CSEC2Y Task Group

Cara Tang*+ | Portland Community College, Portland, OR
Cindy Tucker* | Bluegrass Community and Technical College, Lexington, KY
Christian Servin* | El Paso Community College, El Paso, TX
Markus Geