southern PolyTech	B.S.	Information Technology	IT 4903	400	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	3. Identify and explain the
Southern PolyTech	B.S.	Information Technology	IT 4903	400	225	Skill in the use of penetration testing	Vulnerabilities Assessment	3. Identify and explain the
Southern PolyTech	B.S.	Information Technology	IT 4903	400	252	Knowledge of and experience in Insider	Computer Network Defense	5. Explain the goals and content
Southern PolyTech	B.S.	Information Technology	IT 4903	400	300	Knowledge of intelligence reporting	Organizational Awareness	5. Explain the goals and content
Southern PolyTech	B.S.	Information Technology	IT 4903	400	338	Knowledge of the principal methods,	Reasoning	5. Explain the goals and content
Southern PolyTech	B.S.	Information Technology	IT 4903	400	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	2. Identify the goals of a
Southern PolyTech	B.S.	Information Technology	IT 4903	400	895	Skill in recognizing and categorizing	Information Assurance	2. Identify the goals of a
Southern PolyTech	B.S.	Information Technology	IT 4903	400	952	Knowledge of emerging security	Technology Awareness	2. Identify the goals of a
Southern PolyTech	B.S.	Information Technology	IT 4903	400	1011	Knowledge of processes for	Security	5. Explain the goals and content
Southern PolyTech	B.S.	Information Technology	IT 4903	400	1021	Knowledge of threat assessment	Risk Management	1. Define the overall process of
Southern PolyTech	B.S.	Information Technology	IT 4903	400	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	3. Identify and explain the
Snead State Community	B.S	Computer Science	CIS 280	200	38	Knowledge of organization's	Information Assurance	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	49	Knowledge of host/network access	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	53	Knowledge of the Security Assessment	Information Assurance	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	58	Knowledge of known vulnerabilities from	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	64	Knowledge of information security	Information Systems/ Network	1. Students will identify, common

Snead State Community	B.S	Computer Science	CIS 280	200	69	Knowledge of Risk Management	Information Systems Security	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	70	Knowledge of information	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	77	Knowledege of current industry	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	82	Knowledge of network design	Infrastructure Design	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	87	Knowledge of network traffic	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	88	Knowledge of new and emerging	Technology Awareness	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	100	Knowledge of Privacy Impact Assessments	Personnel Safety and Security	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	2. Students will understand the
Snead State Community	B.S	Computer Science	CIS 280	200	110	Knowledge of security management	Information Assurance	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	111	Knowledge of security system design tools,	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	123	Knowledge of system and application	Vulnerabilities Assessment	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	129	Knowledge of systems lifecycle management	Systems Life Cycle	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	138	Knowledge of the computer network	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	148	Knowledge of VPN security.	Encryption	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	150	Knowledge of what constitutes a network	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	173	Skill in creating policies that relfect	Information Systems Security	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	175	Skill in developing and deploying signatures	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	179	Skill in designing security controls	Information Assurance	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	183	Skill in determining how a security system	Information Assurance	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	191	Skill in developing and applying security	Identity Management	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	205	Skill in implementing, maintaining, and	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	277	Knowledge of defense indepth principles and	Computer Network Defense	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	299	Knowledge of information security	Project Management	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	300	Knowledge of intelligence reporting	Organizational Awareness	2. Students will understand the
Snead State Community	B.S	Computer Science	CIS 280	200	302	Knowledge of investigative	Computer Forensics	2. Students will understand the
Snead State Community	B.S	Computer Science	CIS 280	200	305	Knowledge of laws that affect cyber	Forensics	1. Students will identify, common

Snead State Community	B.S	Computer Science	CIS 280	200	310	2. Students will understand the legal	Criminal Law	2. Students will understand the
Snead State Community	B.S	Computer Science	CIS 280	200	313	Knowledge of logging services for network	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	320	Knowledge of external organizations	External Awareness	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	321	Knowledge of products and	Technology Awareness	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	326	Knowledge of security hardware and	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	327	Knowledge of security implications of	Information Assurance	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	377	Skill in tracking and analyzing technical	Legal, Government and Jurisprudence	2. Students will understand the
Snead State Community	B.S	Computer Science	CIS 280	200	915	Knowledge of frontend collection	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	918	Ability to prepare and deliver education and	Teaching Others	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	923	Knowledge of security event correlation	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	952	Knowledge of emerging security	Technology Awareness	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	967	Knowledge of current and emerging	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	968	Knowledge of softwarerelated	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	975	Skill in integrating black box security	Quality Assurance	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	981	Knowledge of International Traffic in	Criminal Law	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	986	Knowledge of organizational	Identity Management	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	1005	Knowledge of functionality, quality,	Contracting/Procurement	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	1011	Knowledge of processes for	Security	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	1033	Knowledge of basic system	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	1034	Knowledge of Personally Identifiable	Security	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	2. Students will understand the
Snead State Community	B.S	Computer Science	CIS 280	200	1037	Knowledge of information	Risk Management	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	1056	Knowledge of operations security	Public Safety and Security	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	2. Students will understand the
Snead State Community	B.S	Computer Science	CIS 280	200	1072	Knowledge of network security	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	1118	Skill in reading and interpreting	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 280	200	1119	Knowledge of signature	Information Systems/Network	1. Students will identify, common
Snead State Community	B.S	Computer Science	CIS 161	100	123	Knowledge of system and application	Vulnerabilities Assessment	2. Students will be able to
Snead State Community	B.S	Computer Science	CIS 161	100	150	Knowledge of what constitutes a network	Information Systems/Network	2. Students will be able to

Snead State Community	B.S	Computer Science	CIS 161	100	281	Knowledge of electronic devices	Hardware	1. Students will identify, describe
Snead State Community	B.S	Computer Science	CIS 161	100	285	Knowledge of evasion strategies and	Computer Network Defense	1. Students will identify, describe
Snead State Community	B.S	Computer Science	CIS 161	100	302	Knowledge of investigative	Computer Forensics	1. Students will identify, describe
Snead State Community	B.S	Computer Science	CIS 161	100	313	Knowledge of logging services for network	Information Systems/Network	1. Students will identify, describe
Snead State Community	B.S	Computer Science	CIS 161	100	326	Knowledge of security hardware and	Information Systems/Network	1. Students will identify, describe
Snead State Community	B.S	Computer Science	CIS 161	100	341	Knowledge of UNIX and Windows systems	Operating Systems	1. Students will identify, describe
Snead State Community	B.S	Computer Science	CIS 161	100	348	Knowledge of wireless network collection	Cryptography	1. Students will identify, describe
Snead State Community	B.S	Computer Science	CIS 161	100	349	Skill in analyzing data from a variety of	Reasoning	1. Students will identify, describe
Snead State Community	B.S	Computer Science	CIS 161	100	353	Skill in collecting data from a variety of	Computer Network Defense	1. Students will identify, describe
Snead State Community	B.S	Computer Science	CIS 161	100	357	Skill in determining the effects of various	Configuration Management	1. Students will identify, describe
Snead State Community	B.S	Computer Science	CIS 161	100	375	Skill in survey, collection, and	Network Management	1. Students will identify, describe
Snead State Community	B.S	Computer Science	CIS 161	100	385	Skill in using traceroute analysis	Network Management	1. Students will identify, describe
Snead State Community	B.S	Computer Science	CIS 161	100	967	Knowledge of current and emerging	Information Systems/Network	2. Students will be able to
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	3. Apply tools and techniques for
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	4	Ability to identify systemic security	Vulnerabilities Assessment	3. Apply tools and techniques for
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	8	Knowledge of access authentication	Identity Management	6. Identify types of authentication
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	12	Knowledge of communication	Infrastructure Design	7. Distinguish types of
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	7. Distinguish types of
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	27	Knowledge of cryptology	Cryptography	7. Distinguish types of
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	63	Knowledge of Information	Information Assurance	6. Identify types of authentication
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	70	Knowledge of information	Information Systems/Network	1. Explain and differentiate the
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	153	Skill in handling malware	Computer Network Defense	2. Distinguish types of malware
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	284	Knowledge of encryption algorithms	Cryptography	7. Distinguish types of
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	341	Knowledge of UNIX and Windows systems	Operating Systems	6. Identify types of authentication
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	348	Knowledge of wireless network collection	Cryptography	7. Distinguish types of
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	896	Skill in protecting a network against	Computer Network Defense	2. Distinguish types of malware
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	968	Knowledge of softwarerelated	Information Systems/Network	1. Explain and differentiate the
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	1029	Knowledge of malware analysis	Computer Network Defense	2. Distinguish types of malware
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	1087	Skill in deep analysis of captured malicious	Computer Network Defense	2. Distinguish types of malware
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	1096	Knowledge of malware analysis	Computer Network Defense	2. Distinguish types of malware

Whatcom Community	A.S.	Cybersecurity	CIS 110	100	1097	Knowledge of virtual machine aware	Computer Network Defense	2. Distinguish types of malware
Whatcom Community	A.S.	Cybersecurity	CIS 110	100	1114	Knowledge of encryption	Cryptography	7. Distinguish types of
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	4	Ability to identify systemic security	Vulnerabilities Assessment	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	38	Knowledge of organization's	Information Assurance	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	49	Knowledge of host/network access	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	53	Knowledge of the Security Assessment	Information Assurance	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	58	Knowledge of known vulnerabilities from	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	64	Knowledge of information security	Information Systems/ Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	69	Knowledge of Risk Management	Information Systems Security	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	70	Knowledge of information	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	77	Knowledege of current industry	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	82	Knowledge of network design	Infrastructure Design	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	87	Knowledge of network traffic	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	88	Knowledge of new and emerging	Technology Awareness	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	100	Knowledge of Privacy Impact Assessments	Personnel Safety and Security	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	110	Knowledge of security management	Information Assurance	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	111	Knowledge of security system design tools,	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	123	Knowledge of system and application	Vulnerabilities Assessment	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	129	Knowledge of systems lifecycle management	Systems Life Cycle	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	138	Knowledge of the computer network	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	148	Knowledge of VPN security.	Encryption	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	150	Knowledge of what constitutes a network	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	173	Skill in creating policies that relfect	Information Systems Security	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	175	Skill in developing and deploying signatures	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	179	Skill in designing security controls	Information Assurance	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	183	Skill in determining how a security system	Information Assurance	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	191	Skill in developing and applying security	Identity Management	2. Create a secure networking

Whatcom Community	A.S.	Cybersecurity	CIS 214	200	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	205	Skill in implementing, maintaining, and	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	277	Knowledge of defense indepth principles and	Computer Network Defense	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	299	Knowledge of information security	Project Management	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	305	Knowledge of laws that affect cyber	Forensics	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	313	Knowledge of logging services for network	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	320	Knowledge of external organizations	External Awareness	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	321	Knowledge of products and	Technology Awareness	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	326	Knowledge of security hardware and	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	327	Knowledge of security implications of	Information Assurance	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	915	Knowledge of frontend collection	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	918	Ability to prepare and deliver education and	Teaching Others	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	923	Knowledge of security event correlation	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	952	Knowledge of emerging security	Technology Awareness	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	967	Knowledge of current and emerging	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	968	Knowledge of softwarerelated	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	975	Skill in integrating black box security	Quality Assurance	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	981	Knowledge of International Traffic in	Criminal Law	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	986	Knowledge of organizational	Identity Management	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	1005	Knowledge of functionality, quality,	Contracting/Procurement	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	1011	Knowledge of processes for	Security	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	1033	Knowledge of basic system	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	1034	Knowledge of Personally Identifiable	Security	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	1037	Knowledge of information	Risk Management	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	1056	Knowledge of operations security	Public Safety and Security	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	1072	Knowledge of network security	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	1118	Skill in reading and interpreting	Information Systems/Network	2. Create a secure networking
Whatcom Community	A.S.	Cybersecurity	CIS 214	200	1119	Knowledge of signature	Information Systems/Network	2. Create a secure networking

Whatcom Community	A.S	Computer Information	CIS 215	200	15	Knowledge of capabilities and	Hardware	4. Securely configure hosts
Whatcom Community	A.S	Computer Information	CIS 215	200	49	Knowledge of host/network access	Information Systems/Network	4. Securely configure hosts
Whatcom Community	A.S	Computer Information	CIS 215	200	60	Knowledge of incident categories, incident	Incident Management	1. Implement an incident response
Whatcom Community	A.S	Computer Information	CIS 215	200	61	Knowledge of incident response and	Incident Management	1. Implement an incident response
Whatcom Community	A.S	Computer Information	CIS 215	200	106	Knowledge of remote access technology	Information Technology	6. Implement remote access
Whatcom Community	A.S	Computer Information	CIS 215	200	112	Knowledge of server administration and	Systems Life Cycle	4. Securely configure hosts
Whatcom Community	A.S	Computer Information	CIS 215	200	157	Skill in applying host/network access	Identity Management	4. Securely configure hosts
Whatcom Community	A.S	Computer Information	CIS 215	200	206	Skill in installing computer and server	Systems Life Cycle	4. Securely configure hosts
Whatcom Community	A.S	Computer Information	CIS 215	200	212	Skill in network mapping and	Infrastructure Design	3. Design a secure network topology
Whatcom Community	A.S	Computer Information	CIS 215	200	277	Knowledge of defense indepth principles and	Computer Network Defense	2. Apply defense in depth
Whatcom Community	A.S	Computer Information	CIS 215	200	891	Skill in configuring and utilizing	Configuration Management	4. Securely configure hosts
Whatcom Community	A.S	Computer Information	CIS 215	200	1072	Knowledge of network security	Information Systems/Network	2. Apply defense in depth
Whatcom Community	A.S	Computer Information	CIS 216	200	59	Knowledge of Intrusion Detection	Computer Network Defense	6. Implement Intrusion
Whatcom Community	A.S	Computer Information	CIS 225	200	29	Knowledge of data backup, types of	Computer Forensics	1. Acquire and preserve
Whatcom Community	A.S	Computer Information	CIS 225	200	302	Knowledge of investigative	Computer Forensics	1. Acquire and preserve
Whatcom Community	A.S	Computer Information	CIS 225	200				5. Analyze forensic evidence
Whatcom Community	A.S	Computer Information	CIS 225	200				7. Analyze network captures
Whatcom Community	A.S	Computer Information	CIS 225	200	346	Knowledge of which system files (e.g. log	Computer Forensics	4. Analyze forensic evidence
Whatcom Community	A.S	Computer Information	CIS 225	200				5. Analyze forensic evidence
Whatcom Community	A.S	Computer Information	CIS 225	200	366	Skill in law enforcement report	Technical Documentation	8. Document and present the
Whatcom Community	A.S	Computer Information	CIS 225	200	379	Skill in using common digital forensics tools	Computer Forensics	3. Use forensics tools through all
Whatcom Community	A.S	Computer Information	CIS 225	200	1099	Skill in analyzing volatile data	Computer Forensics	6. Analyze forensic evidence
Whatcom Community	A.S	Computer Information	CIS 225	200	1121	Knowledge of Windows/Unix ports	Operating Systems	2. Acquire and preserve live
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	12	Knowledge of communication	Infrastructure Design	(6) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	19	Knowledge of Computer Network	Computer Network Defense	(1) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	21	Knowledge of computer algorithms	Mathematical Reasoning	(6) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	22	Knowledge of computer networking	Infrastructure Design	(2) Students will be able to analyze
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	50	Knowledge of how network services and	Infrastructure Design	(2) Students will be able to analyze
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	58	Knowledge of known vulnerabilities from	Information Systems/Network	(3) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	59	Knowledge of Intrusion Detection	Computer Network Defense	(7) Students will be able to analyze

University of Tennessee at	B.S	Information Security &	CPSC 4550	400	66	Knowledge of intrusion detection	Computer Network Defense	(7) Students will be able to analyze
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	75	Knowledge of mathematics,	Mathematical Reasoning	(6) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	77	Knowledege of current industry	Information Systems/Network	(3) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	81	Knowledge of network	Infrastructure Design	(2) Students will be able to analyze
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	87	Knowledge of network traffic	Information Systems/Network	(4) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	92	Knowledge of how traffic flows across	Infrastructure Design	(4) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	111	Knowledge of security system design tools,	Information Systems/Network	(10) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	115	Knowledge of content development	Computer Network Defense	(6) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	139	Knowledge of common networking	Infrastructure Design	(2) Students will be able to analyze
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	146	Knowledge of the types of Intrusion	Computer Network Defense	(7) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	153	Skill in handling malware	Computer Network Defense	(1) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	181	Skill in detecting host and network based	Computer Network Defense	(7) Students will be able to analyze
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	210	Skill in mimicking threat behaviors	Computer Network Defense	(1) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	270	Knowledge of common adversary	Computer Network Defense	(6) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4550	400	375	Skill in survey, collection, and	Network Management	(8) Students will be able to analyze
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	12	Knowledge of communication	Infrastructure Design	(6) Students will have the ability to
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	(7) Students will have the ability to
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	27	Knowledge of cryptology	Cryptography	(6) Students will have the ability to
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	35	Knowledge of digital rights management	Encryption	(1) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	79	Knowledge of network access,	Identity Management	(9) Student will describe basic key
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	148	Knowledge of VPN security.	Encryption	(1) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	237	Skill in using Virtual Private Network	Encryption	(2) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	284	Knowledge of encryption algorithms	Cryptography	(6) Students will have the ability to
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	348	Knowledge of wireless network collection	Cryptography	(6) Students will have the ability to
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	387	Skill in verifying the integrity of encrypted	Encryption	(9) Student will describe basic key
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	1088	Skill in using binary analysis tools (e.g.,	Computer Languages	(6) Students will have the ability to
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	1091	Skill in one way hash functions (e.g., Secure	Data Management	(7) Students will have the ability to
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	1114	Knowledge of encryption	Cryptography	(8) Students will be able to analyze
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	1115	Skill in reading Hexadecimal data	Computer Languages	(6) Students will have the ability to
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	1116	Skill in identifying common encoding	Computer Languages	(6) Students will have the ability to

University of Tennessee at	B.S	Information Security &	CPSC 4600	400	1118	Skill in reading and interpreting	Information Systems/Network	(1) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC 4600	400	1119	Knowledge of signature	Information Systems/Network	(1) Students will be able to
University of Tennessee at	B.S	Information Security &	CPSC4610	400	68	Knowledge of information	Information Technology	1. To give the students a policy
University of Tennessee at	B.S	Information Security &	CPSC4610	400	108	Knowledge of risk management	Risk Management	9. Students are able to identify,
University of Tennessee at	B.S	Information Security &	CPSC4610	400	110	Knowledge of security management	Information Assurance	8. Students understand
University of Tennessee at	B.S	Information Security &	CPSC4610	400	123	Knowledge of system and application	Vulnerabilities Assessment	2. To give the students the
University of Tennessee at	B.S	Information Security &	CPSC4610	400	173	Skill in creating policies that reflect	Information Systems Security	6. Students are able to write
University of Tennessee at	B.S	Information Security &	CPSC4610	400	193	Skill in developing, testing, and	Information Assurance	5. Students are able to plan for
University of Tennessee at	B.S	Information Security &	CPSC4610	400	252	Knowledge of and experience in Insider	Computer Network Defense	3. To give the students a legal
University of Tennessee at	B.S	Information Security &	CPSC4610	400	290	Knowledge of processes for seizing	Forensics	3. To give the students a legal
University of Tennessee at	B.S	Information Security &	CPSC4610	400	299	Knowledge of information security	Project Management	12. Students understand
University of Tennessee at	B.S	Information Security &	CPSC4610	400	305	Knowledge of laws that affect cyber	Forensics	11. Students understand law
University of Tennessee at	B.S	Information Security &	CPSC4610	400	376	Skill in talking to others to convey	Oral Communication	4. To create and nurture an ideal
University of Tennessee at	B.S	Information Security &	CPSC4610	400	891	Skill in configuring and utilizing	Configuration Management	10. Students master protection
University of Tennessee at	B.S	Information Security &	CPSC4610	400	892	Skill in configuring and utilizing	Configuration Management	10. Students master protection
University of Tennessee at	B.S	Information Security &	CPSC4610	400	985	Skill in configuring and utilizing network	Configuration Management	10. Students master protection
University of Tennessee at	B.S	Information Security &	CPSC4620	400	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	14. Students are able to secure
University of Tennessee at	B.S	Information Security &	CPSC4620	400	27	Knowledge of cryptology	Cryptography	11. Students master
University of Tennessee at	B.S	Information Security &	CPSC4620	400	38	Knowledge of organization's	Information Assurance	8. Students have a highlevel
University of Tennessee at	B.S	Information Security &	CPSC4620	400	77	Knowledge of current industry methods for	Information Systems/Network	3. To introduce to students current
University of Tennessee at	B.S	Information Security &	CPSC4620	400	123	Knowledge of system and application	Vulnerabilities Assessment	1. To make students aware of
University of Tennessee at	B.S	Information Security &	CPSC4620	400				9. Students understand
University of Tennessee at	B.S	Information Security &	CPSC4620	400	150	Knowledge of what constitutes a network	Information Systems/Network	1. To make students aware of
University of Tennessee at	B.S	Information Security &	CPSC4620	400	155	Skill in applying and incorporating	Technology Awareness	4. To cultivate students'
University of Tennessee at	B.S	Information Security &	CPSC4620	400	177	Skill in designing countermeasures to	Vulnerabilities Assessment	13. Students are able to design
University of Tennessee at	B.S	Information Security &	CPSC4620	400	284	Knowledge of encryption algorithms	Cryptography	14. Students are able to secure
University of Tennessee at	B.S	Information Security &	CPSC4620	400	376	Skill in talking to others to convey	Oral Communication	5. To create and nurture an ideal
University of Tennessee at	B.S	Information Security &	CPSC4620	400				6. To improve, students' oral and
University of Tennessee at	B.S	Information Security &	CPSC4620	400	952	Knowledge of emerging security	Technology Awareness	15. Students understand
University of Tennessee at	B.S	Information Security &	CPSC4620	400	1021	Knowledge of threat assessment	Risk Management	10. Students are able to discover,

University of Tennessee at	B.S	Information Security &	CPSC4620	400	1114	Knowledge of encryption	Cryptography	11. Students master
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	28	Knowledge of data administration and	Data Management	• 3. Understand administration of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	32	Knowledge of database	Database Management	• 4. Understand the databases
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	33	Knowledge of database procedures	Incident Management	• 4. Understand the databases
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	34	Knowledge of database systems	Database Management	• 4. Understand the databases
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	38	Knowledge of organization's	Information Assurance	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	42	Knowledge of electrical engineering	Hardware Engineering	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	44	Knowledge of enterprise messaging	Enterprise Architecture	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	49	Knowledge of host/network access	Information Systems/Network	• 2. Master the principles of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	68	Knowledge of information	Information Technology	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	89	Knowledge of new technological	Technology Awareness	• 3. Understand administration of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	92	Knowledge of how traffic flows across	Infrastructure Design	• 2. Master the principles of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	94	Knowledge of parallel and distributed	Information Technology	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	98	Knowledge of policybased and risk	Identity Management	• 2. Master the principles of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	104	Knowledge of query languages such as	Database Management	• 4. Understand the databases
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	106	Knowledge of remote access technology	Information Technology	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	112	Knowledge of server administration and	Systems Life Cycle	• 3. Understand administration of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	118	Knowledge of software	Software Engineering	• 6. Master multilevel secure
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	122	Knowledge of system administration	Operating Systems	• 3. Understand administration of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	127	Knowledge of systems administration	Operating Systems	• 3. Understand administration of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	135	Knowledge of the capabilities and	Data Management	• 4. Understand the databases
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	138	Knowledge of the computer network	Information Systems/Network	• 14. Students are able to give a
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	139	Knowledge of common networking	Infrastructure Design	• 2. Master the principles of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	141	Knowledge of the enterprise	Information Technology	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	143	Knowledge of the organization’s	Enterprise Architecture	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	149	Knowledge of web services, including	Web Technology	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	152	Skill in allocating storage capacity in	Database Administration	• 4. Understand the databases
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	157	Skill in applying host/network access	Identity Management	• 2. Master the principles of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	166	Skill in conducting queries and	Database Management	• 4. Understand the databases
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	172	Skill in creating and utilizing mathematical	Modeling and Simulation	• 6. Master multilevel secure

University of Tennessee at	B.S	Information Security &	CPSC 4670	400	178	Skill in designing databases	Database Administration	• 4. Understand the databases
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	179	Skill in designing security controls	Information Assurance	• 2. Master the principles of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	187	Skill in developing data models	Modeling and Simulation	• 6. Master multilevel secure
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	191	Skill in developing and applying security	Identity Management	• 2. Master the principles of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	• 2. Master the principles of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	201	Skill in generating queries and reports	Database Management	• 4. Understand the databases
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	208	Skill in maintaining databases	Database Management	• 4. Understand the databases
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	213	Skill in optimizing database	Database Administration	• 4. Understand the databases
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	219	Skill in system administration for	Operating Systems	• 3. Understand administration of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	223	Skill in the measuring and reporting of	Knowledge Management	• 14. Students are able to give a
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	224	Skill in the use of design modeling (e.g.,	Modeling and Simulation	• 6. Master multilevel secure
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	252	Knowledge of and experience in Insider	Computer Network Defense	• 14. Students are able to give a
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	264	Knowledge of basic physical computer	Computers and Electronics	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	277	Knowledge of defense indepth principles and	Computer Network Defense	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	281	Knowledge of electronic devices	Hardware	• 2. Master the principles of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	300	Knowledge of intelligence reporting	Organizational Awareness	• 14. Students are able to give a
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	338	Knowledge of the principal methods,	Reasoning	• 14. Students are able to give a
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	366	Skill in law enforcement report	Technical Documentation	• 14. Students are able to give a
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	367	Skill in multidisciplined	Writing	• 14. Students are able to give a
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	910	Knowledge of database theory	Data Management	• 4. Understand the databases
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	954	Knowledge of Export Control regulations	Contracting/Procurement	• 2. Master the principles of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	986	Knowledge of organizational	Identity Management	• 2. Master the principles of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	993	Knowledge of the methods, standards,	Enterprise Architecture	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	1011	Knowledge of processes for	Security	• 14. Students are able to give a
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	1012	Knowledge of Capabilities and	Internal Controls	• 2. Master the principles of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	1022	Knowledge of the nature and function	Enterprise Architecture	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	1033	Knowledge of basic system	Information Systems/Network	• 3. Understand administration of
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	1042	Abililty to apply network	Requirements Analysis	• 6. Master multilevel secure
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	1052	Knowledge of Global Systems for Mobile	Telecommunications	• 1. Master the security
University of Tennessee at	B.S	Information Security &	CPSC 4670	400	1072	Knowledge of network security	Information Systems/Network	• 1. Master the security

University of Tennessee at	B.S	Information Security &	CPSC 4670	400	1073	Knowledge of network systems	Network Management	• 6. Master multilevel secure
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	12	Knowledge of communication	Infrastructure Design	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	17	Knowledge of certified ethical	Vulnerabilities Assessment	10. Students will be understand
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	29	Knowledge of data backup, types of	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	33	Knowledge of database procedures	Incident Management	• 6. Master processing crime
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	37	Knowledge of disaster recovery and	Incident Management	• 6. Master processing crime
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	49	Knowledge of host/network access	Information Systems/Network	• 5. Master digital evidence
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	50	Knowledge of how network services and	Infrastructure Design	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	60	Knowledge of incident categories, incident	Incident Management	• 6. Master processing crime
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	61	Knowledge of incident response and	Incident Management	• 6. Master processing crime
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	81	Knowledge of network	Infrastructure Design	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	90	Knowledge of operating systems	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	98	Knowledge of policybased and risk	Identity Management	• 5. Master digital evidence
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	113	Knowledge of server and client operating	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	114	Knowledge of server diagnostic tools and	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	122	Knowledge of system administration	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	127	Knowledge of systems administration	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	133	Knowledge of telecommunications	Telecommunications	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	139	Knowledge of common networking	Infrastructure Design	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	157	Skill in applying host/network access	Identity Management	• 5. Master digital evidence
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	179	Skill in designing security controls	Information Assurance	• 5. Master digital evidence
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	191	Skill in developing and applying security	Identity Management	• 5. Master digital evidence
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	• 5. Master digital evidence
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	216	Skill in recovering failed servers	Incident Management	• 6. Master processing crime
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	217	Skill in preserving evidence integrity	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	219	Skill in system administration for	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	229	Skill in using incident handling	Incident Management	• 6. Master processing crime
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	252	Knowledge of and experience in Insider	Computer Network Defense	• 17. Understand and master email
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	261	Knowledge of basic concepts,	Telecommunications	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	278	Knowledge of different types of	Telecommunications	• 19. Students will learn oral and

University of Tennessee at	B.S	Information Security &	CPSC 4680	400	286	Knowledge of file extensions (e.g., .dll,	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	287	Knowledge of file system	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	290	Knowledge of processes for seizing	Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	302	Knowledge of investigative	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	305	Knowledge of laws that affect cyber	Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	325	Knowledge of secure acquisitions (e.g.,	Contracting/Procurement	• 7. Master data acquisition
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	336	Knowledge of the nature and function	Telecommunications	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	340	Knowledge of types and collection of	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	341	Knowledge of UNIX and Windows systems	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	344	Knowledge of virtualization	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	346	Knowledge of which system files (e.g. log	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	347	Knowledge of Windows command	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	356	Skill in determining installed patches on	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	359	Skill in developing and executing technical	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	360	Skill in identifying and extracting data of	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	364	Skill in identifying, modifying, and	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	369	Skill in collecting, processing,	Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	371	Skill in reading, interpreting, writing,	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	374	Skill in setting up a forensic workstation	Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	376	Skill in talking to others to convey	Oral Communication	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	379	Skill in using common digital forensics tools	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	381	Skill in using forensic tool suites (e.g.	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	386	Skill in using virtual machines	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	888	Knowledge of types of digital forensics data	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	889	Knowledge of deployable forensics	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	890	Skill in conducting forensic analyses in	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	893	Skill in securing network	Information Assurance	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	901	Knowledge of the capabilities of	Network Management	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	908	Ability to decrypt digital data collections	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	966	Knowledge of enterprise incident	Incident Management	• 6. Master processing crime

University of Tennessee at	B.S	Information Security &	CPSC 4680	400	978	Knowledge of root cause analysis for	Incident Management	• 6. Master processing crime
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	980	Skill in performing root cause analysis for	Incident Management	• 6. Master processing crime
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	989	Knowledge of Voice over Internet Protocol	Telecommunications	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1008	Knowledge of how to troubleshoot basic	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1011	Knowledge of processes for	Security	• 6. Master processing crime
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1012	Knowledge of Capabilities and	Internal Controls	• 5. Master digital evidence
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1033	Knowledge of basic system	Information Systems/Network	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1036	Knowledge of applicable laws (e.g.,	Criminal Law	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1044	Skill in identifying forensic footprints	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1052	Knowledge of Global Systems for Mobile	Telecommunications	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1063	Knowledge of Unix/Linux operating	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1074	Knowledge of transmission records	Telecommunications	• 19. Students will learn oral and
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1086	Knowledge of data carving tools and	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1087	Skill in deep analysis of captured malicious	Computer Network Defense	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1092	Knowledge of antiforensics tactics,	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1093	Knowledge of common forensic tool	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1099	Skill in analyzing volatile data	Computer Forensics	• 1. Understanding
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1117	Skill in utilizing virtual networks for testing	Operating Systems	• 4. Master working with Mac
University of Tennessee at	B.S	Information Security &	CPSC 4680	400	1121	Knowledge of Windows/Unix ports	Operating Systems	• 4. Master working with Mac
University of Maryland	B.S	Network Security	CMIT265	200	83	Knowledge of network hardware	Hardware	3. Select, assemble, and
University of Maryland	B.S	Network Security	CMIT265	200	92	Knowledge of how traffic flows across	Infrastructure Design	1. Apply the concepts of OSI
University of Maryland	B.S	Network Security	CMIT265	200	278	Knowledge of different types of	Telecommunications	4. Identify and apply networking
University of Maryland	B.S	Network Security	CMIT265	200	281	Knowledge of electronic devices	Hardware	2. Identify and compare network
University of Maryland	B.S	Network Security	CMIT320	300	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	4. 4. comply with security policies,
University of Maryland	B.S	Network Security	CMIT320	300	108	Knowledge of risk management	Risk Management	1. Assess risk and implement risk
University of Maryland	B.S	Network Security	CMIT320	300	156	Skill in applying confidentiality,	Information Assurance	3. Apply security controls to
University of Maryland	B.S	Network Security	CMIT320	300	264	Knowledge of basic physical computer	Computers and Electronics	2. evaluate and select
University of Maryland	B.S	Network Security	CMIT321	300	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	3. Assess system vulnerability and
University of Maryland	B.S	Network Security	CMIT321	300	17	Knowledge of certified ethical	Vulnerabilities Assessment	1. Apply laws and regulations

University of Maryland	B.S	Network Security	CMIT321	300	225	Skill in the use of penetration testing	Vulnerabilities Assessment	4. Conduct penetration
University of Maryland	B.S	Network Security	CMIT321	300	886	Skill in wireless network target	Vulnerabilities Assessment	2. Analyze and examine different
University of Maryland	B.S	Network Security	CMIT369	300	122	Knowledge of system administration	Operating Systems	2. Implement Windows Server
University of Maryland	B.S	Network Security	CMIT369	300	339	Knowledge of the structure and intent	Organizational Awareness	1. Plan for Windows Server
University of Maryland	B.S	Network Security	CMIT369	300	341	Knowledge of UNIX and Windows systems	Operating Systems	3. Plan for applaications and
University of Maryland	B.S	Network Security	CMIT369	300	364	Skill in identifying, modifying, and	Operating Systems	2. Implement Windows Server
University of Maryland	B.S	Network Security	CMIT391	300	50	Knowledge of how network services and	Infrastructure Design	4. Configure and troubleshoot
University of Maryland	B.S	Network Security	CMIT391	300	139	Knowledge of common networking	Infrastructure Design	4. Configure and troubleshoot
University of Maryland	B.S	Network Security	CMIT391	300	219	Skill in system administration for	Operating Systems	3. Install and configure system
University of Maryland	B.S	Network Security	CMIT391	300	342	Knowledge of Unix command line (e.g.,	Computer Languages	1. Demonstrate proficiency using
University of Maryland	B.S	Network Security	CMIT391	300	364	Skill in identifying, modifying, and	Operating Systems	2. Perform maintenance
University of Maryland	B.S	Network Security	CMIT391	300	891	Skill in configuring and utilizing	Configuration Management	5. Apply appropriate
University of Maryland	B.S	Network Security	CMIT391	300	892	Skill in configuring and utilizing	Configuration Management	5. Apply appropriate
University of Maryland	B.S	Network Security	CMIT391	300	1063	Knowledge of Unix/Linux operating	Operating Systems	1. Demonstrate proficiency using
University of Maryland	B.S	Network Security	CSIA301	300	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	5. Identify common threats
University of Maryland	B.S	Network Security	CSIA301	300	4	Ability to identify systemic security	Vulnerabilities Assessment	6. Identify the security issues
University of Maryland	B.S	Network Security	CSIA301	300	8	Knowledge of access authentication	Identity Management	2. Analyze the role of security
University of Maryland	B.S	Network Security	CSIA301	300	27	Knowledge of cryptology	Cryptography	3. Explain the role of cryptography
University of Maryland	B.S	Network Security	CSIA301	300	38	Knowledge of organization's	Information Assurance	1. Describe the necessity of
University of Maryland	B.S	Network Security	CSIA301	300	70	Knowledge of information	Information Systems/Network	4. Analyze issues related to
University of Maryland	B.S	Network Security	CMSC 412	400	79	Knowledge of network access,	Identity Management	3. explain the mechanisms
University of Maryland	B.S	Network Security	CMSC 412	400	90	Knowledge of operating systems	Operating Systems	1. design and implement a
University of Maryland	B.S	Network Security	CMSC 412	400	297	Knowledge of industry indicators	Technology Awareness	4. analyze trends in operating
University of Maryland	B.S	Network Security	CSIA 303	300	88	Knowledge of new and emerging	Technology Awareness	3. evaluate and recommend
University of Maryland	B.S	Network Security	CSIA 303	300	156	Skill in applying confidentiality,	Information Assurance	2. integrate confidentiality,
University of Maryland	B.S	Network Security	CSIA 303	300	193	Skill in developing, testing, and	Information Assurance	1. develop an information
University of Maryland	B.S	Network Security	CSIA 412	400	77	Knowledege of current industry	Information Systems/Network	2. comply with requisite
University of Maryland	B.S	Network Security	CSIA 412	400	138	Knowledge of the computer network	Information Systems/Network	3. perform a comprehensive
University of Maryland	B.S	Network Security	CSIA 412	400	376	Skill in talking to others to convey	Oral Communication	4. communicate security analysis
University of Maryland	B.S	Network Security	CSIA 412	400	377	Skill in tracking and analyzing technical	Legal, Government and Jurisprudence	1. analyze, interpret, and

University of Maryland	B.S	Network Security	CSIA 413	400	28	Knowledge of data administration and	Data Management	1. evaluate and select solutions
University of Maryland	B.S	Network Security	CSIA 413	400	77	Knowledege of current industry	Information Systems/Network	2. develop and implement
University of Maryland	B.S	Network Security	CSIA 413	400	332	Ability to develop curriculum that	Teaching Others	3. communicate policies,
University of Maryland	B.S	Network Security	CSIA 413	400	356	Skill in determining installed patches on	Operating Systems	4. implement continuous
University of Maryland	B.S	Network Security	CSIA 485	400	205	Skill in implementing, maintaining, and	Information Systems/Network	1. protect an organization's
University of Maryland	B.S	Network Security	CSIA 485	400	211	Skill in monitoring and optimizing server	Information Technology	2. implement continuous
University of Maryland	B.S	Network Security	CSIA 485	400	340	Knowledge of types and collection of	Computer Forensics	3. analyze advanced
University of Maryland	B.S	Network Security	CSIA 485	400	918	Ability to prepare and deliver education and	Teaching Others	4. formulate, update, and
University of the District of	B.S	Computer Science	CSCI315	300	90	Knowledge of operating systems	Operating Systems	1) Understand UNIX (or
University of the District of	B.S	Computer Science	CSCI315	300	113	Knowledge of server and client operating	Operating Systems	1) Understand UNIX (or
University of the District of	B.S	Computer Science	CSCI315	300	122	Knowledge of system administration	Operating Systems	Understand UNIX system
University of the District of	B.S	Computer Science	CSCI315	300	127	Knowledge of systems administration	Operating Systems	Understand UNIX system
University of the District of	B.S	Computer Science	CSCI315	300	219	Skill in system administration for	Operating Systems	Understand UNIX system
University of the District of	B.S	Computer Science	CSCI315	300	286	Knowledge of file extensions (e.g., .dll,	Operating Systems	Understand UNIX system
University of the District of	B.S	Computer Science	CSCI315	300	287	Knowledge of file system	Operating Systems	1) Understand UNIX (or
University of the District of	B.S	Computer Science	CSCI315	300	341	Knowledge of UNIX and Windows systems	Operating Systems	Understand UNIX system
University of the District of	B.S	Computer Science	CSCI315	300	342	Knowledge of Unix command line (e.g.,	Computer Languages	3) Know how to use UNIX
University of the District of	B.S	Computer Science	CSCI315	300	356	Skill in determining installed patches on	Operating Systems	Understand UNIX system
University of the District of	B.S	Computer Science	CSCI315	300	364	Skill in identifying, modifying, and	Operating Systems	3) Know how to use UNIX
University of the District of	B.S	Computer Science	CSCI315	300	371	Skill in reading, interpreting, writing,	Operating Systems	3) Know how to use UNIX
University of the District of	B.S	Computer Science	CSCI315	300	1033	Knowledge of basic system	Information Systems/Network	2) Understand UNIX system
University of the District of	B.S	Computer Science	CSCI315	300	1063	Knowledge of Unix/Linux operating	Operating Systems	1) Understand UNIX (or
University of the District of	B.S	Computer Science	CSCI315	300	1121	Knowledge of Windows/Unix ports	Operating Systems	2) Understand UNIX system
University of the District of	B.S	Computer Science	CSCI351	300	12	Knowledge of communication	Infrastructure Design	2) Learn fundamental
University of the District of	B.S	Computer Science	CSCI351	300	15	Knowledge of capabilities and	Hardware	5) Understand the various
University of the District of	B.S	Computer Science	CSCI351	300	22	Knowledge of computer networking	Infrastructure Design	2) Learn fundamental
University of the District of	B.S	Computer Science	CSCI351	300	41	Knowledge of organization's Local	Infrastructure Design	1) Know the basic definitions and
University of the District of	B.S	Computer Science	CSCI351	300	50	Knowledge of how network services and	Infrastructure Design	4) Understand basic design and
University of the District of	B.S	Computer Science	CSCI351	300	72	Knowledge of local area network (LAN)	Infrastructure Design	5) Understand the various
University of the District of	B.S	Computer Science	CSCI351	300	81	Knowledge of network	Infrastructure Design	5) Understand the various

University of the District of	B.S	Computer Science	CSCI351	300	92	Knowledge of how traffic flows across	Infrastructure Design	4) Understand basic design and
University of the District of	B.S	Computer Science	CSCI351	300	139	Knowledge of common networking	Infrastructure Design	4) Understand basic design and
University of the District of	B.S	Computer Science	CSCI351	300	194	Skill in diagnosing connectivity problems	Network Management	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	207	Skill in installing, configuring, and		6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	212	Skill in network mapping and	Infrastructure Design	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	221	Skill in testing and configuring network	Network Management	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	231	Skill in using network management tools to	Network Management	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	261	Knowledge of basic concepts,	Telecommunications	2) Learn fundamental
University of the District of	B.S	Computer Science	CSCI351	300	271	Knowledge of common network	Infrastructure Design	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	278	Knowledge of different types of	Telecommunications	1) Know the basic definitions and
University of the District of	B.S	Computer Science	CSCI351	300	341	Knowledge of UNIX and Windows systems	Operating Systems	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	385	Skill in using traceroute analysis	Network Management	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	901	Knowledge of the capabilities of	Network Management	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	902	Knowledge of the range of existing	Network Management	5) Understand the various
University of the District of	B.S	Computer Science	CSCI351	300	903	Knowledge of Wireless Fidelity	Network Management	5) Understand the various
University of the District of	B.S	Computer Science	CSCI351	300	1059	Knowledge of networking protocols	Infrastructure Design	4) Understand basic design and
University of the District of	B.S	Computer Science	CSCI352	300	19	Knowledge of Computer Network	Computer Network Defense	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	22	Knowledge of computer networking	Infrastructure Design	1) Familiar with the fundamental
University of the District of	B.S	Computer Science	CSCI352	300	49	Knowledge of host/network access	Information Systems/Network	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	50	Knowledge of how network services and	Infrastructure Design	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	58	Knowledge of known vulnerabilities from	Information Systems/Network	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	59	Knowledge of Intrusion Detection	Computer Network Defense	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	70	Knowledge of information	Information Systems/Network	4) Know the various ways to
University of the District of	B.S	Computer Science	CSCI352	300	81	Knowledge of network	Infrastructure Design	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	82	Knowledge of network design	Infrastructure Design	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	92	Knowledge of how traffic flows across	Infrastructure Design	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	111	Knowledge of security system design tools,	Information Systems/Network	4) Know the various ways to
University of the District of	B.S	Computer Science	CSCI352	300	139	Knowledge of common networking	Infrastructure Design	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	150	Knowledge of what constitutes a network	Information Systems/Network	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	2) Able to differentiate

University of the District of	B.S	Computer Science	CSCI352	300	252	Knowledge of and experience in Insider	Computer Network Defense	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	274	Knowledge of concepts, principles,	Computer Network Defense	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	277	Knowledge of defense indepth principles and	Computer Network Defense	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	313	Knowledge of logging services for network	Information Systems/Network	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	326	Knowledge of security hardware and	Information Systems/Network	4) Know the various ways to
University of the District of	B.S	Computer Science	CSCI352	300	923	Knowledge of security event correlation	Information Systems/Network	4) Know the various ways to
University of the District of	B.S	Computer Science	CSCI352	300	967	Knowledge of current and emerging	Information Systems/Network	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	984	Knowledge of computer network	Computer Network Defense	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	985	Skill in configuring and utilizing network	Configuration Management	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	990	Knowledge of common attack	Computer Network Defense	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	991	Knowledge of different classes of	Computer Network Defense	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	992	Knowledge of different operational	Computer Network Defense	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	1011	Knowledge of processes for	Security	1) Familiar with the fundamental
University of the District of	B.S	Computer Science	CSCI352	300	1033	Knowledge of basic system	Information Systems/Network	4) Know the various ways to
University of the District of	B.S	Computer Science	CSCI352	300	1072	Knowledge of network security	Information Systems/Network	1) Familiar with the fundamental
University of the District of	B.S	Computer Science	CSCI352	300	1073	Knowledge of network systems	Network Management	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI353	300	8	Knowledge of access authentication	Identity Management	3) Understand identify
University of the District of	B.S	Computer Science	CSCI353	300	35	Knowledge of digital rights management	Encryption	3) Understand identify
University of the District of	B.S	Computer Science	CSCI353	300	37	Knowledge of disaster recovery and	Incident Management	7) Perform business
University of the District of	B.S	Computer Science	CSCI353	300	77	Knowledege of current industry	Information Systems/Network	2) Perform compliance
University of the District of	B.S	Computer Science	CSCI353	300	79	Knowledge of network access,	Identity Management	3) Understand identify
University of the District of	B.S	Computer Science	CSCI353	300	98	Knowledge of policybased and risk	Identity Management	3) Understand identify
University of the District of	B.S	Computer Science	CSCI353	300	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	2) Perform compliance
University of the District of	B.S	Computer Science	CSCI353	300	299	Knowledge of information security	Project Management	5) Plan for change management
University of the District of	B.S	Computer Science	CSCI353	300	986	Knowledge of organizational	Identity Management	1) Design a security policy
University of the District of	B.S	Computer Science	CSCI353	300	1002	Skill in conducting audits or reviews of	Information Technology	6) Perform logging and
University of the District of	B.S	Computer Science	CSCI353	300	1033	Knowledge of basic system	Information Systems/Network	4) Harden systems through
University of the District of	B.S	Computer Science	CSCI353	300	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	4) Harden systems through
University of the District of	B.S	Computer Science	CSCI353	300	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	4) Harden systems through
University of the District of	B.S	Computer Science	CSCI412	400	90	Knowledge of operating systems	Operating Systems	1) Understand the concepts of

University of the District of	B.S	Computer Science	CSCI412	400	113	Knowledge of server and client operating	Operating Systems	1) Understand the concepts of
University of the District of	B.S	Computer Science	CSCI412	400	122	Knowledge of system administration	Operating Systems	2) Know how to perform both
University of the District of	B.S	Computer Science	CSCI412	400	219	Skill in system administration for	Operating Systems	4) Have an ability on controlling
University of the District of	B.S	Computer Science	CSCI412	400	287	Knowledge of file system	Operating Systems	3) Understand resource
University of the District of	B.S	Computer Science	CSCI412	400	342	Knowledge of Unix command line (e.g.,	Computer Languages	2) Know how to perform both
University of the District of	B.S	Computer Science	CSCI412	400	364	Skill in identifying, modifying, and	Operating Systems	4) Have an ability on controlling
University of the District of	B.S	Computer Science	CSCI412	400	371	Skill in reading, interpreting, writing,	Operating Systems	2) Know how to perform both
University of the District of	B.S	Computer Science	CSCI412	400	1008	Knowledge of how to troubleshoot basic	Operating Systems	2) Know how to perform both
University of the District of	B.S	Computer Science	CSCI412	400	1047	Skill in writing kernel level applications	Software Development	1) Understand the concepts of
University of the District of	B.S	Computer Science	CSCI412	400	1063	Knowledge of Unix/Linux operating	Operating Systems	1) Understand the concepts of
University of the District of	B.S	Computer Science	CSCI441	400	24	Knowledge of concepts and	Data Management	1) Understand digital forensic
University of the District of	B.S	Computer Science	CSCI441	400	217	Skill in preserving evidence integrity	Computer Forensics	5) Know how to seize a computer
University of the District of	B.S	Computer Science	CSCI441	400	290	Knowledge of processes for seizing	Forensics	5) Know how to seize a computer
University of the District of	B.S	Computer Science	CSCI441	400	302	Knowledge of investigative	Computer Forensics	2) Know how to examine various
University of the District of	B.S	Computer Science	CSCI441	400	313	Knowledge of logging services for network	Information Systems/Network	2) Know how to examine various
University of the District of	B.S	Computer Science	CSCI441	400	340	Knowledge of types and collection of	Computer Forensics	4) Determine where digital
University of the District of	B.S	Computer Science	CSCI441	400	346	Knowledge of which system files (e.g. log	Computer Forensics	4) Determine where digital
University of the District of	B.S	Computer Science	CSCI441	400	360	Skill in identifying and extracting data of	Computer Forensics	4) Determine where digital
University of the District of	B.S	Computer Science	CSCI441	400	369	Skill in collecting, processing,	Forensics	5) Know how to seize a computer
University of the District of	B.S	Computer Science	CSCI441	400	379	Skill in using common digital forensics tools	Computer Forensics	1) Understand digital forensic
University of the District of	B.S	Computer Science	CSCI441	400	888	Knowledge of types of digital forensics data	Computer Forensics	4) Determine where digital
University of the District of	B.S	Computer Science	CSCI441	400	1044	Skill in identifying forensic footprints	Computer Forensics	4) Determine where digital
University of the District of	B.S	Computer Science	CSCI441	400	1093	Knowledge of common forensic tool	Computer Forensics	2) Know how to examine various
University of the District of	B.S	Computer Science	CSCI453	400	44	Knowledge of enterprise messaging	Enterprise Architecture	4) Explaining the requirements
University of the District of	B.S	Computer Science	CSCI453	400	56	Knowledge of information assurance	Information Assurance	2) Identifying current secure
University of the District of	B.S	Computer Science	CSCI453	400	116	Knowledge of software debugging	Software Development	4) Explaining the requirements
University of the District of	B.S	Computer Science	CSCI453	400	117	Knowledge of software design tools,	Software Development	4) Explaining the requirements
University of the District of	B.S	Computer Science	CSCI453	400	118	Knowledge of software	Software Engineering	3) Showing the practical
University of the District of	B.S	Computer Science	CSCI453	400	119	Knowledge of software engineering	Software Engineering	1) Understanding the importance of
University of the District of	B.S	Computer Science	CSCI453	400	126	Knowledge of system software and	Requirements Analysis	5) Understand professionalism,

University of the District of	B.S	Computer Science	CSCI453	400	129	Knowledge of systems lifecycle management	Systems Life Cycle	3) Showing the practical
University of the District of	B.S	Computer Science	CSCI453	400	327	Knowledge of security implications of	Information Assurance	2) Identifying current secure
University of the District of	B.S	Computer Science	CSCI453	400	968	Knowledge of softwarerelated	Information Systems/Network	2) Identifying current secure
University of the District of	B.S	Computer Science	CSCI453	400	976	Knowledge of software quality	Software Engineering	4) Explaining the requirements
University of the District of	B.S	Computer Science	CSCI453	400	1071	Knowledge of secure software deployment	Software Engineering	3) Showing the practical
University of the District of	B.S	Computer Science	CSCI455	400	21	Knowledge of computer algorithms	Mathematical Reasoning	1) Understand basic algorithm
University of the District of	B.S	Computer Science	CSCI455	400	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	3) Understand symmetric/asym
University of the District of	B.S	Computer Science	CSCI455	400	27	Knowledge of cryptology	Cryptography	3) Understand symmetric/asym
University of the District of	B.S	Computer Science	CSCI455	400	35	Knowledge of digital rights management	Encryption	5) Have knowledge on
University of the District of	B.S	Computer Science	CSCI455	400	284	Knowledge of encryption algorithms	Cryptography	3) Understand symmetric/asym
University of the District of	B.S	Computer Science	CSCI455	400	387	Skill in verifying the integrity of encrypted	Encryption	3) Understand symmetric/asym
University of the District of	B.S	Computer Science	CSCI455	400	1091	Skill in one way hash functions (e.g., Secure	Data Management	5) Have knowledge on
University of the District of	B.S	Computer Science	CSCI455	400	1114	Knowledge of encryption	Cryptography	3) Understand symmetric/asym
University of Advancing	B.S	Technology Forensics	CFR210	200	60	Knowledge of incident categories, incident	Incident Management	Explain the incident response
University of Advancing	B.S	Technology Forensics	CFR210	200	61	Knowledge of incident response and	Incident Management	Explain the incident response
University of Advancing	B.S	Technology Forensics	CFR210	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	Demonstrate, validate, and
University of Advancing	B.S	Technology Forensics	CFR210	200	229	Skill in using incident handling	Incident Management	Explain the incident response
University of Advancing	B.S	Technology Forensics	CFR210	200	231	Skill in using network management tools to	Network Management	Demonstrate, validate, and
University of Advancing	B.S	Technology Forensics	CFR210	200	338	Knowledge of the principal methods,	Reasoning	Articulate and implement a
University of Advancing	B.S	Technology Forensics	CFR210	200	340	Knowledge of types and collection of	Computer Forensics	Describe and demonstrate via
University of Advancing	B.S	Technology Forensics	CFR210	200	348	Knowledge of wireless network collection	Cryptography	Describe and demonstrate via
University of Advancing	B.S	Technology Forensics	CFR210	200	353	Skill in collecting data from a variety of	Computer Network Defense	Describe and demonstrate via
University of Advancing	B.S	Technology Forensics	CFR210	200	367	Skill in multidisciplined	Writing	Articulate and implement a
University of Advancing	B.S	Technology Forensics	CFR210	200	375	Skill in survey, collection, and	Network Management	Describe and demonstrate via
University of Advancing	B.S	Technology Forensics	CFR210	200	922	Skill in using network analysis tools to	Vulnerabilities Assessment	Demonstrate, validate, and
University of Advancing	B.S	Technology Forensics	CFR210	200	978	Knowledge of root cause analysis for	Incident Management	Explain the incident response
University of Advancing	B.S	Technology Forensics	CFR210	200	1011	Knowledge of processes for	Security	Explain the incident response
University of Advancing	B.S	Technology Forensics	CFR210	200	1120	Ability to interpret and incorporate data	Data Management	Demonstrate, validate, and
University of Advancing	B.S	Technology Forensics	CFR227	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Identify and evaluate different
University of Advancing	B.S	Technology Forensics	CFR227	200	10	Knowledge of application	Vulnerabilities Assessment	Identify and evaluate different

University of Advancing	B.S	Technology Forensics	CFR227	200	35	Knowledge of digital rights management	Encryption	Comprehend popular
University of Advancing	B.S	Technology Forensics	CFR227	200	70	Knowledge of information	Information Systems/Network	Analyze and assess computer
University of Advancing	B.S	Technology Forensics	CFR227	200	77	Knowledege of current industry	Information Systems/Network	Analyze and assess computer
University of Advancing	B.S	Technology Forensics	CFR227	200	88	Knowledge of new and emerging	Technology Awareness	Understand the importance of
University of Advancing	B.S	Technology Forensics	CFR227	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	Illustrate the basis for today's
University of Advancing	B.S	Technology Forensics	CFR227	200	111	Knowledge of security system design tools,	Information Systems/Network	Analyze and assess computer
University of Advancing	B.S	Technology Forensics	CFR227	200	123	Knowledge of system and application	Vulnerabilities Assessment	Identify and evaluate different
University of Advancing	B.S	Technology Forensics	CFR227	200	150	Knowledge of what constitutes a network	Information Systems/Network	Identify and evaluate different
University of Advancing	B.S	Technology Forensics	CFR227	200	175	Skill in developing and deploying signatures	Information Systems/Network	Comprehend popular
University of Advancing	B.S	Technology Forensics	CFR227	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	Get handson experience using
University of Advancing	B.S	Technology Forensics	CFR227	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	Illustrate the basis for today's
University of Advancing	B.S	Technology Forensics	CFR227	200	274	Knowledge of concepts, principles,	Computer Network Defense	Get handson experience using
University of Advancing	B.S	Technology Forensics	CFR227	200	277	Knowledge of defense indepth principles and	Computer Network Defense	Analyze and assess computer
University of Advancing	B.S	Technology Forensics	CFR227	200	282	Knowledge of emerging	Technology Awareness	Understand the importance of
University of Advancing	B.S	Technology Forensics	CFR227	200	284	Knowledge of encryption algorithms	Cryptography	Comprehend popular
University of Advancing	B.S	Technology Forensics	CFR227	200	321	Knowledge of products and	Technology Awareness	Understand the importance of
University of Advancing	B.S	Technology Forensics	CFR227	200	379	Skill in using common digital forensics tools	Computer Forensics	Get handson experience using
University of Advancing	B.S	Technology Forensics	CFR227	200	381	Skill in using forensic tool suites (e.g.	Computer Forensics	Get handson experience using
University of Advancing	B.S	Technology Forensics	CFR227	200	892	Skill in configuring and utilizing	Configuration Management	Get handson experience using
University of Advancing	B.S	Technology Forensics	CFR227	200	895	Skill in recognizing and categorizing	Information Assurance	Identify and evaluate different
University of Advancing	B.S	Technology Forensics	CFR227	200	917	Knowledge of social dynamics of computer	External Awareness	Understand the importance of
University of Advancing	B.S	Technology Forensics	CFR227	200	922	Skill in using network analysis tools to	Vulnerabilities Assessment	Get handson experience using
University of Advancing	B.S	Technology Forensics	CFR227	200	952	Knowledge of emerging security	Technology Awareness	Identify and evaluate different
University of Advancing	B.S	Technology Forensics	CFR227	200	967	Knowledge of current and emerging	Information Systems/Network	Identify and evaluate different
University of Advancing	B.S	Technology Forensics	CFR227	200	968	Knowledge of softwarerelated	Information Systems/Network	Analyze and assess computer
University of Advancing	B.S	Technology Forensics	CFR227	200	1002	Skill in conducting audits or reviews of	Information Technology	Get handson experience using
University of Advancing	B.S	Technology Forensics	CFR227	200	1029	Knowledge of malware analysis	Computer Network Defense	Identify and evaluate different
University of Advancing	B.S	Technology Forensics	CFR227	200	1033	Knowledge of basic system	Information Systems/Network	Analyze and assess computer
University of Advancing	B.S	Technology Forensics	CFR227	200	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	Illustrate the basis for today's
University of Advancing	B.S	Technology Forensics	CFR227	200	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	Get handson experience using

University of Advancing	B.S	Technology Forensics	CFR227	200	1072	Knowledge of network security	Information Systems/Network	Analyze and assess computer
University of Advancing	B.S	Technology Forensics	CFR227	200	1087	Skill in deep analysis of captured malicious	Computer Network Defense	Identify and evaluate different
University of Advancing	B.S	Technology Forensics	CFR227	200	1114	Knowledge of encryption	Cryptography	Comprehend popular
University of Advancing	B.S	Technology Forensics	CFR227	200	1118	Skill in reading and interpreting	Information Systems/Network	Comprehend popular
University of Advancing	B.S	Technology Forensics	CFR255	200	19	Knowledge of Computer Network	Computer Network Defense	Explain the commonality of,
University of Advancing	B.S	Technology Forensics	CFR255	200	24	Knowledge of concepts and	Data Management	Test, validate, and understand the
University of Advancing	B.S	Technology Forensics	CFR255	200	59	Knowledge of Intrusion Detection	Computer Network Defense	Explain the commonality of,
University of Advancing	B.S	Technology Forensics	CFR255	200	77	Knowledege of current industry	Information Systems/Network	Explain the commonality of,
University of Advancing	B.S	Technology Forensics	CFR255	200	111	Knowledge of security system design tools,	Information Systems/Network	Explain the commonality of,
University of Advancing	B.S	Technology Forensics	CFR255	200	190	Skill in developing operationsbased	Systems Testing and Evaluation	Create and/or use a safe and
University of Advancing	B.S	Technology Forensics	CFR255	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	Explain the commonality of,
University of Advancing	B.S	Technology Forensics	CFR255	200	274	Knowledge of concepts, principles,	Computer Network Defense	Explain the commonality of,
University of Advancing	B.S	Technology Forensics	CFR255	200	360	Skill in identifying and extracting data of	Computer Forensics	Test, validate, and understand the
University of Advancing	B.S	Technology Forensics	CFR255	200	374	Skill in setting up a forensic workstation	Forensics	Test, validate, and understand the
University of Advancing	B.S	Technology Forensics	CFR255	200	379	Skill in using common digital forensics tools	Computer Forensics	Explain the commonality of,
University of Advancing	B.S	Technology Forensics	CFR255	200	381	Skill in using forensic tool suites (e.g.	Computer Forensics	Test, validate, and understand the
University of Advancing	B.S	Technology Forensics	CFR255	200	890	Skill in conducting forensic analyses in	Computer Forensics	Explain the commonality of,
University of Advancing	B.S	Technology Forensics	CFR255	200	1087	Skill in deep analysis of captured malicious	Computer Network Defense	Identify and describe the
University of Advancing	B.S	Technology Forensics	CFR255	200	1093	Knowledge of common forensic tool	Computer Forensics	Explain the commonality of,
University of Advancing	B.S	Technology Forensics	CFR255	200	1096	Knowledge of malware analysis	Computer Network Defense	Test, validate, and understand the
University of Advancing	B.S	Technology Forensics	CFR255	200	1099	Skill in analyzing volatile data	Computer Forensics	Identify and describe the
University of Advancing	B.S	Technology Forensics	NTS370	300	102	Knowledge of programming	Computer Languages	3. Develop basic programming
University of Advancing	B.S	Technology Forensics	NTS370	300	371	Skill in reading, interpreting, writing,	Operating Systems	1. Select and manipulate the
University of Advancing	B.S	Technology Forensics	NTS370	300	1063	Knowledge of Unix/Linux operating	Operating Systems	1. Select and manipulate the
University of Advancing	B.S	Network Security	NTS415	400	70	Knowledge of information	Information Systems/Network	1. Explain the essentials of
University of Advancing	B.S	Network Security	NTS415	400	77	Knowledege of current industry	Information Systems/Network	2. Discussing the components of
University of Advancing	B.S	Network Security	NTS415	400	87	Knowledge of network traffic	Information Systems/Network	3. Identify key packet filtering
University of Advancing	B.S	Network Security	NTS415	400	93	Knowledge of packetlevel analysis	Vulnerabilities Assessment	3. Identify key packet filtering
University of Advancing	B.S	Network Security	NTS415	400	109	Knowledge of secure configuration	Configuration Management	4. Provide a plan to fortify the
University of Advancing	B.S	Network Security	NTS415	400	111	Knowledge of security system design tools,	Information Systems/Network	4. Provide a plan to fortify the

University of Advancing	B.S	Network Security	NTS415	400	181	Skill in detecting host and network based	Computer Network Defense	7. Explain how to monitor
University of Advancing	B.S	Network Security	NTS415	400	277	Knowledge of defense indepth principles and	Computer Network Defense	6. Discuss the techniques used
University of Advancing	B.S	Network Security	NTS415	400	287	Knowledge of file system	Operating Systems	6. Discuss the techniques used
University of Advancing	B.S	Network Security	NTS435	400	4	Ability to identify systemic security	Vulnerabilities Assessment	3. Address the strengths and
University of Advancing	B.S	Network Security	NTS435	400	70	Knowledge of information	Information Systems/Network	1. Examine and identify key
University of Advancing	B.S	Network Security	NTS435	400	77	Knowledege of current industry	Information Systems/Network	1. Examine and identify key
University of Advancing	B.S	Network Security	NTS435	400	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	2. Identify the responsible
University of Advancing	B.S	Network Security	NTS435	400	183	Skill in determining how a security system	Information Assurance	4. Identify and describe the
University of Advancing	B.S	Network Security	NTS435	400	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	1. Examine and identify key
University of Advancing	B.S	Network Security	NTS435	400	300	Knowledge of intelligence reporting	Organizational Awareness	2. Identify the responsible
University of Advancing	B.S	Network Security	NTS442	400	9	Knowledge of applicable business	Requirements Analysis	3. Complete business related
University of Advancing	B.S	Network Security	NTS442	400	62	Knowledge of industrystandard and	Logical Systems Design	1. Configure a green team
University of Advancing	B.S	Network Security	NTS442	400	326	Knowledge of security hardware and	Information Systems/Network	4. Prevent violation of
University of Advancing	B.S	Network Security	NTS445	400	33	Knowledge of database procedures	Incident Management	1. Analyze and assess the
University of Advancing	B.S	Network Security	NTS445	400	37	Knowledge of disaster recovery and	Incident Management	1. Analyze and assess the
University of Advancing	B.S	Network Security	NTS445	400	60	Knowledge of incident categories, incident	Incident Management	3. Research and analyze incident
University of Advancing	B.S	Network Security	NTS445	400	61	Knowledge of incident response and	Incident Management	3. Research and analyze incident
University of Advancing	B.S	Network Security	NTS445	400	193	Skill in developing, testing, and	Information Assurance	4. Develop incident response
University of Advancing	B.S	Network Security	NTS445	400	229	Skill in using incident handling	Incident Management	2. Access the primary focus of
University of Advancing	B.S	Network Security	NTS445	400	966	Knowledge of enterprise incident	Incident Management	5. Understand the importance of
University of Advancing	B.S	Network Security	NTS465	400	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	1. Enumerate the required steps
University of Advancing	B.S	Network Security	NTS465	400	40	Knowledge of organization's	Systems Testing and Evaluation	6. Interface and interview mission
University of Advancing	B.S	Network Security	NTS465	400	77	Knowledege of current industry	Information Systems/Network	4. Conduct technical
University of Advancing	B.S	Network Security	NTS465	400	143	Knowledge of the organization’s	Enterprise Architecture	3. Define the Critical Path
University of Advancing	B.S	Network Security	NTS465	400	173	Skill in creating policies that relfect	Information Systems Security	2. Demonstrate the ability to help
University of Advancing	B.S	Network Security	NTW102	100	15	Knowledge of capabilities and	Hardware	Compare features,
University of Advancing	B.S	Network Security	NTW102	100	92	Knowledge of how traffic flows across	Infrastructure Design	2. Design a troubleshooting
University of Advancing	B.S	Network Security	NTW102	100	212	Skill in network mapping and	Infrastructure Design	1. Create a visual network
University of Advancing	B.S	Network Security	NTW102	100	234	Skill in using subnetting tools	Infrastructure Design	5. Demonstrate subnetting of IP
University of Advancing	B.S	Network Security	NTW102	100	322	Knowledge of router and routing	Infrastructure Design	7. Configure an industry standard

University of Advancing	B.S	Network Security	NTW213	200	12	Knowledge of communication	Infrastructure Design	3. Construct and manage an
University of Advancing	B.S	Network Security	NTW213	200	198	Skill in establishing a routing schema	Infrastructure Design	2. Design an enterprise
University of Advancing	B.S	Network Security	NTW213	200	993	Knowledge of the methods, standards,	Enterprise Architecture	1. Analyze and recommend
University of Advancing	B.S	Network Security	NTW216	200	113	Knowledge of server and client operating	Operating Systems	1. Install, configure and
University of Advancing	B.S	Network Security	NTW216	200	984	Knowledge of computer network	Computer Network Defense	2. Implement and manage secure
University of Advancing	B.S	Network Security	NTW216	200	1033	Knowledge of basic system	Information Systems/Network	3. Manage and secure access to
University of Advancing	B.S	Network Security	NTS201	200	17	Knowledge of certified ethical	Vulnerabilities Assessment	1. Apply the 12 principles of
University of Advancing	B.S	Network Security	NTS201	200	38	Knowledge of organization's	Information Assurance	5. Design a security program
University of Advancing	B.S	Network Security	NTS201	200	193	Skill in developing, testing, and	Information Assurance	6.Design an INFOSEC –
University of Advancing	B.S	Network Security	NTS201	200	916	Skill in deconflicting cyber operations and	Political Savvy	2. Evaluate and Peer Review the
University of Advancing	B.S	Network Security	NTS201	200	1070	Ability to determine impact of technology	Legal, Government and Jurisprudence	3. Analyze the impact of legal,
University of Advancing	B.S	Network Security	NTS225	200	23	Knowledge of computer	Object Technology	3. Layout a large C, C++, or C#
University of Advancing	B.S	Network Security	NTS225	200	102	Knowledge of programming	Computer Languages	4. Determine how to fix broken
University of Advancing	B.S	Network Security	NTS225	200	174	Skill in creating programs that	Software Testing and Evaluation	1. Skill in creating programs that
University of Advancing	B.S	Network Security	NTS225	200	904	Knowledge of interpreted and	Computer Languages	2. Understand the languages well
University of Advancing	B.S	Network Security	NTS310	300	52	Knowledge of humancomputer	Human Factors	1. Examine and evaluate the
University of Advancing	B.S	Network Security	NTS310	300	201	Skill in generating queries and reports	Database Management	3. Create, perform, and
University of Advancing	B.S	Network Security	NTS330	300	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	3. Apply standard hacking
University of Advancing	B.S	Network Security	NTS330	300	40	Knowledge of organization's	Systems Testing and Evaluation	5. Complete an industry standard
University of Advancing	B.S	Network Security	NTS330	300	177	Skill in designing countermeasures to	Vulnerabilities Assessment	4. Comprehend the prevention of
University of Advancing	B.S	Network Security	NTS330	300	377	Skill in tracking and analyzing technical	Legal, Government and Jurisprudence	1. Recognize and Discuss legal and
University of Advancing	B.S	Network Security	NTS330	300	922	Skill in using network analysis tools to	Vulnerabilities Assessment	2. Identify aspects of
University of Advancing	B.S	Network Security	NTS350	300	77	Knowledege of current industry	Information Systems/Network	1. Discuss the meaning of
University of Advancing	B.S	Network Security	NTS350	300	205	Skill in implementing, maintaining, and	Information Systems/Network	5. Define the best practices for
University of Advancing	B.S	Network Security	NTS350	300	231	Skill in using network management tools to	Network Management	6. Discuss the selection of the
University of Advancing	B.S	Network Security	NTS350	300	993	Knowledge of the methods, standards,	Enterprise Architecture	4. Develop network
University of Advancing	B.S	Network Security	NTS350	300	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	8. Develop an understanding of
University of Advancing	B.S	Network Security	NTS350	300	1073	Knowledge of network systems	Network Management	2. Understand the network
University of Advancing	B.S	Network Security	CFR410	400	33	Knowledge of database procedures	Incident Management	Conduct a thourough
University of Advancing	B.S	Network Security	CFR410	400	37	Knowledge of disaster recovery and	Incident Management	Conduct a thourough

University of Advancing	B.S	Network Security	CFR410	400	60	Knowledge of incident categories, incident	Incident Management	Conduct a thourough
University of Advancing	B.S	Network Security	CFR410	400	61	Knowledge of incident response and	Incident Management	Conduct a thourough
University of Advancing	B.S	Network Security	CFR410	400	122	Knowledge of system administration	Operating Systems	Explain Windows network exploits.
University of Advancing	B.S	Network Security	CFR410	400	166	Skill in conducting queries and	Database Management	Analyze live systems
University of Advancing	B.S	Network Security	CFR410	400	216	Skill in recovering failed servers	Incident Management	Conduct a thourough
University of Advancing	B.S	Network Security	CFR410	400	229	Skill in using incident handling	Incident Management	Conduct a thourough
University of Advancing	B.S	Network Security	CFR410	400	231	Skill in using network management tools to	Network Management	Analyze live systems
University of Advancing	B.S	Network Security	CFR410	400	233	Skill in using protocol analyzers	Vulnerabilities Assessment	Analyze live systems
University of Advancing	B.S	Network Security	CFR410	400	294	Knowledge of hacking methodologies in	Surveillance	Explain Windows network exploits.
University of Advancing	B.S	Network Security	CFR410	400	341	Knowledge of UNIX and Windows systems	Operating Systems	Explain Windows network exploits.
University of Advancing	B.S	Network Security	CFR410	400	346	Knowledge of which system files (e.g. log	Computer Forensics	Analyze log files
University of Advancing	B.S	Network Security	CFR410	400	347	Knowledge of Windows command	Operating Systems	Explain Windows network exploits.
University of Advancing	B.S	Network Security	CFR410	400	364	Skill in identifying, modifying, and	Operating Systems	Explain Windows network exploits.
University of Advancing	B.S	Network Security	CFR410	400	371	Skill in reading, interpreting, writing,	Operating Systems	Explain Windows network exploits.
University of Advancing	B.S	Network Security	CFR410	400	978	Knowledge of root cause analysis for	Incident Management	Conduct a thourough
University of Advancing	B.S	Network Security	CFR410	400	980	Skill in performing root cause analysis for	Incident Management	Conduct a thourough
University of Advancing	B.S	Network Security	CFR410	400	1011	Knowledge of processes for	Security	Conduct a thourough
University of Advancing	B.S	Network Security	CFR410	400	1121	Knowledge of Windows/Unix ports	Operating Systems	Explain Windows network exploits.
Norwich University	B.S.	Computer Security and	IS 240	200	32	Knowledge of database	Database Management	Describe and apply data
Norwich University	B.S.	Computer Security and	IS 240	200	34	Knowledge of database systems	Database Management	Learn to use the technical
Norwich University	B.S.	Computer Security and	IS 240	200	104	Knowledge of query languages such as	Database Management	Apply the relational model
Norwich University	B.S.	Computer Security and	IS 240	200	166	Skill in conducting queries and	Database Management	Learn to use SQL using the
Norwich University	B.S.	Computer Security and	IS 240	200	201	Skill in generating queries and reports	Database Management	Learn to use SQL using the
Norwich University	B.S.	Computer Security and	IS 340	300	8	Knowledge of access authentication	Identity Management	Recognize, name, define, and
Norwich University	B.S.	Computer Security and	IS 340	300	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	Recognize, name, define, and
Norwich University	B.S.	Computer Security and	IS 340	300	27	Knowledge of cryptology	Cryptography	Recognize, name, define, and
Norwich University	B.S.	Computer Security and	IS 340	300	177	Skill in designing countermeasures to	Vulnerabilities Assessment	Recognize, name, define and
Norwich University	B.S.	Computer Security and	IS 340	300	329	Knowledge of surveillance detection	Surveillance	Recognize, name, define and
Norwich University	B.S.	Computer Security and	IS 340	300	891	Skill in configuring and utilizing	Configuration Management	Recognize, name, define, and
Norwich University	B.S.	Computer Security and	IS 340	300	985	Skill in configuring and utilizing network	Configuration Management	Recognize, name, define, and

Norwich University	B.S.	Computer Security and	IS 340	300	989	Knowledge of Voice over Internet Protocol	Telecommunications	Discuss specific security issues
Norwich University	B.S.	Computer Security and	IS 340	300	990	Knowledge of common attack	Computer Network Defense	Discuss specific security issues
Norwich University	B.S.	Computer Security and	IS 340	300	1114	Knowledge of encryption	Cryptography	Recognize, name, define, and
Norwich University	B.S.	Computer Security and	CJ341	300	305	Knowledge of laws that affect cyber	Forensics	Identify and discuss the key
Norwich University	B.S.	Computer Security and	CJ341	300	316	Knowledge of processes for	Criminal Law	Describe how to seize, preserve,
Norwich University	B.S.	Computer Security and	CJ341	300	369	Skill in collecting, processing,	Forensics	Describe how to seize, preserve,
Norwich University	B.S.	Computer Security and	CJ341	300	982	Knowledge of electronic evidence	Criminal Law	Define the international
Norwich University	B.S.	Computer Security and	CJ341	300	1036	Knowledge of applicable laws (e.g.,	Criminal Law	Intelligently discuss legal and
Norwich University	B.S.	Computer Security and	CJ341	300	1040	Knowledge of relevant laws,	Criminal Law	Identify and discuss the key
Norwich University	B.S.	Computer Security and	IS342	300	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Vulnerabilities assessments
Norwich University	B.S.	Computer Security and	IS342	300	29	Knowledge of data backup, types of	Computer Forensics	Data backup and recovery
Norwich University	B.S.	Computer Security and	IS342	300	37	Knowledge of disaster recovery and	Incident Management	Disaster recovery plans.
Norwich University	B.S.	Computer Security and	IS342	300	55	Knowledge of Information	Information Assurance	Modern principles of risk
Norwich University	B.S.	Computer Security and	IS342	300	108	Knowledge of risk management	Risk Management	Modern principles of risk
Norwich University	B.S.	Computer Security and	IS342	300	118	Knowledge of software	Software Engineering	Software development and
Norwich University	B.S.	Computer Security and	IS342	300	126	Knowledge of system software and	Requirements Analysis	Guidelines for effective security
Norwich University	B.S.	Computer Security and	IS342	300	173	Skill in creating policies that relfect	Information Systems Security	Guidelines for effective security
Norwich University	B.S.	Computer Security and	IS342	300	300	Knowledge of intelligence reporting	Organizational Awareness	US legal and regulatory issues
Norwich University	B.S.	Computer Security and	IS342	300	356	Skill in determining installed patches on	Operating Systems	Managing patches and
Norwich University	B.S.	Computer Security and	IS342	300	895	Skill in recognizing and categorizing	Information Assurance	Vulnerabilities assessments
Norwich University	B.S.	Computer Security and	IS342	300	922	Skill in using network analysis tools to	Vulnerabilities Assessment	Vulnerabilities assessments
Norwich University	B.S.	Computer Security and	IS342	300	952	Knowledge of emerging security	Technology Awareness	Modern principles of risk
Norwich University	B.S.	Computer Security and	IS342	300	976	Knowledge of software quality	Software Engineering	Software development and
Norwich University	B.S.	Computer Security and	IS342	300	1002	Skill in conducting audits or reviews of	Information Technology	Audit and control of information
Norwich University	B.S.	Computer Security and	IS342	300	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	Vulnerabilities assessments
Norwich University	B.S.	Computer Security and	IS407	400	134	Knowledge of the capabilities and	Technology Awareness	Evolving concepts of social
Norwich University	B.S.	Computer Security and	IS455	400	107	Knowledge of resource	Project Management	· What are the factors that
Norwich University	B.S.	Computer Security and	IS455	400	299	Knowledge of information security	Project Management	· What are the factors that
Florida State College at	A.S	Computer Forensics	CAP 2140	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	01.09 Identify and discuss issues
Florida State College at	A.S	Computer Forensics	CAP 2140	200	4	Ability to identify systemic security	Vulnerabilities Assessment	01.09 Identify and discuss issues

Florida State College at	A.S	Computer Forensics	CAP 2140	200	112	Knowledge of server administration and	Systems Life Cycle	08.15 Address security issues
Florida State College at	A.S	Computer Forensics	CAP 2140	200	126	Knowledge of system software and	Requirements Analysis	08.02 Establish, document and
Florida State College at	A.S	Computer Forensics	CAP 2140	200	145	Knowledge of the type and frequency of	Systems Life Cycle	04.05 Use system software to
Florida State College at	A.S	Computer Forensics	CAP 2140	200	167	Skill in conducting server planning,	Network Management	08.15 Address security issues
Florida State College at	A.S	Computer Forensics	CAP 2140	200	206	Skill in installing computer and server	Systems Life Cycle	12.03 Evaluating skills and taking
Florida State College at	A.S	Computer Forensics	CAP 2140	200	264	Knowledge of basic physical computer	Computers and Electronics	04.01 Describe the functions and
Florida State College at	A.S	Computer Forensics	CAP 2140	200	892	Skill in configuring and utilizing	Configuration Management	08.12 Install and update antivirus
Florida State College at	A.S	Computer Forensics	CAP 2140	200	952	Knowledge of emerging security	Technology Awareness	01.09 Identify and discuss issues
Florida State College at	A.S	Computer Forensics	CAP 2140	200	984	Knowledge of computer network	Computer Network Defense	08.11 Document security policies
Florida State College at	A.S	Computer Forensics	CAP 2140	200	986	Knowledge of organizational	Identity Management	08.11 Document security policies
Florida State College at	A.S	Computer Forensics	CAP 2140	200	1037	Knowledge of information	Risk Management	08.11 Document security policies
Florida State College at	A.S	Computer Forensics	CAP 2140	200	1073	Knowledge of network systems	Network Management	08.08 Perform network
Florida State College at	A.S	Computer Forensics	CAP 2141	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	01.09 Identify and discuss issues
Florida State College at	A.S	Computer Forensics	CAP 2141	200	4	Ability to identify systemic security	Vulnerabilities Assessment	01.09 Identify and discuss issues
Florida State College at	A.S	Computer Forensics	CAP 2141	200	112	Knowledge of server administration and	Systems Life Cycle	08.15 Address security issues
Florida State College at	A.S	Computer Forensics	CAP 2141	200	126	Knowledge of system software and	Requirements Analysis	08.02 Establish, document and
Florida State College at	A.S	Computer Forensics	CAP 2141	200	145	Knowledge of the type and frequency of	Systems Life Cycle	04.05 Use system software to
Florida State College at	A.S	Computer Forensics	CAP 2141	200	167	Skill in conducting server planning,	Network Management	08.15 Address security issues
Florida State College at	A.S	Computer Forensics	CAP 2141	200	206	Skill in installing computer and server	Systems Life Cycle	12.03 Evaluating skills and taking
Florida State College at	A.S	Computer Forensics	CAP 2141	200	264	Knowledge of basic physical computer	Computers and Electronics	04.01 Describe the functions and
Florida State College at	A.S	Computer Forensics	CAP 2141	200	892	Skill in configuring and utilizing	Configuration Management	08.12 Install and update antivirus
Florida State College at	A.S	Computer Forensics	CAP 2141	200	952	Knowledge of emerging security	Technology Awareness	01.09 Identify and discuss issues
Florida State College at	A.S	Computer Forensics	CAP 2141	200	984	Knowledge of computer network	Computer Network Defense	08.11 Document security policies
Florida State College at	A.S	Computer Forensics	CAP 2141	200	986	Knowledge of organizational	Identity Management	08.11 Document security policies
Florida State College at	A.S	Computer Forensics	CAP 2141	200	1037	Knowledge of information	Risk Management	08.11 Document security policies
Florida State College at	A.S	Computer Forensics	CAP 2141	200	1073	Knowledge of network systems	Network Management	08.08 Perform network
Florida State College at	A.S	Biomedical Engineering	CET 1114	100	75	Knowledge of mathematics,	Mathematical Reasoning	13.01 Add, subtract, multiply
Florida State College at	A.S	Biomedical Engineering	CET 1114	100	264	Knowledge of basic physical computer	Computers and Electronics	07.08 Understand computer
Florida State College at	A.S	Biomedical Engineering	CET 1114	100	349	Skill in analyzing data from a variety of	Reasoning	07.01 Understand basic electrical
Florida State College at	A.S	Biomedical Engineering	CET 1114	100	360	Skill in identifying and extracting data of	Computer Forensics	07.07 Understand data acquisition

Florida State College at	A.S	Biomedical Engineering	CET 1114	100	1038	Knowledge of local specialized system	Infrastructure Design	07.15 Demonstrate
Florida State College at	N/A	N/A	CET1173	100	16	Knowledge of capabilities and	Requirements Analysis	06.01 Understand basic network
Florida State College at	N/A	N/A	CET1173	100	22	Knowledge of computer networking	Infrastructure Design	06.01 Understand basic network
Florida State College at	N/A	N/A	CET1173	100	32	Knowledge of database	Database Management	03.07 Demonstrate
Florida State College at	N/A	N/A	CET1173	100	34	Knowledge of database systems	Database Management	03.02 Understand database
Florida State College at	N/A	N/A	CET1173	100	81	Knowledge of network	Infrastructure Design	06.04 Demonstrate
Florida State College at	N/A	N/A	CET1173	100	90	Knowledge of operating systems	Operating Systems	02.01 Load and run operating
Florida State College at	N/A	N/A	CET1173	100	92	Knowledge of how traffic flows across	Infrastructure Design	06.04 Demonstrate
Florida State College at	N/A	N/A	CET1173	100	128	Knowledge of systems diagnostic tools and	Systems Testing and Evaluation	02.02 Load and run diagnostic
Florida State College at	N/A	N/A	CET1173	100	139	Knowledge of common networking	Infrastructure Design	06.04 Demonstrate
Florida State College at	N/A	N/A	CET1173	100	201	Skill in generating queries and reports	Database Management	03.07 Demonstrate
Florida State College at	N/A	N/A	CET1173	100	278	Knowledge of different types of	Telecommunicatio ns	06.03 Demonstrate
Florida State College at	N/A	N/A	CET1173	100	287	Knowledge of file system	Operating Systems	09.03 Describe various disk
Florida State College at	N/A	N/A	CET1173	100	347	Knowledge of Windows command	Operating Systems	09.08 Program using the
Florida State College at	N/A	N/A	CET1173	100	902	Knowledge of the range of existing	Network Management	06.03 Demonstrate
Florida State College at	N/A	N/A	CET1513	100	90	Knowledge of operating systems	Operating Systems	02.01 Load and run operating
Florida State College at	N/A	N/A	CET1513	100	128	Knowledge of systems diagnostic tools and	Systems Testing and Evaluation	02.02 Load and run diagnostic
Florida State College at	N/A	N/A	CET1513	100	287	Knowledge of file system	Operating Systems	09.03 Describe various disk
Florida State College at	N/A	N/A	CET1513	100	347	Knowledge of Windows command	Operating Systems	09.08 Program using the
Florida State College at	A.S	Engineering Technology	CET 1630	100	9	Knowledge of applicable business	Requirements Analysis	05.02 Calculate and determine
Florida State College at	A.S	Engineering Technology	CET 1630	100	16	Knowledge of capabilities and	Requirements Analysis	05.02 Calculate and determine
Florida State College at	A.S	Engineering Technology	CET 1630	100	1038	Knowledge of local specialized system	Infrastructure Design	05.02 Calculate and determine
Florida State College at	N/A	N/A	CET 1936	100	9	Knowledge of applicable business	Requirements Analysis	05.02 Calculate and determine
Florida State College at	N/A	N/A	CET 1936	100	16	Knowledge of capabilities and	Requirements Analysis	05.02 Calculate and determine
Florida State College at	N/A	N/A	CET 1936	100	1038	Knowledge of local specialized system	Infrastructure Design	05.02 Calculate and determine
Florida State College at	N/A	N/A	CET2172	200	18	Knowledge of circuit analysis	Computers and Electronics	07.13 Demonstrate
Florida State College at	N/A	N/A	CET2172	200	42	Knowledge of electrical engineering	Hardware Engineering	07.01 Understand basic electrical
Florida State College at	N/A	N/A	CET2172	200	43	Knowledge of embedded systems	Embedded Computers	07.07 Understand microprocessors
Florida State College at	N/A	N/A	CET2172	200	52	Knowledge of humancomputer	Human Factors	11.08 Pointing devices for
Florida State College at	N/A	N/A	CET2172	200	78	Knowledge of microprocessors	Computers and Electronics	07.07 Understand microprocessors

Florida State College at	N/A	N/A	CET2172	200	121	Knowledge of structured analysis	Logical Systems Design	01.01 Draw and explain systems
Florida State College at	N/A	N/A	CET2172	200	137	Knowledge of the characteristics of	Data Management	11.02 Analyze various types of
Florida State College at	N/A	N/A	CET2172	200	143	Knowledge of the organization’s	Enterprise Architecture	12.02 Read and understand
Florida State College at	N/A	N/A	CET2172	200	235	Skill in using the appropriate tools for	Computers and Electronics	02.09 Analyze firmware
Florida State College at	N/A	N/A	CET2172	200	264	Knowledge of basic physical computer	Computers and Electronics	07.10 Understand computer
Florida State College at	N/A	N/A	CET2172	200	340	Knowledge of types and collection of	Computer Forensics	07.09 Understand data acquisition
Florida State College at	N/A	N/A	CET2172	200	942	Knowledge of the organization's core	Organizational Awareness	12.02 Read and understand
Florida State College at	N/A	N/A	CET2172	200	986	Knowledge of organizational	Identity Management	12.02 Read and understand
Florida State College at	N/A	N/A	CET2179	200	43	Knowledge of embedded systems	Embedded Computers	03.02 Identify, define and
Florida State College at	N/A	N/A	CET2179	200	76	Knowledge of measures or	Information Technology	03.04 Identify and define
Florida State College at	N/A	N/A	CET2179	200	81	Knowledge of network	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2179	200	92	Knowledge of how traffic flows across	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2179	200	96	Knowledge of performance tuning	Information Technology	03.04 Identify and define
Florida State College at	N/A	N/A	CET2179	200	137	Knowledge of the characteristics of	Data Management	04.06 Define environmental
Florida State College at	N/A	N/A	CET2179	200	139	Knowledge of common networking	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2179	200	154	Skill in analyzing network traffic	Capacity Management	03.04 Identify and define
Florida State College at	N/A	N/A	CET2179	200	264	Knowledge of basic physical computer	Computers and Electronics	03.01 Identify and define serial
Florida State College at	N/A	N/A	CET2179	200	287	Knowledge of file system	Operating Systems	09.03 Describe various disk
Florida State College at	N/A	N/A	CET2179	200	322	Knowledge of router and routing	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2179	200	364	Skill in identifying, modifying, and	Operating Systems	03.07 Identify and define
Florida State College at	N/A	N/A	CET2179	200	901	Knowledge of the capabilities of	Network Management	03.05 Identify and define
Florida State College at	N/A	N/A	CET2179	200	1002	Skill in conducting audits or reviews of	Information Technology	03.04 Identify and define
Florida State College at	N/A	N/A	CET2179	200	1038	Knowledge of local specialized system	Infrastructure Design	03.04 Identify and define
Florida State College at	N/A	N/A	CET2179	200	1073	Knowledge of network systems	Network Management	03.04 Identify and define
Florida State College at	A.S	Networking Services	CET2588	200	15	Knowledge of capabilities and	Hardware	01.21 Design a LAN, including
Florida State College at	A.S	Networking Services	CET2588	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	08.13 Describe current
Florida State College at	A.S	Networking Services	CET2588	200	29	Knowledge of data backup, types of	Computer Forensics	04.05 Use system software to
Florida State College at	A.S	Networking Services	CET2588	200	63	Knowledge of Information	Information Assurance	07.18 Explain three major
Florida State College at	A.S	Networking Services	CET2588	200	70	Knowledge of information	Information Systems/Network	08.14 Describe the functions and
Florida State College at	A.S	Networking Services	CET2588	200	72	Knowledge of local area network (LAN)	Infrastructure Design	08.35 Describe typical WAN links

Florida State College at	A.S	Networking Services	CET2588	200	77	Knowledege of current industry	Information Systems/Network	08.08 Perform network
Florida State College at	A.S	Networking Services	CET2588	200	79	Knowledge of network access,	Identity Management	08.13 Describe current
Florida State College at	A.S	Networking Services	CET2588	200	82	Knowledge of network design	Infrastructure Design	01.07 Identify several
Florida State College at	A.S	Networking Services	CET2588	200	83	Knowledge of network hardware	Hardware	01.21 Design a LAN, including
Florida State College at	A.S	Networking Services	CET2588	200	88	Knowledge of new and emerging	Technology Awareness	01.18 Identify major emerging
Florida State College at	A.S	Networking Services	CET2588	200	92	Knowledge of how traffic flows across	Infrastructure Design	01.11 List and define layers in
Florida State College at	A.S	Networking Services	CET2588	200	113	Knowledge of server and client operating	Operating Systems	06.02 Compare and contrast
Florida State College at	A.S	Networking Services	CET2588	200	128	Knowledge of systems diagnostic tools and	Systems Testing and Evaluation	09.01 Describe the use and
Florida State College at	A.S	Networking Services	CET2588	200	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	03.13 Design and implement test
Florida State College at	A.S	Networking Services	CET2588	200	133	Knowledge of telecommunications	Telecommunications	02.01 Differentiate
Florida State College at	A.S	Networking Services	CET2588	200	142	Knowledge of the operations and	Systems Life Cycle	09.02 Describe effective
Florida State College at	A.S	Networking Services	CET2588	200	145	Knowledge of the type and frequency of	Systems Life Cycle	04.05 Use system software to
Florida State College at	A.S	Networking Services	CET2588	200	156	Skill in applying confidentiality,	Information Assurance	08.08 Perform network
Florida State College at	A.S	Networking Services	CET2588	200	194	Skill in diagnosing connectivity problems	Network Management	09.05 Trace for connectivity
Florida State College at	A.S	Networking Services	CET2588	200	212	Skill in network mapping and	Infrastructure Design	01.13 Illustrate typical network
Florida State College at	A.S	Networking Services	CET2588	200	221	Skill in testing and configuring network	Network Management	05.15 Describe the requirements
Florida State College at	A.S	Networking Services	CET2588	200	261	Knowledge of basic concepts,	Telecommunications	02.03 Compare and contrast
Florida State College at	A.S	Networking Services	CET2588	200	278	Knowledge of different types of	Telecommunications	05.10 Identify advantages and
Florida State College at	A.S	Networking Services	CET2588	200	281	Knowledge of electronic devices	Hardware	02.05 Describe the functioning of
Florida State College at	A.S	Networking Services	CET2588	200	341	Knowledge of UNIX and Windows systems	Operating Systems	08.16 Discuss the functions of
Florida State College at	A.S	Networking Services	CET2588	200	346	Knowledge of which system files (e.g. log	Computer Forensics	04.08 Create, use, and maintain
Florida State College at	A.S	Networking Services	CET2588	200	364	Skill in identifying, modifying, and	Operating Systems	01.10 Identify and discuss issues
Florida State College at	A.S	Networking Services	CET2588	200	952	Knowledge of emerging security	Technology Awareness	01.18 Identify major emerging
Florida State College at	A.S	Networking Services	CET2588	200	985	Skill in configuring and utilizing network	Configuration Management	08.16 Discuss the functions of
Florida State College at	A.S	Networking Services	CET2588	200	1008	Knowledge of how to troubleshoot basic	Operating Systems	09.02 Describe effective
Florida State College at	A.S	Networking Services	CET2588	200	1037	Knowledge of information	Risk Management	08.09 Establish procedures for
Florida State College at	A.S	Networking Services	CET2588	200	1063	Knowledge of Unix/Linux operating	Operating Systems	04.06 Use operating
Florida State College at	A.S	Networking Services	CET2588	200	1115	Skill in reading Hexadecimal data	Computer Languages	01.03 Convert numbers among
Florida State College at	A.S	Networking Services	CET2588	200	1116	Skill in identifying common encoding	Computer Languages	01.05 Identify various coding
Florida State College at	B.S	Information Technology	CET2600	200	15	Knowledge of capabilities and	Hardware	01.21 Design a LAN, including

Florida State College at	B.S	Information Technology	CET2600	200	16	Knowledge of capabilities and	Requirements Analysis	06.01 Understand basic network
Florida State College at	B.S	Information Technology	CET2600	200	22	Knowledge of computer networking	Infrastructure Design	06.01 Understand basic network
Florida State College at	B.S	Information Technology	CET2600	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	08.13 Describe current
Florida State College at	B.S	Information Technology	CET2600	200	29	Knowledge of data backup, types of	Computer Forensics	04.05 Use system software to
Florida State College at	B.S	Information Technology	CET2600	200	35	Knowledge of digital rights management	Encryption	14.10 Identify and discuss
Florida State College at	B.S	Information Technology	CET2600	200	41	Knowledge of organization's Local	Infrastructure Design	01.21 Design a LAN, including
Florida State College at	B.S	Information Technology	CET2600	200	63	Knowledge of Information	Information Assurance	07.18 Explain three major
Florida State College at	B.S	Information Technology	CET2600	200	70	Knowledge of information	Information Systems/Network	07.16 Explain the function and
Florida State College at	B.S	Information Technology	CET2600	200	72	Knowledge of local area network (LAN)	Infrastructure Design	07.02 Differentiate
Florida State College at	B.S	Information Technology	CET2600	200	75	Knowledge of mathematics,	Mathematical Reasoning	13.01 Add, subtract, multiply
Florida State College at	B.S	Information Technology	CET2600	200	77	Knowledege of current industry	Information Systems/Network	08.08 Perform network
Florida State College at	B.S	Information Technology	CET2600	200	79	Knowledge of network access,	Identity Management	08.13 Describe current
Florida State College at	B.S	Information Technology	CET2600	200	81	Knowledge of network	Infrastructure Design	03.05 Identify and define
Florida State College at	B.S	Information Technology	CET2600	200	82	Knowledge of network design	Infrastructure Design	01.07 Identify several
Florida State College at	B.S	Information Technology	CET2600	200	83	Knowledge of network hardware	Hardware	01.21 Design a LAN, including
Florida State College at	B.S	Information Technology	CET2600	200	88	Knowledge of new and emerging	Technology Awareness	01.18 Identify major emerging
Florida State College at	B.S	Information Technology	CET2600	200	90	Knowledge of operating systems	Operating Systems	04.02 Identify current operating
Florida State College at	B.S	Information Technology	CET2600	200	92	Knowledge of how traffic flows across	Infrastructure Design	01.11 List and define layers in
Florida State College at	B.S	Information Technology	CET2600	200	113	Knowledge of server and client operating	Operating Systems	06.02 Compare and contrast
Florida State College at	B.S	Information Technology	CET2600	200	122	Knowledge of system administration	Operating Systems	04.01 Describe the functions and
Florida State College at	B.S	Information Technology	CET2600	200	126	Knowledge of system software and	Requirements Analysis	08.03 Create and test account
Florida State College at	B.S	Information Technology	CET2600	200	128	Knowledge of systems diagnostic tools and	Systems Testing and Evaluation	09.01 Describe the use and
Florida State College at	B.S	Information Technology	CET2600	200	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	03.13 Design and implement test
Florida State College at	B.S	Information Technology	CET2600	200	133	Knowledge of telecommunications	Telecommunications	02.01 Differentiate
Florida State College at	B.S	Information Technology	CET2600	200	139	Knowledge of common networking	Infrastructure Design	06.04 Demonstrate
Florida State College at	B.S	Information Technology	CET2600	200	142	Knowledge of the operations and	Systems Life Cycle	09.02 Describe effective
Florida State College at	B.S	Information Technology	CET2600	200	145	Knowledge of the type and frequency of	Systems Life Cycle	04.05 Use system software to
Florida State College at	B.S	Information Technology	CET2600	200	156	Skill in applying confidentiality,	Information Assurance	08.08 Perform network
Florida State College at	B.S	Information Technology	CET2600	200	167	Skill in conducting server planning,	Network Management	09.12 Define windows of
Florida State College at	B.S	Information Technology	CET2600	200	194	Skill in diagnosing connectivity problems	Network Management	09.05 Trace for connectivity

Florida State College at	B.S	Information Technology	CET2600	200	204	Skill in identifying possible causes of	Systems Life Cycle	09.13 Determine type of
Florida State College at	B.S	Information Technology	CET2600	200	205	Skill in implementing, maintaining, and	Information Systems/Network	09.14 Determine service intervals
Florida State College at	B.S	Information Technology	CET2600	200	212	Skill in network mapping and	Infrastructure Design	01.13 Illustrate typical network
Florida State College at	B.S	Information Technology	CET2600	200	221	Skill in testing and configuring network	Network Management	05.15 Describe the requirements
Florida State College at	B.S	Information Technology	CET2600	200	231	Skill in using network management tools to	Network Management	08.29 Use network
Florida State College at	B.S	Information Technology	CET2600	200	261	Knowledge of basic concepts,	Telecommunications	02.03 Compare and contrast
Florida State College at	B.S	Information Technology	CET2600	200	264	Knowledge of basic physical computer	Computers and Electronics	05.01 Describe the major
Florida State College at	B.S	Information Technology	CET2600	200	278	Knowledge of different types of	Telecommunications	05.10 Identify advantages and
Florida State College at	B.S	Information Technology	CET2600	200	281	Knowledge of electronic devices	Hardware	02.05 Describe the functioning of
Florida State College at	B.S	Information Technology	CET2600	200	322	Knowledge of router and routing	Infrastructure Design	07.03 Compare and contrast
Florida State College at	B.S	Information Technology	CET2600	200	332	Ability to develop curriculum that	Teaching Others	11.06 Develop an ongoing training
Florida State College at	B.S	Information Technology	CET2600	200	341	Knowledge of UNIX and Windows systems	Operating Systems	08.16 Discuss the functions of
Florida State College at	B.S	Information Technology	CET2600	200	346	Knowledge of which system files (e.g. log	Computer Forensics	04.08 Create, use, and maintain
Florida State College at	B.S	Information Technology	CET2600	200	347	Knowledge of Windows command	Operating Systems	06.02 Understand basic network
Florida State College at	B.S	Information Technology	CET2600	200	349	Skill in analyzing data from a variety of	Reasoning	07.01 Understand basic electrical
Florida State College at	B.S	Information Technology	CET2600	200	358	Skill in determining tactics, techniques,	Strategic Thinking	09.07 Follow standard
Florida State College at	B.S	Information Technology	CET2600	200	360	Skill in identifying and extracting data of	Computer Forensics	07.07 Understand data acquisition
Florida State College at	B.S	Information Technology	CET2600	200	364	Skill in identifying, modifying, and	Operating Systems	01.10 Identify and discuss issues
Florida State College at	B.S	Information Technology	CET2600	200	902	Knowledge of the range of existing	Network Management	06.03 Demonstrate
Florida State College at	B.S	Information Technology	CET2600	200	915	Knowledge of frontend collection	Information Systems/Network	07.17 Configure access lists to
Florida State College at	B.S	Information Technology	CET2600	200	952	Knowledge of emerging security	Technology Awareness	01.18 Identify major emerging
Florida State College at	B.S	Information Technology	CET2600	200	985	Skill in configuring and utilizing network	Configuration Management	08.16 Discuss the functions of
Florida State College at	B.S	Information Technology	CET2600	200	986	Knowledge of organizational	Identity Management	08.05 Grant/deny access to
Florida State College at	B.S	Information Technology	CET2600	200	1008	Knowledge of how to troubleshoot basic	Operating Systems	09.02 Describe effective
Florida State College at	B.S	Information Technology	CET2600	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	14.12 Identify and discuss
Florida State College at	B.S	Information Technology	CET2600	200	1037	Knowledge of information	Risk Management	08.09 Establish procedures for
Florida State College at	B.S	Information Technology	CET2600	200	1038	Knowledge of local specialized system	Infrastructure Design	07.15 Demonstrate
Florida State College at	B.S	Information Technology	CET2600	200	1063	Knowledge of Unix/Linux operating	Operating Systems	04.06 Use operating
Florida State College at	B.S	Information Technology	CET2600	200	1073	Knowledge of network systems	Network Management	08.30 Explain RMON and SNMP
Florida State College at	B.S	Information Technology	CET2600	200	1114	Knowledge of encryption	Cryptography	14.13 Identify and discuss

Florida State College at	B.S	Information Technology	CET2600	200	1115	Skill in reading Hexadecimal data	Computer Languages	01.03 Convert numbers among
Florida State College at	B.S	Information Technology	CET2600	200	1116	Skill in identifying common encoding	Computer Languages	01.05 Identify various coding
Florida State College at	A.S	Networking Services	CET2629	200	15	Knowledge of capabilities and	Hardware	01.21 Design a LAN, including
Florida State College at	A.S	Networking Services	CET2629	200	63	Knowledge of Information	Information Assurance	07.18 Explain three major
Florida State College at	A.S	Networking Services	CET2629	200	82	Knowledge of network design	Infrastructure Design	01.09 Identify and discuss issues
Florida State College at	A.S	Networking Services	CET2629	200	83	Knowledge of network hardware	Hardware	01.21 Design a LAN, including
Florida State College at	A.S	Networking Services	CET2629	200	88	Knowledge of new and emerging	Technology Awareness	01.18 Identify major emerging
Florida State College at	A.S	Networking Services	CET2629	200	92	Knowledge of how traffic flows across	Infrastructure Design	07.06 Explain how the first
Florida State College at	A.S	Networking Services	CET2629	200	142	Knowledge of the operations and	Systems Life Cycle	09.02 Describe effective
Florida State College at	A.S	Networking Services	CET2629	200	156	Skill in applying confidentiality,	Information Assurance	08.08 Perform network
Florida State College at	A.S	Networking Services	CET2629	200	167	Skill in conducting server planning,	Network Management	12.03 Evaluating skills and taking
Florida State College at	A.S	Networking Services	CET2629	200	194	Skill in diagnosing connectivity problems	Network Management	09.05 Trace for connectivity
Florida State College at	A.S	Networking Services	CET2629	200	212	Skill in network mapping and	Infrastructure Design	01.13 Illustrate typical network
Florida State College at	A.S	Networking Services	CET2629	200	221	Skill in testing and configuring network	Network Management	05.15 Describe the requirements
Florida State College at	A.S	Networking Services	CET2629	200	231	Skill in using network management tools to	Network Management	08.29 Use network
Florida State College at	A.S	Networking Services	CET2629	200	261	Knowledge of basic concepts,	Telecommunications	05.09 Describe current wireless
Florida State College at	A.S	Networking Services	CET2629	200	264	Knowledge of basic physical computer	Computers and Electronics	07.08 Understand computer
Florida State College at	A.S	Networking Services	CET2629	200	278	Knowledge of different types of	Telecommunications	05.10 Identify advantages and
Florida State College at	A.S	Networking Services	CET2629	200	346	Knowledge of which system files (e.g. log	Computer Forensics	09.03 Recognize and resolve basic
Florida State College at	A.S	Networking Services	CET2629	200	358	Skill in determining tactics, techniques,	Strategic Thinking	09.07 Follow standard
Florida State College at	A.S	Networking Services	CET2629	200	364	Skill in identifying, modifying, and	Operating Systems	01.10 Identify and discuss issues
Florida State College at	A.S	Networking Services	CET2629	200	915	Knowledge of frontend collection	Information Systems/Network	07.17 Configure access lists to
Florida State College at	A.S	Networking Services	CET2629	200	918	Ability to prepare and deliver education and	Teaching Others	14.03 Participate in group
Florida State College at	A.S	Networking Services	CET2629	200	952	Knowledge of emerging security	Technology Awareness	01.18 Identify major emerging
Florida State College at	A.S	Networking Services	CET2629	200	986	Knowledge of organizational	Identity Management	08.05 Grant/deny access to
Florida State College at	A.S	Networking Services	CET2629	200	1008	Knowledge of how to troubleshoot basic	Operating Systems	09.02 Describe effective
Florida State College at	A.S	Networking Services	CET2629	200	1038	Knowledge of local specialized system	Infrastructure Design	07.15 Demonstrate
Florida State College at	Certifica	Program Computer	CET2662	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	06.05 Employ cryptographic
Florida State College at	Certifica	Program Computer	CET2662	200	35	Knowledge of digital rights management	Encryption	18.09 Identify and discuss
Florida State College at	Certifica	Program Computer	CET2662	200	37	Knowledge of disaster recovery and	Incident Management	13.02 Diagnose an enterprise's

Florida State College at	Certifica	Program Computer	CET2662	200	59	Knowledge of Intrusion Detection	Computer Network Defense	05.12 Monitor the network
Florida State College at	Certifica	Program Computer	CET2662	200	60	Knowledge of incident categories, incident	Incident Management	17.06 Identify the major categories
Florida State College at	Certifica	Program Computer	CET2662	200	63	Knowledge of Information	Information Assurance	06.03 Utilize various forms of
Florida State College at	Certifica	Program Computer	CET2662	200	66	Knowledge of intrusion detection	Computer Network Defense	05.11 Demonstrate an
Florida State College at	Certifica	Program Computer	CET2662	200	92	Knowledge of how traffic flows across	Infrastructure Design	07.01 Utilize protocol layering
Florida State College at	Certifica	Program Computer	CET2662	200	137	Knowledge of the characteristics of	Data Management	15.09 Compare different forms of
Florida State College at	Certifica	Program Computer	CET2662	200	139	Knowledge of common networking	Infrastructure Design	07.07 Discuss the security
Florida State College at	Certifica	Program Computer	CET2662	200	175	Skill in developing and deploying signatures	Information Systems/Network	06.04 Discuss the creation and use
Florida State College at	Certifica	Program Computer	CET2662	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	13.03 Specify possible
Florida State College at	Certifica	Program Computer	CET2662	200	179	Skill in designing security controls	Information Assurance	10.06 Discuss the steps necessary
Florida State College at	Certifica	Program Computer	CET2662	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	05.11 Demonstrate an
Florida State College at	Certifica	Program Computer	CET2662	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	14.13 Perform penetration
Florida State College at	Certifica	Program Computer	CET2662	200	226	Skill in the use of social engineering	Human Factors	14.13 Perform penetration
Florida State College at	Certifica	Program Computer	CET2662	200	261	Knowledge of basic concepts,	Telecommunicatio ns	07.02 Evaluate the security
Florida State College at	Certifica	Program Computer	CET2662	200	284	Knowledge of encryption algorithms	Cryptography	06.08 Utilize application and
Florida State College at	Certifica	Program Computer	CET2662	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	05.13 Investigate audit trails for
Florida State College at	Certifica	Program Computer	CET2662	200	895	Skill in recognizing and categorizing	Information Assurance	05.10 Analyze methods of
Florida State College at	Certifica	Program Computer	CET2662	200	896	Skill in protecting a network against	Computer Network Defense	15.06 Analyze local environment
Florida State College at	Certifica	Program Computer	CET2662	200	915	Knowledge of frontend collection	Information Systems/Network	05.11 Demonstrate an
Florida State College at	Certifica	Program Computer	CET2662	200	917	Knowledge of social dynamics of computer	External Awareness	13.01 Identify the physical threats
Florida State College at	Certifica	Program Computer	CET2662	200	965	Knowledge of organization's risk	Risk Management	14.14 Understand principles of risk
Florida State College at	Certifica	Program Computer	CET2662	200	985	Skill in configuring and utilizing network	Configuration Management	13.05 Evaluate the applicability
Florida State College at	Certifica	Program Computer	CET2662	200	1021	Knowledge of threat assessment	Risk Management	13.01 Identify the physical threats
Florida State College at	Certifica	Program Computer	CET2662	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	17.01 Understand the major
Florida State College at	Certifica	Program Computer	CET2662	200	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	05.14 Perform penetration
Florida State College at	Certifica	Program Computer	CET2662	200	1072	Knowledge of network security	Information Systems/Network	07.03 Describe security concerns
Florida State College at	Certifica	Program Computer	CET2662	200	1114	Knowledge of encryption	Cryptography	06.01 Demonstrate an
Florida State College at	N/A	N/A	CET2687	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	06.05 Employ cryptographic
Florida State College at	N/A	N/A	CET2687	200	35	Knowledge of digital rights management	Encryption	18.09 Identify and discuss
Florida State College at	N/A	N/A	CET2687	200	37	Knowledge of disaster recovery and	Incident Management	13.02 Diagnose an enterprise’s

Florida State College at	N/A	N/A	CET2687	200	59	Knowledge of Intrusion Detection	Computer Network Defense	05.12 Monitor the network
Florida State College at	N/A	N/A	CET2687	200	60	Knowledge of incident categories, incident	Incident Management	17.06 Identify the major categories
Florida State College at	N/A	N/A	CET2687	200	63	Knowledge of Information	Information Assurance	06.03 Utilize various forms of
Florida State College at	N/A	N/A	CET2687	200	66	Knowledge of intrusion detection	Computer Network Defense	05.11 Demonstrate an
Florida State College at	N/A	N/A	CET2687	200	92	Knowledge of how traffic flows across	Infrastructure Design	07.01 Utilize protocol layering
Florida State College at	N/A	N/A	CET2687	200	137	Knowledge of the characteristics of	Data Management	15.09 Compare different forms of
Florida State College at	N/A	N/A	CET2687	200	139	Knowledge of common networking	Infrastructure Design	07.07 Discuss the security
Florida State College at	N/A	N/A	CET2687	200	175	Skill in developing and deploying signatures	Information Systems/Network	06.04 Discuss the creation and use
Florida State College at	N/A	N/A	CET2687	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	13.03 Specify possible
Florida State College at	N/A	N/A	CET2687	200	179	Skill in designing security controls	Information Assurance	10.06 Discuss the steps necessary
Florida State College at	N/A	N/A	CET2687	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	05.11 Demonstrate an
Florida State College at	N/A	N/A	CET2687	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	14.13 Perform penetration
Florida State College at	N/A	N/A	CET2687	200	226	Skill in the use of social engineering	Human Factors	14.13 Perform penetration
Florida State College at	N/A	N/A	CET2687	200	261	Knowledge of basic concepts,	Telecommunications	07.02 Evaluate the security
Florida State College at	N/A	N/A	CET2687	200	284	Knowledge of encryption algorithms	Cryptography	06.08 Utilize application and
Florida State College at	N/A	N/A	CET2687	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	05.13 Investigate audit trails for
Florida State College at	N/A	N/A	CET2687	200	895	Skill in recognizing and categorizing	Information Assurance	05.10 Analyze methods of
Florida State College at	N/A	N/A	CET2687	200	896	Skill in protecting a network against	Computer Network Defense	15.06 Analyze local environment
Florida State College at	N/A	N/A	CET2687	200	915	Knowledge of frontend collection	Information Systems/Network	05.11 Demonstrate an
Florida State College at	N/A	N/A	CET2687	200	917	Knowledge of social dynamics of computer	External Awareness	13.01 Identify the physical threats
Florida State College at	N/A	N/A	CET2687	200	965	Knowledge of organization's risk	Risk Management	14.14 Understand principles of risk
Florida State College at	N/A	N/A	CET2687	200	985	Skill in configuring and utilizing network	Configuration Management	13.05 Evaluate the applicability
Florida State College at	N/A	N/A	CET2687	200	1021	Knowledge of threat assessment	Risk Management	13.01 Identify the physical threats
Florida State College at	N/A	N/A	CET2687	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	17.01 Understand the major
Florida State College at	N/A	N/A	CET2687	200	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	05.14 Perform penetration
Florida State College at	N/A	N/A	CET2687	200	1072	Knowledge of network security	Information Systems/Network	07.03 Describe security concerns
Florida State College at	N/A	N/A	CET2687	200	1114	Knowledge of encryption	Cryptography	06.01 Demonstrate an
Florida State College at	N/A	N/A	CET2752	200	4	Ability to identify systemic security	Vulnerabilities Assessment	14.07 Determine what resources,
Florida State College at	N/A	N/A	CET2752	200	29	Knowledge of data backup, types of	Computer Forensics	14.03 Perform backups of critical
Florida State College at	N/A	N/A	CET2752	200	81	Knowledge of network	Infrastructure Design	02.04 Describe the functions and

Florida State College at	N/A	N/A	CET2752	200	83	Knowledge of network hardware	Hardware	02.05 Describe the major
Florida State College at	N/A	N/A	CET2752	200	87	Knowledge of network traffic	Information Systems/Network	14.11 Utilize monitoring tools
Florida State College at	N/A	N/A	CET2752	200	98	Knowledge of policybased and risk	Identity Management	14.06 Demonstrate an
Florida State College at	N/A	N/A	CET2752	200	137	Knowledge of the characteristics of	Data Management	02.08 Describe the function of
Florida State College at	N/A	N/A	CET2752	200	145	Knowledge of the type and frequency of	Systems Life Cycle	01.05 Perform preventive
Florida State College at	N/A	N/A	CET2752	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	13.03 Specify possible
Florida State College at	N/A	N/A	CET2752	200	179	Skill in designing security controls	Information Assurance	14.04 Protect the privacy of
Florida State College at	N/A	N/A	CET2752	200	191	Skill in developing and applying security	Identity Management	05.01 Specify by access control
Florida State College at	N/A	N/A	CET2752	200	221	Skill in testing and configuring network	Network Management	01.06 Set up and configure
Florida State College at	N/A	N/A	CET2752	200	231	Skill in using network management tools to	Network Management	14.11 Utilize monitoring tools
Florida State College at	N/A	N/A	CET2752	200	264	Knowledge of basic physical computer	Computers and Electronics	01.02 Identify the architecture of
Florida State College at	N/A	N/A	CET2752	200	341	Knowledge of UNIX and Windows systems	Operating Systems	03.09 Install and configure client
Florida State College at	N/A	N/A	CET2752	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	05.13 Investigate audit trails for
Florida State College at	N/A	N/A	CET2752	200	364	Skill in identifying, modifying, and	Operating Systems	05.03 Administer computer, group,
Florida State College at	N/A	N/A	CET2752	200	892	Skill in configuring and utilizing	Configuration Management	03.07 Install and configure a
Florida State College at	N/A	N/A	CET2752	200	917	Knowledge of social dynamics of computer	External Awareness	13.01 Identify the physical threats
Florida State College at	N/A	N/A	CET2752	200	952	Knowledge of emerging security	Technology Awareness	01.04 Discuss the potential impact
Florida State College at	N/A	N/A	CET2752	200	986	Knowledge of organizational	Identity Management	05.01 Specify by access control
Florida State College at	N/A	N/A	CET2752	200	1021	Knowledge of threat assessment	Risk Management	13.01 Identify the physical threats
Florida State College at	N/A	N/A	CET2752	200	1033	Knowledge of basic system	Information Systems/Network	05.02 Compare and contrast
Florida State College at	N/A	N/A	CET2752	200	1072	Knowledge of network security	Information Systems/Network	02.01 Discuss fundamental
Florida State College at	N/A	N/A	CET2759	200	15	Knowledge of capabilities and	Hardware	10.05 Identify and define
Florida State College at	N/A	N/A	CET2759	200	22	Knowledge of computer networking	Infrastructure Design	8.01 Identify and define computer
Florida State College at	N/A	N/A	CET2759	200	42	Knowledge of electrical engineering	Hardware Engineering	10.06 Apply digital
Florida State College at	N/A	N/A	CET2759	200	43	Knowledge of embedded systems	Embedded Computers	03.02 Identify, define and
Florida State College at	N/A	N/A	CET2759	200	50	Knowledge of how network services and	Infrastructure Design	10.09 Define communication
Florida State College at	N/A	N/A	CET2759	200	76	Knowledge of measures or	Information Technology	03.04 Identify and define
Florida State College at	N/A	N/A	CET2759	200	81	Knowledge of network	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2759	200	92	Knowledge of how traffic flows across	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2759	200	96	Knowledge of performance tuning	Information Technology	03.04 Identify and define

Florida State College at	N/A	N/A	CET2759	200	139	Knowledge of common networking	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2759	200	154	Skill in analyzing network traffic	Capacity Management	03.04 Identify and define
Florida State College at	N/A	N/A	CET2759	200	212	Skill in network mapping and	Infrastructure Design	8.01 Identify and define computer
Florida State College at	N/A	N/A	CET2759	200	264	Knowledge of basic physical computer	Computers and Electronics	03.01 Identify and define serial
Florida State College at	N/A	N/A	CET2759	200	322	Knowledge of router and routing	Infrastructure Design	03.05 Identify and define
Florida State College at	N/A	N/A	CET2759	200	364	Skill in identifying, modifying, and	Operating Systems	03.07 Identify and define
Florida State College at	N/A	N/A	CET2759	200	901	Knowledge of the capabilities of	Network Management	03.05 Identify and define
Florida State College at	N/A	N/A	CET2759	200	1002	Skill in conducting audits or reviews of	Information Technology	03.04 Identify and define
Florida State College at	N/A	N/A	CET2759	200	1038	Knowledge of local specialized system	Infrastructure Design	03.04 Identify and define
Florida State College at	N/A	N/A	CET2759	200	1073	Knowledge of network systems	Network Management	03.04 Identify and define
New Jersey City University	B.S	National Security Studies	SECU 422	400	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	Cryptosecurity and Key
New Jersey City University	B.S	National Security Studies	SECU 422	400	27	Knowledge of cryptology	Cryptography	Cryptosecurity and Key
New Jersey City University	B.S	National Security Studies	SECU 422	400	37	Knowledge of disaster recovery and	Incident Management	Contingency Planning/Disaster
New Jersey City University	B.S	National Security Studies	SECU 422	400	55	Knowledge of Information	Information Assurance	Risk Management Physical Security
New Jersey City University	B.S	National Security Studies	SECU 422	400	56	Knowledge of information assurance	Information Assurance	Software Security
New Jersey City University	B.S	National Security Studies	SECU 422	400	69	Knowledge of Risk Management	Information Systems Security	Risk Management
New Jersey City University	B.S	National Security Studies	SECU 422	400	77	Knowledege of current industry	Information Systems/Network	Auditing and Monitoring
New Jersey City University	B.S	National Security Studies	SECU 422	400	98	Knowledge of policybased and risk	Identity Management	Security Planning
New Jersey City University	B.S	National Security Studies	SECU 422	400	108	Knowledge of risk management	Risk Management	Risk Management
New Jersey City University	B.S	National Security Studies	SECU 422	400	111	Knowledge of security system design tools,	Information Systems/Network	Systems Lifecycle Management
New Jersey City University	B.S	National Security Studies	SECU 422	400	129	Knowledge of systems lifecycle management	Systems Life Cycle	Systems Lifecycle Management
New Jersey City University	B.S	National Security Studies	SECU 422	400	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	Systems Lifecycle Management
New Jersey City University	B.S	National Security Studies	SECU 422	400	132	Knowledge of technoloy integration	Systems Integration	Systems Lifecycle Management
New Jersey City University	B.S	National Security Studies	SECU 422	400	141	Knowledge of the enterprise	Information Technology	Systems Lifecycle Management
New Jersey City University	B.S	National Security Studies	SECU 422	400	144	Knowledge of the systems engineering	Systems Life Cycle	Systems Lifecycle Management
New Jersey City University	B.S	National Security Studies	SECU 422	400	145	Knowledge of the type and frequency of	Systems Life Cycle	Systems Lifecycle Management
New Jersey City University	B.S	National Security Studies	SECU 422	400	173	Skill in creating policies that relfect	Information Systems Security	Security Planning
New Jersey City University	B.S	National Security Studies	SECU 422	400	179	Skill in designing security controls	Information Assurance	Physical Security Measures
New Jersey City University	B.S	National Security Studies	SECU 422	400	183	Skill in determining how a security system	Information Assurance	Security Planning Systems Lifecycle
New Jersey City University	B.S	National Security Studies	SECU 422	400	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	Physical Security Measures

New Jersey City University	B.S	National Security Studies	SECU 422	400	204	Skill in identifying possible causes of	Systems Life Cycle	Systems Lifecycle Management
New Jersey City University	B.S	National Security Studies	SECU 422	400	326	Knowledge of security hardware and	Information Systems/Network	Physical Security Measures
New Jersey City University	B.S	National Security Studies	SECU 422	400	327	Knowledge of security implications of	Information Assurance	Software Security
New Jersey City University	B.S	National Security Studies	SECU 422	400	893	Skill in securing network	Information Assurance	Network Security
New Jersey City University	B.S	National Security Studies	SECU 422	400	965	Knowledge of organization's risk	Risk Management	Risk Management
New Jersey City University	B.S	National Security Studies	SECU 422	400	968	Knowledge of softwarerelated	Information Systems/Network	Software Security
New Jersey City University	B.S	National Security Studies	SECU 422	400	979	Knowledge of supply chain risk	Risk Management	Risk Management
New Jersey City University	B.S	National Security Studies	SECU 422	400	1021	Knowledge of threat assessment	Risk Management	Risk Management
New Jersey City University	B.S	National Security Studies	SECU 422	400	1061	Knowledge of the lifecycle process	Systems Life Cycle	Systems Lifecycle Management
New Jersey City University	B.S	National Security Studies	SECU 222	200	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Threats and Vulnerabilities
New Jersey City University	B.S	National Security Studies	SECU 222	200	4	Ability to identify systemic security	Vulnerabilities Assessment	Threats and Vulnerabilities
New Jersey City University	B.S	National Security Studies	SECU 222	200	5	Ability to match the appropriate	Knowledge Management	Threats and Vulnerabilities
New Jersey City University	B.S	National Security Studies	SECU 222	200	10	Knowledge of application	Vulnerabilities Assessment	Threats and Vulnerabilities
New Jersey City University	B.S	National Security Studies	SECU 222	200	63	Knowledge of Information	Information Assurance	Availability; Confidentiality;
New Jersey City University	B.S	National Security Studies	SECU 222	200	90	Knowledge of operating systems	Operating Systems	System Operating Environment
New Jersey City University	B.S	National Security Studies	SECU 222	200	124	Knowledge of system design tools,	Logical Systems Design	History; Current Methodology
New Jersey City University	B.S	National Security Studies	SECU 222	200	156	Skill in applying confidentiality,	Information Assurance	Availability; Confidentiality;
New Jersey City University	B.S	National Security Studies	SECU 222	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	INFOSEC Material Information
New Jersey City University	B.S	National Security Studies	SECU 222	200	281	Knowledge of electronic devices	Hardware	Automated Information
New Jersey City University	B.S	National Security Studies	SECU 222	200	329	Knowledge of surveillance detection	Surveillance	INFOSEC Material Information
New Jersey City University	B.S	National Security Studies	SECU 222	200	337	Knowledge of the nexus between Cyber	External Awareness	INFOSEC Material Information
New Jersey City University	B.S	National Security Studies	SECU 222	200	1074	Knowledge of transmission records	Telecommunications	Communications II
Oklahoma City Community	A.S	Information Technology	CS116	100	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Identify security issues when they
Oklahoma City Community	A.S	Information Technology	CS116	100	4	Ability to identify systemic security	Vulnerabilities Assessment	Identify security issues when they
Oklahoma City Community	A.S	Information Technology	CS116	100	49	Knowledge of host/network access	Information Systems/Network	Define and identify Access
Oklahoma City Community	A.S	Information Technology	CS116	100	157	Skill in applying host/network access	Identity Management	Define and identify Access
Oklahoma City Community	A.S	Information Technology	CS116	100	191	Skill in developing and applying security	Identity Management	Define and identify Access
Oklahoma City Community	A.S	Information Technology	CS116	100	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	Discuss and analyze how
Oklahoma City Community	A.S	Information Technology	CS116	100	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	Provide ideas on establishing
Oklahoma City Community	A.S	Information Technology	CS116	100	985	Skill in configuring and utilizing network	Configuration Management	Discuss and analyze how

Oklahoma City Community	A.S	Information Technology	CS116	100	986	Knowledge of organizational	Identity Management	Define and identify Access
Oklahoma City Community	A.S	Information Technology	CS116	100	1036	Knowledge of applicable laws (e.g.,	Criminal Law	Name and discuss the cryptographic
Oklahoma City Community	A.S	Information Technology	CS2713	200	69	Knowledge of Risk Management	Information Systems Security	Define risk management, risk
Oklahoma City Community	A.S	Information Technology	CS2713	200	108	Knowledge of risk management	Risk Management	Define risk management, risk
Oklahoma City Community	A.S	Information Technology	CS2713	200	110	Knowledge of security management	Information Assurance	List the recommended
Oklahoma City Community	A.S	Information Technology	CS2743	200	37	Knowledge of disaster recovery and	Incident Management	List the elements of a sample
Oklahoma City Community	A.S	Information Technology	CS2743	200	59	Knowledge of Intrusion Detection	Computer Network Defense	Explain the components of
Oklahoma City Community	A.S	Information Technology	CS2743	200	60	Knowledge of incident categories, incident	Incident Management	Explain the components of
Oklahoma City Community	A.S	Information Technology	CS2743	200	64	Knowledge of information security	Information Systems/ Network	· Define and explain
Oklahoma City Community	A.S	Information Technology	CS2743	200	69	Knowledge of Risk Management	Information Systems Security	· Identify and explain the basic
Oklahoma City Community	A.S	Information Technology	CS2743	200	146	Knowledge of the types of Intrusion	Computer Network Defense	Explain the components of
Oklahoma City Community	A.S	Information Technology	CS2743	200	193	Skill in developing, testing, and	Information Assurance	· List and discuss the
Oklahoma City Community	A.S	Information Technology	CS2743	200	980	Skill in performing root cause analysis for	Incident Management	· Discuss the elements
Oklahoma City Community	A.S	Information Technology	CS2743	200	985	Skill in configuring and utilizing network	Configuration Management	Explain the components of
Oklahoma City Community	A.S	Information Technology	CS2783	200	29	Knowledge of data backup, types of	Computer Forensics	· Explain how to locate and
Oklahoma City Community	A.S	Information Technology	CS2783	200	217	Skill in preserving evidence integrity	Computer Forensics	Describe procedures for
Oklahoma City Community	A.S	Information Technology	CS2783	200	287	Knowledge of file system	Operating Systems	· Explain the purpose and
Oklahoma City Community	A.S	Information Technology	CS2783	200	290	Knowledge of processes for seizing	Forensics	· Explain guidelines for
Oklahoma City Community	A.S	Information Technology	CS2783	200	316	Knowledge of processes for	Criminal Law	· Explain guidelines for
Oklahoma City Community	A.S	Information Technology	CS2783	200	344	Knowledge of virtualization	Operating Systems	· Explain the purpose of a
Oklahoma City Community	A.S	Information Technology	CS2783	200	369	Skill in collecting, processing,	Forensics	· Describe how to collect
Oklahoma City Community	A.S	Information Technology	CS2783	200	374	Skill in setting up a forensic workstation	Forensics	· Explain how to prepare a
Oklahoma City Community	A.S	Information Technology	CS2783	200	890	Skill in conducting forensic analyses in	Computer Forensics	· Explain how to locate and
Oklahoma City Community	A.S	Information Technology	CS2783	200	1091	Skill in one way hash functions (e.g., Secure	Data Management	· Explain how to obtain a digital
Oklahoma City Community	A.S	Information Technology	CS2723	200	9	Knowledge of applicable business	Requirements Analysis	Why companies concentrate on
Oklahoma City Community	A.S	Information Technology	CS2723	200	50	Knowledge of how network services and	Infrastructure Design	How Internet, email, and Web
Oklahoma City Community	A.S	Information Technology	CS2723	200	81	Knowledge of network	Infrastructure Design	About Internet addressing and
Oklahoma City Community	A.S	Information Technology	CS2723	200	92	Knowledge of how traffic flows across	Infrastructure Design	How packetswitched
Oklahoma City Community	A.S	Information Technology	CS2723	200	139	Knowledge of common networking	Infrastructure Design	How Internet, email, and Web
Oklahoma City Community	A.S	Information Technology	CS2723	200	900	Knowledge of web filtering technologies	Web Technology	How to identify and manage

Oklahoma City Community	A.S	Information Technology	CS2723	200	901	Knowledge of the capabilities of	Network Management	What electronic commerce is and
Oklahoma City Community	A.S	Information Technology	CS2723	200	942	Knowledge of the organization's core	Organizational Awareness	Why companies concentrate on
Oklahoma City Community	A.S	Information Technology	CS2723	200	1064	Knowledge of Extensible Markup	Infrastructure Design	About the history and use of
Frances Tuttle	N/A	Information Technology	CS2743	200	49	Knowledge of host/network access	Information Systems/Network	Explain why access control is
Frances Tuttle	N/A	Information Technology	CS2743	200	59	Knowledge of Intrusion Detection	Computer Network Defense	Identify and describe the
Frances Tuttle	N/A	Information Technology	CS2743	200	69	Knowledge of Risk Management	Information Systems Security	Define risk management and
Frances Tuttle	N/A	Information Technology	CS2743	200	70	Knowledge of information	Information Systems/Network	Identify the various types of
Frances Tuttle	N/A	Information Technology	CS2743	200	98	Knowledge of policybased and risk	Identity Management	Define information
Frances Tuttle	N/A	Information Technology	CS2743	200	108	Knowledge of risk management	Risk Management	Define risk management and
Frances Tuttle	N/A	Information Technology	CS2743	200	146	Knowledge of the types of Intrusion	Computer Network Defense	Identify and describe the
Frances Tuttle	N/A	Information Technology	CS2743	200	157	Skill in applying host/network access	Identity Management	Describe the various access
Frances Tuttle	N/A	Information Technology	CS2743	200	173	Skill in creating policies that relfect	Information Systems Security	Develop, implement, and
Frances Tuttle	N/A	Information Technology	CS2743	200	191	Skill in developing and applying security	Identity Management	Explain why access control is
Frances Tuttle	N/A	Information Technology	CS2743	200	193	Skill in developing, testing, and	Information Assurance	Explain the principal
Frances Tuttle	N/A	Information Technology	CS2743	200	891	Skill in configuring and utilizing	Configuration Management	Identify the various types of
Frances Tuttle	N/A	Information Technology	CS2743	200	965	Knowledge of organization's risk	Risk Management	Define risk management and
Frances Tuttle	N/A	Information Technology	CS2743	200	985	Skill in configuring and utilizing network	Configuration Management	Identify the various types of
Frances Tuttle	N/A	Information Technology	CS2743	200	986	Knowledge of organizational	Identity Management	Define information
Frances Tuttle	N/A	Information Technology	CS2743	200	1114	Knowledge of encryption	Cryptography	Explain cryptography and
Frances Tuttle	N/A	Information Technology	CS2783	200	287	Knowledge of file system	Operating Systems	• Explain the structure of New
Frances Tuttle	N/A	Information Technology	CS2783	200	290	Knowledge of processes for seizing	Forensics	• List digital evidence storage
Frances Tuttle	N/A	Information Technology	CS2783	200	305	Knowledge of laws that affect cyber	Forensics	· Explain the rules for digital
Frances Tuttle	N/A	Information Technology	CS2783	200	316	Knowledge of processes for	Criminal Law	• List digital evidence storage
Frances Tuttle	N/A	Information Technology	CS2783	200	369	Skill in collecting, processing,	Forensics	· Explain guidelines for
Frances Tuttle	N/A	Information Technology	CS2783	200	890	Skill in conducting forensic analyses in	Computer Forensics	· Explain the basic concepts of
Frances Tuttle	N/A	Information Technology	CS2783	200	908	Ability to decrypt digital data collections	Computer Forensics	· List some options for
Frances Tuttle	N/A	Information Technology	CS2783	200	968	Knowledge of softwarerelated	Information Systems/Network	Explain common datahiding
Frances Tuttle	N/A	Information Technology	CS2783	200	1063	Knowledge of Unix/Linux operating	Operating Systems	· Explain UNIX and Linux disk
Frances Tuttle	N/A	Information Technology	ECS 2224	200	50	Knowledge of how network services and	Infrastructure Design	· Describe the purpose and
Frances Tuttle	N/A	Information Technology	ECS 2224	200	81	Knowledge of network	Infrastructure Design	· Describe the purpose and

Frances Tuttle	N/A	Information Technology	ECS 2224	200	90	Knowledge of operating systems	Operating Systems	· Understand the purpose of an
Frances Tuttle	N/A	Information Technology	ECS 2224	200	113	Knowledge of server and client operating	Operating Systems	· Understand the purpose of an
Frances Tuttle	N/A	Information Technology	ECS 2224	200	139	Knowledge of common networking	Infrastructure Design	· Describe the purpose and
Frances Tuttle	N/A	Information Technology	ECS 2224	200	219	Skill in system administration for	Operating Systems	· Outline the key features of
Frances Tuttle	N/A	Information Technology	ECS 2224	200	281	Knowledge of electronic devices	Hardware	Configure a modem, ISDN,
Frances Tuttle	N/A	Information Technology	ECS 2224	200	341	Knowledge of UNIX and Windows systems	Operating Systems	· Configure infrastructure
Frances Tuttle	N/A	Information Technology	ECS 2224	200	364	Skill in identifying, modifying, and	Operating Systems	· Understand and navigate the
Frances Tuttle	N/A	Information Technology	ECS 2224	200	1059	Knowledge of networking protocols	Infrastructure Design	· Describe the purpose and
Frances Tuttle	N/A	Information Technology	ECS 2224	200	1063	Knowledge of Unix/Linux operating	Operating Systems	· Outline the key features of
Frances Tuttle	N/A	Information Technology	ECS1214	100	23	Knowledge of computer	Object Technology	Explain the principles of
Frances Tuttle	N/A	Information Technology	ECS1214	100	90	Knowledge of operating systems	Operating Systems	Explain the purpose of an
Frances Tuttle	N/A	Information Technology	ECS1214	100	92	Knowledge of how traffic flows across	Infrastructure Design	Explain OSI and TCP/IP data
Frances Tuttle	N/A	Information Technology	ECS1214	100	113	Knowledge of server and client operating	Operating Systems	Describe desktop and network
Frances Tuttle	N/A	Information Technology	ECS1214	100	123	Knowledge of system and application	Vulnerabilities Assessment	Describe security threats
Frances Tuttle	N/A	Information Technology	ECS1214	100	139	Knowledge of common networking	Infrastructure Design	Describe basic networking
Frances Tuttle	N/A	Information Technology	ECS1214	100	205	Skill in implementing, maintaining, and	Information Systems/Network	Identify common preventive
Frances Tuttle	N/A	Information Technology	ECS1214	100	212	Skill in network mapping and	Infrastructure Design	Describe network topologies
Frances Tuttle	N/A	Information Technology	ECS1214	100	226	Skill in the use of social engineering	Human Factors	Explain social engineering, data
Frances Tuttle	N/A	Information Technology	ECS1214	100	264	Knowledge of basic physical computer	Computers and Electronics	Describe the physical
Frances Tuttle	N/A	Information Technology	ECS1214	100	356	Skill in determining installed patches on	Operating Systems	Describe characteristics of
Frances Tuttle	N/A	Information Technology	ECS1214	100	1033	Knowledge of basic system	Information Systems/Network	Describe desktop and network
Frances Tuttle	N/A	Information Technology	ECS1214	100	1059	Knowledge of networking protocols	Infrastructure Design	Describe basic networking
Frances Tuttle	N/A	Information Technology	ECS1214	100	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Identify common preventive
Frances Tuttle	N/A	Information Technology	ECS1214	100	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Identify common preventive
Frances Tuttle	N/A	Information Technology	ECS2514	200	8	Knowledge of access authentication	Identity Management	Explain the function and
Frances Tuttle	N/A	Information Technology	ECS2514	200	12	Knowledge of communication	Infrastructure Design	Explain how cryptology
Frances Tuttle	N/A	Information Technology	ECS2514	200	27	Knowledge of cryptology	Cryptography	Explain how cryptology
Frances Tuttle	N/A	Information Technology	ECS2514	200	59	Knowledge of Intrusion Detection	Computer Network Defense	Configure IPS to mitigate attacks
Frances Tuttle	N/A	Information Technology	ECS2514	200	63	Knowledge of Information	Information Assurance	Explain the function and
Frances Tuttle	N/A	Information Technology	ECS2514	200	82	Knowledge of network design	Infrastructure Design	Describe the principles of

Frances Tuttle	N/A	Information Technology	ECS2514	200	108	Knowledge of risk management	Risk Management	Describe threat identification and
Frances Tuttle	N/A	Information Technology	ECS2514	200	173	Skill in creating policies that relfect	Information Systems Security	Given the security needs of
Frances Tuttle	N/A	Information Technology	ECS2514	200	237	Skill in using Virtual Private Network	Encryption	Describe the purpose and
Frances Tuttle	N/A	Information Technology	ECS2514	200	891	Skill in configuring and utilizing	Configuration Management	Implement firewall
Frances Tuttle	N/A	Information Technology	ECS2514	200	892	Skill in configuring and utilizing	Configuration Management	Implement firewall
Frances Tuttle	N/A	Information Technology	ECS2514	200	901	Knowledge of the capabilities of	Network Management	Describe wireless, VoIP, and SAN
Frances Tuttle	N/A	Information Technology	ECS2514	200	985	Skill in configuring and utilizing network	Configuration Management	Implement firewall
Frances Tuttle	N/A	Information Technology	ECS2514	200	989	Knowledge of Voice over Internet Protocol	Telecommunicatio ns	Describe wireless, VoIP, and SAN
Frances Tuttle	N/A	Information Technology	ECS2514	200	1021	Knowledge of threat assessment	Risk Management	Describe threat identification and
Frances Tuttle	N/A	Information Technology	ECS2514	200	1114	Knowledge of encryption	Cryptography	Explain how cryptology
Frances Tuttle	N/A	Information Technology	CS2713	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	Explain components of
Frances Tuttle	N/A	Information Technology	CS2713	200	33	Knowledge of database procedures	Incident Management	Define incidenthandling
Frances Tuttle	N/A	Information Technology	CS2713	200	60	Knowledge of incident categories, incident	Incident Management	Define incidenthandling
Frances Tuttle	N/A	Information Technology	CS2713	200	61	Knowledge of incident response and	Incident Management	Define incidenthandling
Frances Tuttle	N/A	Information Technology	CS2713	200	87	Knowledge of network traffic	Information Systems/Network	Describe how signature analysis
Frances Tuttle	N/A	Information Technology	CS2713	200	108	Knowledge of risk management	Risk Management	Explain the fundamental
Frances Tuttle	N/A	Information Technology	CS2713	200	229	Skill in using incident handling	Incident Management	Define incidenthandling
Frances Tuttle	N/A	Information Technology	CS2713	200	231	Skill in using network management tools to	Network Management	Describe how signature analysis
Frances Tuttle	N/A	Information Technology	CS2713	200	917	Knowledge of social dynamics of computer	External Awareness	Describe common network
Frances Tuttle	N/A	Information Technology	CS2713	200	986	Knowledge of organizational	Identity Management	Identify security policy categories
Frances Tuttle	N/A	Information Technology	CS2713	200	990	Knowledge of common attack	Computer Network Defense	Describe common network
Frances Tuttle	N/A	Information Technology	CS2713	200	991	Knowledge of different classes of	Computer Network Defense	Describe common network
Frances Tuttle	N/A	Information Technology	CS2713	200	1011	Knowledge of processes for	Security	Define incidenthandling
Frances Tuttle	N/A	Information Technology	CS2713	200	1021	Knowledge of threat assessment	Risk Management	Explain the fundamental
Frances Tuttle	N/A	Information Technology	CS2713	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Describe common network
Frances Tuttle	N/A	Information Technology	CS2713	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Describe common network
University of the District of	B.S	Computer Science	CSCI315	300	90	Knowledge of operating systems	Operating Systems	1) Understand UNIX (or
University of the District of	B.S	Computer Science	CSCI315	300	113	Knowledge of server and client operating	Operating Systems	1) Understand UNIX (or
University of the District of	B.S	Computer Science	CSCI315	300	122	Knowledge of system administration	Operating Systems	Understand UNIX system
University of the District of	B.S	Computer Science	CSCI315	300	127	Knowledge of systems administration	Operating Systems	Understand UNIX system

University of the District of	B.S	Computer Science	CSCI315	300	219	Skill in system administration for	Operating Systems	Understand UNIX system
University of the District of	B.S	Computer Science	CSCI315	300	286	Knowledge of file extensions (e.g., .dll,	Operating Systems	Understand UNIX system
University of the District of	B.S	Computer Science	CSCI315	300	287	Knowledge of file system	Operating Systems	1) Understand UNIX (or
University of the District of	B.S	Computer Science	CSCI315	300	341	Knowledge of UNIX and Windows systems	Operating Systems	Understand UNIX system
University of the District of	B.S	Computer Science	CSCI315	300	342	Knowledge of Unix command line (e.g.,	Computer Languages	3) Know how to use UNIX
University of the District of	B.S	Computer Science	CSCI315	300	356	Skill in determining installed patches on	Operating Systems	Understand UNIX system
University of the District of	B.S	Computer Science	CSCI315	300	364	Skill in identifying, modifying, and	Operating Systems	3) Know how to use UNIX
University of the District of	B.S	Computer Science	CSCI315	300	371	Skill in reading, interpreting, writing,	Operating Systems	3) Know how to use UNIX
University of the District of	B.S	Computer Science	CSCI315	300	1033	Knowledge of basic system	Information Systems/Network	2) Understand UNIX system
University of the District of	B.S	Computer Science	CSCI315	300	1063	Knowledge of Unix/Linux operating	Operating Systems	1) Understand UNIX (or
University of the District of	B.S	Computer Science	CSCI315	300	1121	Knowledge of Windows/Unix ports	Operating Systems	2) Understand UNIX system
University of the District of	B.S	Computer Science	CSCI351	300	12	Knowledge of communication	Infrastructure Design	2) Learn fundamental
University of the District of	B.S	Computer Science	CSCI351	300	15	Knowledge of capabilities and	Hardware	5) Understand the various
University of the District of	B.S	Computer Science	CSCI351	300	22	Knowledge of computer networking	Infrastructure Design	2) Learn fundamental
University of the District of	B.S	Computer Science	CSCI351	300	41	Knowledge of organization's Local	Infrastructure Design	1) Know the basic definitions and
University of the District of	B.S	Computer Science	CSCI351	300	50	Knowledge of how network services and	Infrastructure Design	4) Understand basic design and
University of the District of	B.S	Computer Science	CSCI351	300	72	Knowledge of local area network (LAN)	Infrastructure Design	5) Understand the various
University of the District of	B.S	Computer Science	CSCI351	300	81	Knowledge of network	Infrastructure Design	5) Understand the various
University of the District of	B.S	Computer Science	CSCI351	300	92	Knowledge of how traffic flows across	Infrastructure Design	4) Understand basic design and
University of the District of	B.S	Computer Science	CSCI351	300	139	Knowledge of common networking	Infrastructure Design	4) Understand basic design and
University of the District of	B.S	Computer Science	CSCI351	300	194	Skill in diagnosing connectivity problems	Network Management	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	207	Skill in installing, configuring, and		6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	212	Skill in network mapping and	Infrastructure Design	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	221	Skill in testing and configuring network	Network Management	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	231	Skill in using network management tools to	Network Management	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	261	Knowledge of basic concepts,	Telecommunications	2) Learn fundamental
University of the District of	B.S	Computer Science	CSCI351	300	271	Knowledge of common network	Infrastructure Design	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	278	Knowledge of different types of	Telecommunications	1) Know the basic definitions and
University of the District of	B.S	Computer Science	CSCI351	300	341	Knowledge of UNIX and Windows systems	Operating Systems	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	385	Skill in using traceroute analysis	Network Management	6) Have practical experience to

University of the District of	B.S	Computer Science	CSCI351	300	901	Knowledge of the capabilities of	Network Management	6) Have practical experience to
University of the District of	B.S	Computer Science	CSCI351	300	902	Knowledge of the range of existing	Network Management	5) Understand the various
University of the District of	B.S	Computer Science	CSCI351	300	903	Knowledge of Wireless Fidelity	Network Management	5) Understand the various
University of the District of	B.S	Computer Science	CSCI351	300	1059	Knowledge of networking protocols	Infrastructure Design	4) Understand basic design and
University of the District of	B.S	Computer Science	CSCI352	300	19	Knowledge of Computer Network	Computer Network Defense	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	22	Knowledge of computer networking	Infrastructure Design	1) Familiar with the fundamental
University of the District of	B.S	Computer Science	CSCI352	300	49	Knowledge of host/network access	Information Systems/Network	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	50	Knowledge of how network services and	Infrastructure Design	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	58	Knowledge of known vulnerabilities from	Information Systems/Network	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	59	Knowledge of Intrusion Detection	Computer Network Defense	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	70	Knowledge of information	Information Systems/Network	4) Know the various ways to
University of the District of	B.S	Computer Science	CSCI352	300	81	Knowledge of network	Infrastructure Design	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	82	Knowledge of network design	Infrastructure Design	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	92	Knowledge of how traffic flows across	Infrastructure Design	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	111	Knowledge of security system design tools,	Information Systems/Network	4) Know the various ways to
University of the District of	B.S	Computer Science	CSCI352	300	139	Knowledge of common networking	Infrastructure Design	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	150	Knowledge of what constitutes a network	Information Systems/Network	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	252	Knowledge of and experience in Insider	Computer Network Defense	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	274	Knowledge of concepts, principles,	Computer Network Defense	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	277	Knowledge of defense indepth principles and	Computer Network Defense	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	313	Knowledge of logging services for network	Information Systems/Network	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	326	Knowledge of security hardware and	Information Systems/Network	4) Know the various ways to
University of the District of	B.S	Computer Science	CSCI352	300	923	Knowledge of security event correlation	Information Systems/Network	4) Know the various ways to
University of the District of	B.S	Computer Science	CSCI352	300	967	Knowledge of current and emerging	Information Systems/Network	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	984	Knowledge of computer network	Computer Network Defense	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	985	Skill in configuring and utilizing network	Configuration Management	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI352	300	990	Knowledge of common attack	Computer Network Defense	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	991	Knowledge of different classes of	Computer Network Defense	2) Able to differentiate
University of the District of	B.S	Computer Science	CSCI352	300	992	Knowledge of different operational	Computer Network Defense	2) Able to differentiate

University of the District of	B.S	Computer Science	CSCI352	300	1011	Knowledge of processes for	Security	1) Familiar with the fundamental
University of the District of	B.S	Computer Science	CSCI352	300	1033	Knowledge of basic system	Information Systems/Network	4) Know the various ways to
University of the District of	B.S	Computer Science	CSCI352	300	1072	Knowledge of network security	Information Systems/Network	1) Familiar with the fundamental
University of the District of	B.S	Computer Science	CSCI352	300	1073	Knowledge of network systems	Network Management	3) Have an understanding on
University of the District of	B.S	Computer Science	CSCI353	300	8	Knowledge of access authentication	Identity Management	3) Understand identify
University of the District of	B.S	Computer Science	CSCI353	300	35	Knowledge of digital rights management	Encryption	3) Understand identify
University of the District of	B.S	Computer Science	CSCI353	300	37	Knowledge of disaster recovery and	Incident Management	7) Perform business
University of the District of	B.S	Computer Science	CSCI353	300	77	Knowledege of current industry	Information Systems/Network	2) Perform compliance
University of the District of	B.S	Computer Science	CSCI353	300	79	Knowledge of network access,	Identity Management	3) Understand identify
University of the District of	B.S	Computer Science	CSCI353	300	98	Knowledge of policybased and risk	Identity Management	3) Understand identify
University of the District of	B.S	Computer Science	CSCI353	300	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	2) Perform compliance
University of the District of	B.S	Computer Science	CSCI353	300	299	Knowledge of information security	Project Management	5) Plan for change management
University of the District of	B.S	Computer Science	CSCI353	300	986	Knowledge of organizational	Identity Management	1) Design a security policy
University of the District of	B.S	Computer Science	CSCI353	300	1002	Skill in conducting audits or reviews of	Information Technology	6) Perform logging and
University of the District of	B.S	Computer Science	CSCI353	300	1033	Knowledge of basic system	Information Systems/Network	4) Harden systems through
University of the District of	B.S	Computer Science	CSCI353	300	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	4) Harden systems through
University of the District of	B.S	Computer Science	CSCI353	300	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	4) Harden systems through
University of the District of	B.S	Computer Science	CSCI412	400	90	Knowledge of operating systems	Operating Systems	1) Understand the concepts of
University of the District of	B.S	Computer Science	CSCI412	400	113	Knowledge of server and client operating	Operating Systems	1) Understand the concepts of
University of the District of	B.S	Computer Science	CSCI412	400	122	Knowledge of system administration	Operating Systems	2) Know how to perform both
University of the District of	B.S	Computer Science	CSCI412	400	219	Skill in system administration for	Operating Systems	4) Have an ability on controlling
University of the District of	B.S	Computer Science	CSCI412	400	287	Knowledge of file system	Operating Systems	3) Understand resource
University of the District of	B.S	Computer Science	CSCI412	400	342	Knowledge of Unix command line (e.g.,	Computer Languages	2) Know how to perform both
University of the District of	B.S	Computer Science	CSCI412	400	364	Skill in identifying, modifying, and	Operating Systems	4) Have an ability on controlling
University of the District of	B.S	Computer Science	CSCI412	400	371	Skill in reading, interpreting, writing,	Operating Systems	2) Know how to perform both
University of the District of	B.S	Computer Science	CSCI412	400	1008	Knowledge of how to troubleshoot basic	Operating Systems	2) Know how to perform both
University of the District of	B.S	Computer Science	CSCI412	400	1047	Skill in writing kernel level applications	Software Development	1) Understand the concepts of
University of the District of	B.S	Computer Science	CSCI412	400	1063	Knowledge of Unix/Linux operating	Operating Systems	1) Understand the concepts of
University of the District of	B.S	Computer Science	CSCI441	400	24	Knowledge of concepts and	Data Management	1) Understand digital forensic
University of the District of	B.S	Computer Science	CSCI441	400	217	Skill in preserving evidence integrity	Computer Forensics	5) Know how to seize a computer

University of the District of	B.S	Computer Science	CSCI441	400	290	Knowledge of processes for seizing	Forensics	5) Know how to seize a computer
University of the District of	B.S	Computer Science	CSCI441	400	302	Knowledge of investigative	Computer Forensics	2) Know how to examine various
University of the District of	B.S	Computer Science	CSCI441	400	313	Knowledge of logging services for network	Information Systems/Network	2) Know how to examine various
University of the District of	B.S	Computer Science	CSCI441	400	340	Knowledge of types and collection of	Computer Forensics	4) Determine where digital
University of the District of	B.S	Computer Science	CSCI441	400	346	Knowledge of which system files (e.g. log	Computer Forensics	4) Determine where digital
University of the District of	B.S	Computer Science	CSCI441	400	360	Skill in identifying and extracting data of	Computer Forensics	4) Determine where digital
University of the District of	B.S	Computer Science	CSCI441	400	369	Skill in collecting, processing,	Forensics	5) Know how to seize a computer
University of the District of	B.S	Computer Science	CSCI441	400	379	Skill in using common digital forensics tools	Computer Forensics	1) Understand digital forensic
University of the District of	B.S	Computer Science	CSCI441	400	888	Knowledge of types of digital forensics data	Computer Forensics	4) Determine where digital
University of the District of	B.S	Computer Science	CSCI441	400	1044	Skill in identifying forensic footprints	Computer Forensics	4) Determine where digital
University of the District of	B.S	Computer Science	CSCI441	400	1093	Knowledge of common forensic tool	Computer Forensics	2) Know how to examine various
University of the District of	B.S	Computer Science	CSCI453	400	44	Knowledge of enterprise messaging	Enterprise Architecture	4) Explaining the requirements
University of the District of	B.S	Computer Science	CSCI453	400	56	Knowledge of information assurance	Information Assurance	2) Identifying current secure
University of the District of	B.S	Computer Science	CSCI453	400	116	Knowledge of software debugging	Software Development	4) Explaining the requirements
University of the District of	B.S	Computer Science	CSCI453	400	117	Knowledge of software design tools,	Software Development	4) Explaining the requirements
University of the District of	B.S	Computer Science	CSCI453	400	118	Knowledge of software	Software Engineering	3) Showing the practical
University of the District of	B.S	Computer Science	CSCI453	400	119	Knowledge of software engineering	Software Engineering	1) Understanding the importance of
University of the District of	B.S	Computer Science	CSCI453	400	126	Knowledge of system software and	Requirements Analysis	5) Understand professionalism,
University of the District of	B.S	Computer Science	CSCI453	400	129	Knowledge of systems lifecycle management	Systems Life Cycle	3) Showing the practical
University of the District of	B.S	Computer Science	CSCI453	400	327	Knowledge of security implications of	Information Assurance	2) Identifying current secure
University of the District of	B.S	Computer Science	CSCI453	400	968	Knowledge of softwarerelated	Information Systems/Network	2) Identifying current secure
University of the District of	B.S	Computer Science	CSCI453	400	976	Knowledge of software quality	Software Engineering	4) Explaining the requirements
University of the District of	B.S	Computer Science	CSCI453	400	1071	Knowledge of secure software deployment	Software Engineering	3) Showing the practical
University of the District of	B.S	Computer Science	CSCI455	400	21	Knowledge of computer algorithms	Mathematical Reasoning	1) Understand basic algorithm
University of the District of	B.S	Computer Science	CSCI455	400	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	3) Understand symmetric/asym
University of the District of	B.S	Computer Science	CSCI455	400	27	Knowledge of cryptology	Cryptography	3) Understand symmetric/asym
University of the District of	B.S	Computer Science	CSCI455	400	35	Knowledge of digital rights management	Encryption	5) Have knowledge on
University of the District of	B.S	Computer Science	CSCI455	400	284	Knowledge of encryption algorithms	Cryptography	3) Understand symmetric/asym
University of the District of	B.S	Computer Science	CSCI455	400	387	Skill in verifying the integrity of encrypted	Encryption	3) Understand symmetric/asym
University of the District of	B.S	Computer Science	CSCI455	400	1091	Skill in one way hash functions (e.g., Secure	Data Management	5) Have knowledge on

University of the District of	B.S	Computer Science	CSCI455	400	1114	Knowledge of encryption	Cryptography	3) Understand symmetric/asym
ValenciaCollege	B.S	Network Engineering	CET 2660C	200	59	Knowledge of Intrusion Detection	Computer Network Defense	Student will be able to
ValenciaCollege	B.S	Network Engineering	CET 2660C	200	146	Knowledge of the types of Intrusion	Computer Network Defense	Student will be able to
ValenciaCollege	B.S	Network Engineering	CET 2660C	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	Student will be able to
ValenciaCollege	B.S	Network Engineering	CET 2660C	200	342	Knowledge of Unix command line (e.g.,	Computer Languages	Student will be able to Employ
ValenciaCollege	B.S	Network Engineering	CET 2660C	200	985	Skill in configuring and utilizing network	Configuration Management	Student will be able to
ValenciaCollege	B.S	Network Engineering	CET 2660C	200	1067	Skill in utlilizing network analysis tools	Vulnerabilities Assessment	Student will be able to Employ
ValenciaCollege	B.S	Network Engineering	CET 2660C	200	1088	Skill in using binary analysis tools (e.g.,	Computer Languages	Student will be able to Employ
ValenciaCollege	B.S	Network Engineering	CET 2660C	200	1115	Skill in reading Hexadecimal data	Computer Languages	Student will be able to Compare
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	27	Knowledge of cryptology	Cryptography	Student will be able to Explain
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	37	Knowledge of disaster recovery and	Incident Management	Student will be able to Explain
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	49	Knowledge of host/network access	Information Systems/Network	Student will be able to Describe
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	64	Knowledge of information security	Information Systems/ Network	Student will be able to Explain
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	70	Knowledge of information	Information Systems/Network	Student will be able to Describe
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	79	Knowledge of network access,	Identity Management	Student will be able to Describe
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	Student will be able to Students
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	157	Skill in applying host/network access	Identity Management	Student will be able to Describe
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	Student will be able to Using
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	237	Skill in using Virtual Private Network	Encryption	Student will be able to Describe
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	271	Knowledge of common network	Infrastructure Design	Student will be able to perform
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	299	Knowledge of information security	Project Management	Student will be able to Describe
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	985	Skill in configuring and utilizing network	Configuration Management	Students will be able to configure
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	991	Knowledge of different classes of	Computer Network Defense	Student will be able to Describe
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	1091	Skill in one way hash functions (e.g., Secure	Data Management	Student will be able to Describe
ValenciaCollege	B.S	Network Engineering	CET 2830C	200	1114	Knowledge of encryption	Cryptography	Student will be able to Explain
ValenciaCollege	B.S	Network Engineering	CET 2881C	200	29	Knowledge of data backup, types of	Computer Forensics	Student will be able to Recover
ValenciaCollege	B.S	Network Engineering	CET 2881C	200	364	Skill in identifying, modifying, and	Operating Systems	Student will be able to Identify
ValenciaCollege	B.S	Network Engineering	CET 2881C	200	366	Skill in law enforcement report	Technical Documentation	Student will be able to Prepare a
ValenciaCollege	B.S	Network Engineering	CET 2890C	200	70	Knowledge of information	Information Systems/Network	Student will be able to Discuss
ValenciaCollege	B.S	Network Engineering	CET 2890C	200	87	Knowledge of network traffic	Information Systems/Network	Student will be able to Analyze

ValenciaCollege	B.S	Network Engineering	CET 2890C	200	214	Skill in performing packetlevel analysis	Vulnerabilities Assessment	Student will be able to
ValenciaCollege	B.S	Network Engineering	CET 2890C	200	231	Skill in using network management tools to	Network Management	Student will be able to Analyze
ValenciaCollege	B.S	Network Engineering	CET 2890C	200	891	Skill in configuring and utilizing	Configuration Management	Student will be able to Select
ValenciaCollege	B.S	Network Engineering	CET 2890C	200	892	Skill in configuring and utilizing	Configuration Management	Student will be able to Select
ValenciaCollege	B.S	Network Engineering	CET 2890C	200	900	Knowledge of web filtering technologies	Web Technology	Student will be able to Select the
ValenciaCollege	B.S	Network Engineering	CET 2890C	200	915	Knowledge of frontend collection	Information Systems/Network	Student will be able to Select the
ValenciaCollege	B.S	Network Engineering	CET 2890C	200	1033	Knowledge of basic system	Information Systems/Network	Student will be able to Harden
ValenciaCollege	B.S	Network Engineering	CET 2894C	200	60	Knowledge of incident categories, incident	Incident Management	Student will be able to Plan for
ValenciaCollege	B.S	Network Engineering	CET 2894C	200	61	Knowledge of incident response and	Incident Management	Student will be able to Plan for
ValenciaCollege	B.S	Network Engineering	CET 2894C	200	299	Knowledge of information security	Project Management	student will be able to Discuss
ValenciaCollege	B.S	Network Engineering	CET 2894C	200	966	Knowledge of enterprise incident	Incident Management	Student will be able to Plan for
ValenciaCollege	B.S	Network Engineering	CET 2894C	200	985	Skill in configuring and utilizing network	Configuration Management	Student will be able to Deploy
ValenciaCollege	B.S	Network Engineering	CET2830C	200	27	Knowledge of cryptology	Cryptography	· Explain how to use
ValenciaCollege	B.S	Network Engineering	CET2830C	200	110	Knowledge of security management	Information Assurance	Describe Security Management and
ValenciaCollege	B.S	Network Engineering	CET2830C	200	891	Skill in configuring and utilizing	Configuration Management	Secure the network
ValenciaCollege	B.S	Network Engineering	CET2830C	200	892	Skill in configuring and utilizing	Configuration Management	Secure the network
ValenciaCollege	B.S	Network Engineering	CET2830C	200	985	Skill in configuring and utilizing network	Configuration Management	Secure the network
ValenciaCollege	B.S	Network Engineering	CET2830C	200	1033	Knowledge of basic system	Information Systems/Network	Protect network by disabling
ValenciaCollege	B.S	Network Engineering	CET2830C	200	1066	Skill in utlilizing exploitation tools	Vulnerabilities Assessment	Assess the need for penetration
ValenciaCollege	B.S	Network Engineering	CET2830C	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Perform network enumeration
ValenciaCollege	B.S	Network Engineering	CET2892C	200	34	Knowledge of database systems	Database Management	Student will be able to Configure
ValenciaCollege	B.S	Network Engineering	CET2892C	200	92	Knowledge of how traffic flows across	Infrastructure Design	Student will be able to Configure
ValenciaCollege	B.S	Network Engineering	CET2892C	200	106	Knowledge of remote access technology	Information Technology	Student will be able to Configure
ValenciaCollege	B.S	Network Engineering	CET2892C	200	191	Skill in developing and applying security	Identity Management	Student will be able to
ValenciaCollege	B.S	Network Engineering	CET2892C	200	208	Skill in maintaining databases	Database Management	Student will be able to Configure
ValenciaCollege	B.S	Network Engineering	CET2892C	200	237	Skill in using Virtual Private Network	Encryption	Student will be able to Deploy
ValenciaCollege	B.S	Network Engineering	CET2892C	200	313	Knowledge of logging services for network	Information Systems/Network	Student will be able to Configure
ValenciaCollege	B.S	Network Engineering	CET2892C	200	901	Knowledge of the capabilities of	Network Management	tudent will be able to Configure
ValenciaCollege	B.S	Network Engineering	CET2892C	200	985	Skill in configuring and utilizing network	Configuration Management	Student will be able to Deploy
ValenciaCollege	B.S	Network Engineering	CET2892C	200	986	Knowledge of organizational	Identity Management	Student will be able to

ValenciaCollege	B.S	Network Engineering	CET2892C	200	989	Knowledge of Voice over Internet Protocol	Telecommunications	tudent will be able to Configure
ValenciaCollege	B.S	Network Engineering	CET 2880C	200	29	Knowledge of data backup, types of	Computer Forensics	Student will be able to Perform
ValenciaCollege	B.S	Network Engineering	CET 2880C	200	146	Knowledge of the types of Intrusion	Computer Network Defense	Student will be able to Define
ValenciaCollege	B.S	Network Engineering	CET 2880C	200	287	Knowledge of file system	Operating Systems	Student will be able to Explain
ValenciaCollege	B.S	Network Engineering	CET 2880C	200	290	Knowledge of processes for seizing	Forensics	Student will be able to Outline
ValenciaCollege	B.S	Network Engineering	CET 2880C	200	381	Skill in using forensic tool suites (e.g.	Computer Forensics	Student will be able to Operate
ValenciaCollege	B.S	Network Engineering	CET 2880C	200	895	Skill in recognizing and categorizing	Information Assurance	Student will be able to Identify
ValenciaCollege	B.S	Network Engineering	CET 2880C	200	968	Knowledge of softwarerelated	Information Systems/Network	Student will be able to Explain
ValenciaCollege	B.S	Network Engineering	CET 2880C	200	991	Knowledge of different classes of	Computer Network Defense	Student will be able to Identify
New Jersey City University	B.S	Elective	SECU 422	400	25	Knowledge of critical p	Cryptography	Cryptosecurity and Key
New Jersey City University	B.S	Elective	SECU 422	400	27	Knowledge of cryptolo	Cryptography	Cryptosecurity and Key
New Jersey City University	B.S	Elective	SECU 422	400	37	Knowledge of disaster	Incident Manageme	Contingency Planning/Disaster
New Jersey City University	B.S	Elective	SECU 422	400	55	Knowledge of Informat	Information Assurar	Risk Management Physical Security
New Jersey City University	B.S	Elective	SECU 422	400	56	Knowledge of informat	Information Assurar	Software Security
New Jersey City University	B.S	Elective	SECU 422	400	69	Knowledge of Risk Mar	Information System	Risk Management
New Jersey City University	B.S	Elective	SECU 422	400	77	Knowledege of current	Information System	Auditing and Monitoring
New Jersey City University	B.S	Elective	SECU 422	400	98	Knowledge of policy-ba	Identity Manageme	Security Planning
New Jersey City University	B.S	Elective	SECU 422	400	108	Knowledge of risk man	Risk Management	Risk Management
New Jersey City University	B.S	Elective	SECU 422	400	111	Knowledge of security	Information System	Systems Lifecycle Management
New Jersey City University	B.S	Elective	SECU 422	400	129	Knowledge of systems	Systems Life Cycle	Systems Lifecycle Management
New Jersey City University	B.S	Elective	SECU 422	400	130	Knowledge of systems	Systems Testing and	Systems Lifecycle Management
New Jersey City University	B.S	Elective	SECU 422	400	132	Knowledge of technolo	Systems Integration	Systems Lifecycle Management
New Jersey City University	B.S	Elective	SECU 422	400	141	Knowledge of the ente	Information Technol	Systems Lifecycle Management
New Jersey City University	B.S	Elective	SECU 422	400	144	Knowledge of the syste	Systems Life Cycle	Systems Lifecycle Management
New Jersey City University	B.S	Elective	SECU 422	400	145	Knowledge of the type	Systems Life Cycle	Systems Lifecycle Management
New Jersey City University	B.S	Elective	SECU 422	400	173	Skill in creating policies	Information System	Security Planning
New Jersey City University	B.S	Elective	SECU 422	400	179	Skill in designing securi	Information Assurar	Physical Security Measures
New Jersey City University	B.S	Elective	SECU 422	400	183	Skill in determining ho	Information Assurar	Security Planning Systems Lifecycle
New Jersey City University	B.S	Elective	SECU 422	400	197	Skill in discerning the p	Information System	Physical Security Measures
New Jersey City University	B.S	Elective	SECU 422	400	204	Skill in identifying poss	Systems Life Cycle	Systems Lifecycle Management

New Jersey City University	B.S	Elective	SECU 422	400	326	Knowledge of security	Information Systems	Physical Security Measures
New Jersey City University	B.S	Elective	SECU 422	400	327	Knowledge of security	Information Assurar	Software Security
New Jersey City University	B.S	Elective	SECU 422	400	893	Skill in securing networ	Information Assurar	Network Security
New Jersey City University	B.S	Elective	SECU 422	400	965	Knowledge of organiza	Risk Management	Risk Management
New Jersey City University	B.S	Elective	SECU 422	400	968	Knowledge of software	Information Systems	Software Security
New Jersey City University	B.S	Elective	SECU 422	400	979	Knowledge of supply cl	Risk Management	Risk Management
New Jersey City University	B.S	Elective	SECU 422	400	1021	Knowledge of threat as	Risk Management	Risk Management
New Jersey City University	B.S	Elective	SECU 422	400	1061	Knowledge of the lifecy	Systems Life Cycle	Systems Lifecycle Management
New Jersey City University	B.S	National Security Studies	SECU 222	200	3	Skill in conducting vuln	Vulnerabilities Asses	Threats and Vulnerabilities
New Jersey City University	B.S	National Security Studies	SECU 222	200	4	Ability to identify syste	Vulnerabilities Asses	Threats and Vulnerabilities
New Jersey City University	B.S	National Security Studies	SECU 222	200	5	Ability to match the ap	Knowledge Manage	Threats and Vulnerabilities
New Jersey City University	B.S	National Security Studies	SECU 222	200	10	Knowledge of applicati	Vulnerabilities Asses	Threats and Vulnerabilities
New Jersey City University	B.S	National Security Studies	SECU 222	200	63	Knowledge of Informat	Information Assurar	Availability; Confidentiality;
New Jersey City University	B.S	National Security Studies	SECU 222	200	90	Knowledge of operatin	Operating Systems	System Operating Environment
New Jersey City University	B.S	National Security Studies	SECU 222	200	124	Knowledge of system d	Logical Systems Des	History; Current Methodology
New Jersey City University	B.S	National Security Studies	SECU 222	200	156	Skill in applying confide	Information Assurar	Availability; Confidentiality;
New Jersey City University	B.S	National Security Studies	SECU 222	200	177	Skill in designing count	Vulnerabilities Asses	INFOSEC Material Information
New Jersey City University	B.S	National Security Studies	SECU 222	200	281	Knowledge of electron	Hardware	Automated Information
New Jersey City University	B.S	National Security Studies	SECU 222	200	329	Knowledge of surveilla	Surveillance	INFOSEC Material Information
New Jersey City University	B.S	National Security Studies	SECU 222	200	337	Knowledge of the nexu	External Awareness	INFOSEC Material Information
New Jersey City University	B.S	National Security Studies	SECU 222	200	1074	Knowledge of transmis	Telecommunications	Communications II
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	5	Ability to match the appropriate	Knowledge Management	1.6. Defining Cryptographic
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	8	Knowledge of access authentication	Identity Management	4.1.1. Authentication
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	9	Knowledge of applicable business	Requirements Analysis	11.1. Business Processes
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	12	Knowledge of communication	Infrastructure Design	1. Cryptographic Overview
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	22	Knowledge of computer networking	Infrastructure Design	
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	3.3.1. SHA -1 3.3.2. MD-5
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	27	Knowledge of cryptology	Cryptography	1. Cryptographic Overview
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	28	Knowledge of data administration and	Data Management	4.4.4. Data Considerations –
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	44	Knowledge of enterprise messaging	Enterprise Architecture	8.3.4. Bulk Data Confidentiality &

Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	50	Knowledge of how network services and	Infrastructure Design	7.2.1. Secure Data Network
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	63	Knowledge of Information	Information Assurance	4.1.1. Authentication
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	70	Knowledge of information	Information Systems/Network	3.1. Asymmetric Encryption is: two
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	79	Knowledge of network access,	Identity Management	5. PKI 5.1. Multiple
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	87	Knowledge of network traffic	Information Systems/Network	9.3. Sniff Network Traffic to evaluate
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	108	Knowledge of risk management	Risk Management	4.4. Key Management
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	109	Knowledge of secure configuration	Configuration Management	4.4. Key Management
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	110	Knowledge of security management	Information Assurance	4.4. Key Management
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	120	Knowledge of sources,	Data Management	4.4.4. Data Considerations –
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	129	Knowledge of systems lifecycle management	Systems Life Cycle	4.4.1. Key Lifecycle
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	11.3.2. Build Test Cases
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	132	Knowledge of technoloy integration	Systems Integration	11.6.1. Integration with
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	145	Knowledge of the type and frequency of	Systems Life Cycle	11.4. VPN Maintenance
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	148	Knowledge of VPN security.	Encryption	7. VPN Overview 7.1. VPN
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	169	Skill in conducting test events	Systems Testing and Evaluation	11.3.2. Build Test Cases
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	179	Skill in designing security controls	Information Assurance	4.1.1. Authentication
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	193	Skill in developing, testing, and	Information Assurance	11.3.2. Build Test Cases
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	237	Skill in using Virtual Private Network	Encryption	7. VPN Overview 7.1. VPN
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	284	Knowledge of encryption algorithms	Cryptography	8.4. SSL 8.4.1. History of
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	387	Skill in verifying the integrity of encrypted	Encryption	4.1.3. Integrity
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	979	Knowledge of supply chain risk	Risk Management	11.6.2. Periodic Risk Assessments
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	1021	Knowledge of threat assessment	Risk Management	11.6.2. Periodic Risk Assessments
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	1037	Knowledge of information	Risk Management	11.6.2. Periodic Risk Assessments
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	1059	Knowledge of networking protocols	Infrastructure Design	7.2.1. Secure Data Network
Howard Community	A.S	Encryption and VPN Technology	CMSY 262	200	1114	Knowledge of encryption	Cryptography	1. Cryptographic Overview
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	11.1. Threats, Vulnerabilities,
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	4	Ability to identify systemic security	Vulnerabilities Assessment	11.1. Threats, Vulnerabilities,
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	8	Knowledge of access authentication	Identity Management	9. Access Control Systems and
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	9	Knowledge of applicable business	Requirements Analysis	11.1. Threats, Vulnerabilities,
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	10	Knowledge of application	Vulnerabilities Assessment	11.1. Threats, Vulnerabilities,

Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	38	Knowledge of organization's	Information Assurance	13. Security Architecture and
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	49	Knowledge of host/network access	Information Systems/Network	9. Access Control Systems and
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	50	Knowledge of how network services and	Infrastructure Design	13.1. Network Protocol Stack
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	51	Knowledge of how system components	Systems Integration	8.1. Install and Configure an IDS
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	59	Knowledge of Intrusion Detection	Computer Network Defense	2. IDS System Concepts
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	60	Knowledge of incident categories, incident	Incident Management	6.4. Demonstrate Incident response
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	61	Knowledge of incident response and	Incident Management	6.4. Demonstrate Incident response
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	66	Knowledge of intrusion detection	Computer Network Defense	2. IDS System Concepts
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	68	Knowledge of information	Information Technology	13. Security Architecture and
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	79	Knowledge of network access,	Identity Management	9. Access Control Systems and
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	81	Knowledge of network	Infrastructure Design	1. TCP/IP Structure of a
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	82	Knowledge of network design	Infrastructure Design	13.2. Common flaws and security
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	83	Knowledge of network hardware	Hardware	2. IDS System Concepts
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	92	Knowledge of how traffic flows across	Infrastructure Design	1. TCP/IP Structure of a
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	93	Knowledge of packet-level analysis	Vulnerabilities Assessment	1. TCP/IP Structure of a
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	111	Knowledge of security system design tools,	Information Systems/Network	13.2. Common flaws and security
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	120	Knowledge of sources,	Data Management	11.1. Threats, Vulnerabilities,
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	123	Knowledge of system and application	Vulnerabilities Assessment	11.1. Threats, Vulnerabilities,
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	126	Knowledge of system software and	Requirements Analysis	14.1. ISO/OSI Layers and
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	8.4. Simulate Attacks on the
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	133	Knowledge of telecommunications	Telecommunications	14. Telecommunicati
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	139	Knowledge of common networking	Infrastructure Design	1. TCP/IP Structure of a
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	141	Knowledge of the enterprise	Information Technology	13. Security Architecture and
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	145	Knowledge of the type and frequency of	Systems Life Cycle	8.5. Adjust the system for
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	146	Knowledge of the types of Intrusion	Computer Network Defense	2. IDS System Concepts
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	150	Knowledge of what constitutes a network	Information Systems/Network	11.1. Threats, Vulnerabilities,
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	157	Skill in applying host/network access	Identity Management	9. Access Control Systems and
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	8.6.2.4. Taking Corrective
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	169	Skill in conducting test events	Systems Testing and Evaluation	8.4. Simulate Attacks on the
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	170	Skill in configuring and optimizing	Software Engineering	8.1. Install and Configure an IDS

Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	173	Skill in creating policies that relfect	Information Systems Security	11.2.1. Systems Housekeeping
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	177	Skill in designing countermeasures to	Vulnerabilities Assessment	8.5. Adjust the system for
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	180	Skill in designing the integration of	Systems Integration	13.2. Common flaws and security
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	181	Skill in detecting host and network based	Computer Network Defense	2.3.1. Network-Based Intrusion
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	191	Skill in developing and applying security	Identity Management	9. Access Control Systems and
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	210	Skill in mimicking threat behaviors	Computer Network Defense	8.4. Simulate Attacks on the
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	214	Skill in performing packet-level analysis	Vulnerabilities Assessment	1.2. Packet Sniffing
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	217	Skill in preserving evidence integrity	Computer Forensics	8.6.2.5. Gathering Data for
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	221	Skill in testing and configuring network	Network Management	8.1. Install and Configure an IDS
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	229	Skill in using incident handling	Incident Management	6.4. Demonstrate Incident response
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	277	Knowledge of defense in-depth principles	Computer Network Defense	13. Security Architecture and
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	290	Knowledge of processes for seizing	Forensics	8.6.2.5. Gathering Data for
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	895	Skill in recognizing and categorizing	Information Assurance	11.1. Threats, Vulnerabilities,
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	966	Knowledge of enterprise incident	Incident Management	6.4. Demonstrate Incident response
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	979	Knowledge of supply chain risk	Risk Management	12.2. Defining Risk
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	990	Knowledge of common attack	Computer Network Defense	4. Attacks 4.1. Define the
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	1021	Knowledge of threat assessment	Risk Management	12.3. Risk Assessment
Howard Community	A.S	Introduction to Intrusion	CMSY 164	100	1120	Ability to interpret and incorporate data	Data Management	2.4.1. Freeware NIDS: Snort
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	Active Reconnaissance
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	10	Knowledge of application	Vulnerabilities Assessment	Identify different vulnerabilities
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	22	Knowledge of computer networking	Infrastructure Design	Describe the Network
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	31	Knowledge of data mining and data	Data Management	Describe the concepts of Data
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	58	Knowledge of known vulnerabilities from	Information Systems/Network	Physical Attacks and Network
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	59	Knowledge of Intrusion Detection	Computer Network Defense	Analyzing Attack Artifacts
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	87	Knowledge of network traffic	Information Systems/Network	Analyzing Attack Artifacts
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	92	Knowledge of how traffic flows across	Infrastructure Design	Overview of Networks
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	93	Knowledge of packet-level analysis	Vulnerabilities Assessment	Analyzing Attack Artifacts
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	95	Knowledge of penetration testing	Vulnerabilities Assessment	Physical Attacks and Network
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	106	Knowledge of remote access technology	Information Technology	Post Exploitation *Uploading
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	123	Knowledge of system and application	Vulnerabilities Assessment	Identify different vulnerabilities

Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	150	Knowledge of what constitutes a network	Information Systems/Network	Execute the attack or Attack
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	153	Skill in handling malware	Computer Network Defense	Describe various Malware and
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	214	Skill in performing packet-level analysis	Vulnerabilities Assessment	Analyzing Attack Artifacts
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	225	Skill in the use of penetration testing	Vulnerabilities Assessment	Passive Reconnaissance
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	233	Skill in using protocol analyzers	Vulnerabilities Assessment	Analyzing Attack Artifacts
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	274	Knowledge of concepts, principles,	Computer Network Defense	Physical Attacks and Network
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	285	Knowledge of evasion strategies and	Computer Network Defense	Passive Reconnaissance
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	294	Knowledge of hacking methodologies in	Surveillance	Perform scanning and probing the
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	342	Knowledge of Unix command line (e.g.,	Computer Languages	Perform Reconnaissance
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	346	Knowledge of which system files (e.g. log	Computer Forensics	Data Manipulation
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	347	Knowledge of Windows command	Operating Systems	Perform Reconnaissance
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	Analyze different attack
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	899	Skill in gathering information from	Information Management	Perform Reconnaissance
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	907	Skill in data mining techniques	Data Management	Data Manipulation
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	922	Skill in using network analysis tools to	Vulnerabilities Assessment	Active Reconnaissance
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	990	Knowledge of common attack	Computer Network Defense	Physical Attacks and Network
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	1029	Knowledge of malware analysis	Computer Network Defense	Malware Analysis *Static Analysis
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	1044	Skill in identifying forensic footprints	Computer Forensics	Active Reconnaissance
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Passive Reconnaissance
Howard Community	A.S	Cyber Forensics 1	CFOR 909	100	1096	Knowledge of malware analysis	Computer Network Defense	Malware Analysis *Static Analysis
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	8	Knowledge of access authentication	Identity Management	2.4.3. User Accounts,
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	9	Knowledge of applicable business	Requirements Analysis	2.8. Continuity Planning and
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	12	Knowledge of communication	Infrastructure Design	7.1.2. Principles of Cryptography
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	15	Knowledge of capabilities and	Hardware	1. Firewall Planning and
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	19	Knowledge of Computer Network	Computer Network Defense	6.7. Password Security Tools
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	22	Knowledge of computer networking	Infrastructure Design	3.3. Firewall Network
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	7.4.3. Using IPSec Encryption
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	27	Knowledge of cryptology	Cryptography	7.1.2. Principles of Cryptography
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	28	Knowledge of data administration and	Data Management	6.1.1.1. Data Classification
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	37	Knowledge of disaster recovery and	Incident Management	2.8.1. Defining Incident, Incident

Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	38	Knowledge of organization's	Information Assurance	3.2.4. Firewall Architectures
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	49	Knowledge of host/network access	Information Systems/Network	6.1. Access Control
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	50	Knowledge of how network services and	Infrastructure Design	9.4. Tunneling Protocols Used
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	51	Knowledge of how system components	Systems Integration	8.1. Installing A Bastian Host:
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	52	Knowledge of human-computer interaction	Human Factors	6.6. Password Security Issues
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	58	Knowledge of known vulnerabilities from	Information Systems/Network	
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	59	Knowledge of Intrusion Detection	Computer Network Defense	11.4.1. Using an Intrusion
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	60	Knowledge of incident categories, incident	Incident Management	2.8.1. Defining Incident, Incident
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	61	Knowledge of incident response and	Incident Management	2.8.1. Defining Incident, Incident
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	63	Knowledge of Information	Information Assurance	6.2. The Authentication
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	66	Knowledge of intrusion detection	Computer Network Defense	11.4.1. Using an Intrusion
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	70	Knowledge of information	Information Systems/Network	1. Firewall Planning and
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	79	Knowledge of network access,	Identity Management	7.2. Digital Certificates, and
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	82	Knowledge of network design	Infrastructure Design	1. Firewall Planning and
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	93	Knowledge of packet-level analysis	Vulnerabilities Assessment	4.1. Understanding
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	98	Knowledge of policy-based and risk	Identity Management	2.4.3. User Accounts,
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	106	Knowledge of remote access technology	Information Technology	2.4.3. User Accounts,
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	108	Knowledge of risk management	Risk Management	2.5.5. Identify Security Risks
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	111	Knowledge of security system design tools,	Information Systems/Network	1. Firewall Planning and
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	113	Knowledge of server and client operating	Operating Systems	6.4.2. Client Authentication
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	123	Knowledge of system and application	Vulnerabilities Assessment	2.8.2.1. Identification and
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	146	Knowledge of the types of Intrusion	Computer Network Defense	11.4.1. Using an Intrusion
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	157	Skill in applying host/network access	Identity Management	6.1. Access Control
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	173	Skill in creating policies that relfect	Information Systems Security	2. Developing a Security Policy
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	177	Skill in designing countermeasures to	Vulnerabilities Assessment	11.4.4. During and After an
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	181	Skill in detecting host and network based	Computer Network Defense	11.4.1. Using an Intrusion
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	191	Skill in developing and applying security	Identity Management	6.1. Access Control
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	193	Skill in developing, testing, and	Information Assurance	2.8.1. Defining Incident, Incident
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	11.1. Making Your Firewall Meet
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	1. Firewall Planning and

Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	217	Skill in preserving evidence integrity	Computer Forensics	11.4.5. Compiling Legal Evidence
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	237	Skill in using Virtual Private Network	Encryption	9.1. VPN Components and
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	277	Knowledge of defense in-depth principles	Computer Network Defense	3.2.4. Firewall Architectures
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	356	Skill in determining installed patches on	Operating Systems	11.1.2. Adding Software Updates
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	891	Skill in configuring and utilizing hardware-	Configuration Management	3. Firewall Configuration
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	895	Skill in recognizing and categorizing	Information Assurance	2.8.2.1. Identification and
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	897	Skill in performing damage assessments	Information Assurance	2.8.2.3. Assessment of
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	952	Knowledge of emerging security	Technology Awareness	11.1.1. Identifying New
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	966	Knowledge of enterprise incident	Incident Management	2.8.3. Incident Response
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	985	Skill in configuring and utilizing network	Configuration Management	9.1. VPN Components and
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	986	Knowledge of organizational	Identity Management	2.4.3. User Accounts,
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	1011	Knowledge of processes for	Security	11.3.1. Preparing Usage Reports
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	1059	Knowledge of networking protocols	Infrastructure Design	9.4. Tunneling Protocols Used
Howard Community	A.S	Firewalls and Internet Security	CMSY 163	100	1114	Knowledge of encryption	Cryptography	7. Encryption and Firewalls
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	3	Skill in conducting vulnerability scans	Vulnerabilities Assessment	5. Vulnerability Assessment and
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	4	Ability to identify systemic security	Vulnerabilities Assessment	5. Vulnerability Assessment and
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	5	Ability to match the appropriate	Knowledge Management	1.2.1. Key Information
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	8	Knowledge of access authentication	Identity Management	11.3. Authentication
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	10	Knowledge of application	Vulnerabilities Assessment	13.5. Designing Security Policy
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	12	Knowledge of communication	Infrastructure Design	14. Cryptography 14.1. Defining
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	17	Knowledge of certified ethical	Vulnerabilities Assessment	4. Legal, Ethical and Professional
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	22	Knowledge of computer networking	Infrastructure Design	8. Network Security and
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	24	Knowledge of concepts and	Data Management	15.4.1. Forensics Defined
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	27	Knowledge of cryptology	Cryptography	14. Cryptography 14.1. Defining
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	28	Knowledge of data administration and	Data Management	1.11.3. Data Responsibilities
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	29	Knowledge of data backup, types of	Computer Forensics	15.2.3. Data Backups
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	31	Knowledge of data mining and data	Data Management	6.3.2. Database Collection,
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	37	Knowledge of disaster recovery and	Incident Management	15. Business Continuity
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	38	Knowledge of organization's	Information Assurance	3.1.1. Enterprise Information
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	41	Knowledge of organization's Local	Infrastructure Design	8.3.3. Virtual LANs (VLANs)

Howard Community	A.S	Introduction to Network Security	CMSY 162	100	46	Knowledge of fault tolerance	Information Assurance	15.2.2. Redundancy and
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	49	Knowledge of host/network access	Information Systems/Network	11.2.1. Access Control Lists
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	50	Knowledge of how network services and	Infrastructure Design	9.1. Common Network
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	51	Knowledge of how system components	Systems Integration	1.5. Components of an Information
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	52	Knowledge of human-computer interaction	Human Factors	3.9. Security Education,
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	55	Knowledge of Information	Information Assurance	1.2.2. Information Assurance
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	60	Knowledge of incident categories, incident	Incident Management	15.1.2. Incident Response
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	61	Knowledge of incident response and	Incident Management	15.1.2. Incident Response
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	63	Knowledge of Information	Information Assurance	1.3.1. Availability, Accuracy,
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	68	Knowledge of information	Information Technology	3.10. Design of Security
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	69	Knowledge of Risk Management	Information Systems Security	13. Risk Management:
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	70	Knowledge of information	Information Systems/Network	8. Network Security and
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	77	Knowledege of current industry	Information Systems/Network	1.8. Top-Down Approach to
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	79	Knowledge of network access,	Identity Management	14.5. Public Key Infrastructure
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	82	Knowledge of network design	Infrastructure Design	11.3.4. Lightweight
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	83	Knowledge of network hardware	Hardware	6.1.1.2. Hardware Security
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	90	Knowledge of operating systems	Operating Systems	6.1.2. Securing the Operating
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	98	Knowledge of policy-based and risk	Identity Management	11.2.2. Group Policies
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	105	Knowledge of legal governance related to	Legal, Government and Jurisprudence	4. Legal, Ethical and Professional
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	106	Knowledge of remote access technology	Information Technology	8.3.3. Virtual LANs (VLANs)
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	107	Knowledge of resource	Project Management	7.1. Information Security Project
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	108	Knowledge of risk management	Risk Management	13. Risk Management:
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	109	Knowledge of secure configuration	Configuration Management	5.3.2. Configuring Controls
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	110	Knowledge of security management	Information Assurance	7.5.1. Security Change/Configurat
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	111	Knowledge of security system design tools,	Information Systems/Network	3.3. Systems design
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	113	Knowledge of server and client operating	Operating Systems	2.2.3. Client-Side Attacks
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	122	Knowledge of system administration	Operating Systems	9.2. Network Administration
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	123	Knowledge of system and application	Vulnerabilities Assessment	5. Vulnerability Assessment and
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	124	Knowledge of system design tools,	Logical Systems Design	3.3. Systems design
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	126	Knowledge of system software and	Requirements Analysis	3.1. Information Security Policy,

Howard Community	A.S	Introduction to Network Security	CMSY 162	100	129	Knowledge of systems lifecycle management	Systems Life Cycle	1.9. The System Development Life
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	130	Knowledge of systems testing and evaluation	Systems Testing and Evaluation	5.2. Vulnerability Scanning vs.
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	133	Knowledge of telecommunications	Telecommunications	16.7. Telecommunicati
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	135	Knowledge of the capabilities and	Data Management	6.3.2. Database Collection,
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	137	Knowledge of the characteristics of	Data Management	15.2.3. Data Backups
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	139	Knowledge of common networking	Infrastructure Design	9.1. Common Network
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	141	Knowledge of the enterprise	Information Technology	3.1.1. Enterprise Information
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	143	Knowledge of the organization's	Enterprise Architecture	3.1.1. Enterprise Information
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	150	Knowledge of what constitutes a network	Information Systems/Network	5. Vulnerability Assessment and
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	156	Skill in applying confidentiality,	Information Assurance	1.3.1. Availability, Accuracy,
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	157	Skill in applying host/network access	Identity Management	11.2.1. Access Control Lists
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	160	Skill in assessing the robustness of security	Vulnerabilities Assessment	5. Vulnerability Assessment and
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	170	Skill in configuring and optimizing	Software Engineering	5.3.2. Configuring Controls
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	173	Skill in creating policies that relfect	Information Systems Security	3.1. Information Security Policy,
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	179	Skill in designing security controls	Information Assurance	1.2.2. Information Assurance
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	191	Skill in developing and applying security	Identity Management	11. Access Control
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	193	Skill in developing, testing, and	Information Assurance	15. Business Continuity
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	205	Skill in implementing, maintaining, and	Information Systems/Network	7.5. Information Technology
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	225	Skill in the use of penetration testing	Vulnerabilities Assessment	5. Vulnerability Assessment and
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	226	Skill in the use of social engineering	Human Factors	2.1. Malware and Social
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	229	Skill in using incident handling	Incident Management	15.1.2. Incident Response
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	231	Skill in using network management tools to	Network Management	9.1.2. Simple Network
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	234	Skill in using sub-netting tools	Infrastructure Design	8.3.2. Subnetting
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	237	Skill in using Virtual Private Network	Encryption	14.3.1. Encryption
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	261	Knowledge of basic concepts,	Telecommunications	9.3.2. IP Telephony
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	277	Knowledge of defense in-depth principles	Computer Network Defense	3.10. Design of Security
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	278	Knowledge of different types of	Telecommunications	8.3.3. Virtual LANs (VLANs)
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	284	Knowledge of encryption algorithms	Cryptography	14.7.1. Secure Sockets Layer
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	299	Knowledge of information security	Project Management	7.1. Information Security Project
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	320	Knowledge of external organizations	External Awareness	1.11. Security Professionals and

Howard Community	A.S	Introduction to Network Security	CMSY 162	100	344	Knowledge of virtualization	Operating Systems	8.3.3. Virtual LANs (VLANs)
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	379	Skill in using common digital forensics tools	Computer Forensics	15.4.1. Forensics Defined
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	891	Skill in configuring and utilizing hardware-	Configuration Management	5.3.2. Configuring Controls
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	895	Skill in recognizing and categorizing	Information Assurance	2. Attacks and Threats
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	896	Skill in protecting a network against	Computer Network Defense	2.1. Malware and Social
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	922	Skill in using network analysis tools to	Vulnerabilities Assessment	5.1.2. Assessment Tools
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	965	Knowledge of organization's risk	Risk Management	15.4. Incident Response
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	968	Knowledge of software-related	Information Systems/Network	3.10.1. Spheres of Security
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	979	Knowledge of supply chain risk	Risk Management	13. Risk Management:
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	986	Knowledge of organizational	Identity Management	11. Access Control
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	990	Knowledge of common attack	Computer Network Defense	2.2. Application and Network
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	1011	Knowledge of processes for	Security	5.3.4. Reporting 16.15.
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	1021	Knowledge of threat assessment	Risk Management	2. Attacks and Threats
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	1037	Knowledge of information	Risk Management	13.2. Risk Management
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	1038	Knowledge of local specialized system	Infrastructure Design	7.5.3.1. Vendor Support and
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	1061	Knowledge of the lifecycle process	Systems Life Cycle	1.9. The System Development Life
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	1072	Knowledge of network security	Information Systems/Network	3.10. Design of Security
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	1074	Knowledge of transmission records	Telecommunicatio ns	10.1.1. Attacks on Bluetooth
Howard Community	A.S	Introduction to Network Security	CMSY 162	100	1114	Knowledge of encryption	Cryptography	14.3.1. Encryption
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	29	Knowledge of data backup, types of	Computer Forensics	Live Acquisition vs. Static
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	60	Knowledge of incident categories, incident	Incident Management	Incident Response Process
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	61	Knowledge of incident response and	Incident Management	Incident Response
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	66	Knowledge of intrusion detection	Computer Network Defense	Analysis of Log Files
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	87	Knowledge of network traffic	Information Systems/Network	Analysis of Network TrafficX
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	108	Knowledge of risk management	Risk Management	Incident Response
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	137	Knowledge of the characteristics of	Data Management	Live Acquisition vs. Static
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	150	Knowledge of what constitutes a network	Information Systems/Network	Incident Response Process
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	153	Skill in handling malware	Computer Network Defense	Malware analysis *Definition of
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	Incident Response
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	214	Skill in performing packet-level analysis	Vulnerabilities Assessment	Analysis of Network Traffic

Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	346	Knowledge of which system files (e.g. log	Computer Forensics	Analysis of Log Files
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	360	Skill in identifying and extracting data of	Computer Forensics	Volatile data Analysis
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	367	Skill in multi-disciplined	Writing	Writing Computer Forensics Report
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	896	Skill in protecting a network against	Computer Network Defense	Malware analysis *Definition of
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	897	Skill in performing damage assessments	Information Assurance	II. Incident Response
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	922	Skill in using network analysis tools to	Vulnerabilities Assessment	Analysis of Network Traffic
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	966	Knowledge of enterprise incident	Incident Management	Incident Response Process
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	1093	Knowledge of common forensic tool	Computer Forensics	Analysis of Network Traffic
Howard Community	A.S	Cyber Forensics 2	CFOR 910	200	1099	Skill in analyzing volatile data	Computer Forensics	Volatile data Analysis
Howard Community	A.S	Microcomputer Operating	CMSY 219	200	90	Knowledge of operating systems	Operating Systems	Identify the versions of
Howard Community	A.S	Microcomputer Operating	CMSY 219	200	182	Skill in determining an appropriate level of	Systems Testing and Evaluation	
Howard Community	A.S	Microcomputer Operating	CMSY 219	200	287	Knowledge of file system	Operating Systems	Identify file systems
Howard Community	A.S	Microcomputer Operating	CMSY 219	200	342	Knowledge of Unix command line (e.g.,	Computer Languages	Work with the Windows
Howard Community	A.S	Microcomputer Operating	CMSY 219	200	347	Knowledge of Windows command	Operating Systems	Work with the Windows
Howard Community	A.S	Microcomputer Operating	CMSY 219	200	356	Skill in determining installed patches on	Operating Systems	Describe how to manage and
Howard Community	A.S	Microcomputer Operating	CMSY 219	200	364	Skill in identifying, modifying, and	Operating Systems	Manage local security and
Howard Community	A.S	Microcomputer Operating	CMSY 219	200	386	Skill in using virtual machines	Operating Systems	Select and implement a
Howard Community	A.S	Microcomputer Operating	CMSY 219	200	1063	Knowledge of Unix/Linux operating	Operating Systems	Understand the boot-up process
Howard Community	A.S	Microcomputer Operating	CMSY 219	200	1121	Knowledge of Windows/Unix ports	Operating Systems	Describe how to manage and
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	4	Ability to identify systemic security	Vulnerabilities Assessment	Identifying Suspicious Events
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	5	Ability to match the appropriate	Knowledge Management	* Using The Common
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	8	Knowledge of access authentication	Identity Management	*Authentication and Password
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	12	Knowledge of communication	Infrastructure Design	* Virtual Private Network (VPN)
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	22	Knowledge of computer networking	Infrastructure Design	*TCP/IP Networking
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	25	Knowledge of critical protocols (e.g., IPSEC,	Cryptography	* VPN Core Activity 3:
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	27	Knowledge of cryptology	Cryptography	Understanding VPN Concepts
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	55	Knowledge of Information	Information Assurance	* Security Policy Designs and Risk
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	59	Knowledge of Intrusion Detection	Computer Network Defense	Network Defense Fundamentals
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	62	Knowledge of industry-standard and	Logical Systems Design	Define the elements of
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	63	Knowledge of Information	Information Assurance	* Ensuring Privacy

Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	64	Knowledge of information security	Information Systems/ Network	*Network Defense
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	70	Knowledge of information	Information Systems/Network	Network Defense Fundamentals
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	72	Knowledge of local area network (LAN)	Infrastructure Design	Strengthening Defense Through
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	76	Knowledge of measures or	Information Technology	Strengthening and Managing
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	77	Knowledege of current industry	Information Systems/Network	*Virtual Private Network (VPN)
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	81	Knowledge of network	Infrastructure Design	Network Defense Fundamentals
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	87	Knowledge of network traffic	Information Systems/Network	Network Defense Fundamentals
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	92	Knowledge of how traffic flows across	Infrastructure Design	Network Defense Fundamentals
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	93	Knowledge of packet-level analysis	Vulnerabilities Assessment	* Exploring IP Packet Structure
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	95	Knowledge of penetration testing	Vulnerabilities Assessment	* Penetration Testing
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	96	Knowledge of performance tuning	Information Technology	Strengthening Performance:
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	98	Knowledge of policy-based and risk	Identity Management	Security Policy Designs and Risk
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	106	Knowledge of remote access technology	Information Technology	Virtual Private Network (VPN)
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	108	Knowledge of risk management	Risk Management	Security Policy Designs and Risk
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	109	Knowledge of secure configuration	Configuration Management	Security Policy Development
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	110	Knowledge of security management	Information Assurance	Security Policy Development
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	111	Knowledge of security system design tools,	Information Systems/Network	Security Policy Development
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	137	Knowledge of the characteristics of	Data Management	Strengthening Defense Through
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	148	Knowledge of VPN security.	Encryption	VPN Core Activity 2: Encryption X
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	150	Knowledge of what constitutes a network	Information Systems/Network	Overview of Threats to
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	157	Skill in applying host/network access	Identity Management	Security Policy Development
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	173	Skill in creating policies that relfect	Information Systems Security	Security Policy Development
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	177	Skill in designing countermeasures to	Vulnerabilities Assessment	Security Policy Development
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	179	Skill in designing security controls	Information Assurance	Security Policy Development
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	197	Skill in discerning the protection needs (i.e.,	Information Systems/Network	Security Policy Designs and Risk
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	199	Skill in evaluating the adequacy of security	Vulnerabilities Assessment	Strengthening Defense Through
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	205	Skill in implementing, maintaining, and	Information Systems/Network	*Network Defense
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	210	Skill in mimicking threat behaviors	Computer Network Defense	Network Traffic Signatures
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	225	Skill in the use of penetration testing	Vulnerabilities Assessment	Network Traffic Signatures
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	237	Skill in using Virtual Private Network	Encryption	Virtual Private Network (VPN)

Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	277	Knowledge of defense in-depth principles	Computer Network Defense	Strengthening Defense Through
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	352	Skill in applying white hack hacking/security	Vulnerabilities Assessment	Network Traffic Signatures
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	975	Skill in integrating black box security	Quality Assurance	Network Traffic Signatures
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	985	Skill in configuring and utilizing network	Configuration Management	Virtual Private Network (VPN)
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	1037	Knowledge of information	Risk Management	Security Policy Designs and Risk
Howard Community	A.S	Hardening the Infrastructure	CMSY 263	200	1069	Knowledge of general attack stages (e.g.,	Computer Network Defense	Penetration Testing
Howard Community	A.S	Computer Forensics 1	CFOR 101	100	51	Knowledge of how system components	Systems Integration	Identify PC motherboard
Howard Community	A.S	Computer Forensics 1	CFOR 101	100	264	Knowledge of basic physical computer	Computers and Electronics	Identify PC motherboard
Howard Community	A.S	Computer Forensics 1	CFOR 101	100	281	Knowledge of electronic devices	Hardware	Identify PC motherboard
Howard Community	A.S	Computer Forensics 1	CFOR 101	100	290	Knowledge of processes for seizing	Forensics	Describe processing crime
Howard Community	A.S	Computer Forensics 1	CFOR 101	100	316	Knowledge of processes for	Criminal Law	Apply computer forensic
Howard Community	A.S	Computer Forensics 1	CFOR 101	100	347	Knowledge of Windows command	Operating Systems	Perform basic forensic
Howard Community	A.S	Computer Forensics 1	CFOR 101	100	369	Skill in collecting, processing,	Forensics	Apply computer forensic
Howard Community	A.S	Computer Forensics 1	CFOR 101	100	379	Skill in using common digital forensics tools	Computer Forensics	Perform basic forensic
Howard Community	A.S	Computer Forensics 1	CFOR 101	100	982	Knowledge of electronic evidence	Criminal Law	Define computer forensics and
Howard Community	A.S	Computer Forensics 1	CFOR 101	100	1036	Knowledge of applicable laws (e.g.,	Criminal Law	Define computer forensics and
Howard Community	A.S	Computer Forensics 2	CFOR 200	200	290	Knowledge of processes for seizing	Forensics	Describe proper evidence
Howard Community	A.S	Computer Forensics 2	CFOR 200	200	305	Knowledge of laws that affect cyber	Forensics	Examine local and national laws
Howard Community	A.S	Computer Forensics 2	CFOR 200	200	316	Knowledge of processes for	Criminal Law	Describe proper evidence
Howard Community	A.S	Computer Forensics 2	CFOR 200	200	366	Skill in law enforcement report	Technical Documentation	Prepare electronic
Howard Community	A.S	Computer Forensics 2	CFOR 200	200	369	Skill in collecting, processing,	Forensics	Describe proper evidence
Howard Community	A.S	Computer Forensics 2	CFOR 200	200	379	Skill in using common digital forensics tools	Computer Forensics	Describe proper evidence
Howard Community	A.S	Computer Forensics 2	CFOR 200	200	968	Knowledge of software-related	Information Systems/Network	Examine various data hiding
Howard Community	A.S	Computer Forensics 2	CFOR 200	200	982	Knowledge of electronic evidence	Criminal Law	Examine local and national laws
Howard Community	A.S	Computer Forensics 2	CFOR 200	200	1036	Knowledge of applicable laws (e.g.,	Criminal Law	Examine local and national laws
Howard Community	A.S	Computer Forensics 3	CFOR 210	200	24	Knowledge of concepts and	Data Management	Prepare a basic computer
Howard Community	A.S	Computer Forensics 3	CFOR 210	200	340	Knowledge of types and collection of	Computer Forensics	Explore methods of data storage
Howard Community	A.S	Computer Forensics 3	CFOR 210	200	360	Skill in identifying and extracting data of	Computer Forensics	Examine the data acquisition
Howard Community	A.S	Computer Forensics 3	CFOR 210	200	374	Skill in setting up a forensic workstation	Forensics	Prepare a basic computer
Howard Community	A.S	Computer Forensics 3	CFOR 210	200	379	Skill in using common digital forensics tools	Computer Forensics	Become familiar with the

Howard Community	A.S	Computer Forensics 3	CFOR 210	200	381	Skill in using forensic tool suites (e.g.	Computer Forensics	Become familiar with the
Howard Community	A.S	Computer Forensics 3	CFOR 210	200	889	Knowledge of deployable forensics	Computer Forensics	Develop basic computer
Howard Community	A.S	Computer Forensics 3	CFOR 210	200	890	Skill in conducting forensic analyses in	Computer Forensics	Examine electronic
Howard Community	A.S	Introduction to Unix and Linux	CMSY 255	200	342	Knowledge of Unix command line (e.g.,	Computer Languages	Understand the Unix/Linux file
Howard Community	A.S	Introduction to Unix and Linux	CMSY 255	200	371	Skill in reading, interpreting, writing,	Operating Systems	Learn to write shell scripts.
Howard Community	A.S	Introduction to Unix and Linux	CMSY 255	200	1063	Knowledge of Unix/Linux operating	Operating Systems	Understand the Unix/Linux file
Howard Community	A.S	Linux Sever Administration	CMSY 256	200	99	Knowledge of principles and	Systems Integration	Integrate Linux with an existing
Howard Community	A.S	Linux Sever Administration	CMSY 256	200	122	Knowledge of system administration	Operating Systems	Install Linux. ;Use RPM and YUM to
Howard Community	A.S	Linux Sever Administration	CMSY 256	200	132	Knowledge of technoloy integration	Systems Integration	Integrate Linux with an existing
Howard Community	A.S	Linux Sever Administration	CMSY 256	200	219	Skill in system administration for	Operating Systems	Install Linux. ;Use RPM and YUM to
Howard Community	A.S	Linux Sever Administration	CMSY 256	200	364	Skill in identifying, modifying, and	Operating Systems	Install Linux. ;Use RPM and YUM to
Howard Community	A.S	Linux Sever Administration	CMSY 256	200	1063	Knowledge of Unix/Linux operating	Operating Systems	Use RPM and YUM to maintain
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	98	Knowledge of policy-based and risk adaptive access controls	Identity Management	Define and identify Access Control and Authentication processes and be
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	173	Skill in creating policies that relfect system security objectives	Information Systems Security Certification	Discuss and analyze how computers and computer networks can be made secure.
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	984	Knowledge of computer network defense (CND) policies, procedures, and regulations	Computer Network Defense	Discuss and analyze how computers and computer networks can be made secure. Thereby, enabling
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	1070	Ability to determine impact of technology trend data on laws, regulations, and/or policies	Legal, Government and Jurisprudence	Discuss and analyze how computers and computer networks can be made secure. Thereby, enabling them to provide
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	8	Knowledge of access authentication methods	Identity Management	Define and identify Access Control and Authentication processes and be able to implement them.
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	49	Knowledge of host/network access controls (e.g., access control list)	Information Systems/Network Security	Define and identify Access Control and Authentication processes and be able to implement them.
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	63	Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Define and identify Access Control and Authentication processes and be able to implement them.
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	157	Skill in applying host/network access controls (e.g., access control list)	Identity Management	Define and identify Access Control and Authentication processes and be able to implement them.

Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	191	Skill in developing and applying security system access controls	Identity Management	Define and identify Access Control and Authentication processes and be able to implement them.
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	986	Knowledge of organizational information technology (IT) user security policies (e..g, account creation, password rules, access control)	Identity Management	Define and identify Access Control and Authentication processes and be able to implement them.
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	918	Ability to prepare and deliver education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures	Teaching Others	Discuss and analyze how computers and computer networks can be made secure. Thereby, enabling them to provide input on policies and plans for securing their computers and computer networks.
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	123	Knowledge of system and application security threats and vulnerabilities	Vulnerabilities Assessment	Foresee security threats and/or vulnerabilities and try to mitigate them ahead of time.
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities	Information Systems/Network Security	Foresee security threats and/or vulnerabilities and try to mitigate them ahead of time.
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	967	Knowledge of current and emerging threats/threat vectors	Information Systems/Network Security	Foresee security threats and/or vulnerabilities and try to mitigate them ahead of time.
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	4	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data	Vulnerabilities Assessment	Identify security issues when they are confronted, or recognize them before they happen.
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	27	Knowledge of cryptology	Cryptography	Name and discuss the cryptographic systems, recognize
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	1114	Knowledge of encryption methodologies	Cryptography	Name and discuss the cryptographic systems, recognize
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	197	Skill in discerning the protection needs (i.e., security controls) of information systems and networks	Information Systems/Network Security	Participate in discussions on choosing the best protection or prevention methods, given a specific network of
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	1033	Knowledge of basic system administration, network, and operating system hardening techniques	Information Systems/Network Security	Participate in discussions on choosing the best protection or prevention methods, given a specific network of computers, by
Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	29	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools	Computer Forensics	Provide ideas on establishing administrative security such as auditing, back ups, and training employees.

Mass Bay Community College	A.S.	Fundamentals of Cyber Security	CS 116	100	1040	Knowledge of relevant laws, policies, procedures ,or governance as they relate to work that may impact critical infrastructure	Criminal Law	Provide ideas on establishing administrative security such as auditing, back ups, and training employees.

CYBERSECURITY EDUCATION
SOLUTIONS FOR THE NATION

National CyberWatch Center
Prince George's Community College
Room 129B
301 Largo Road
Largo, MD 20774

www.nationalcyberwatch.org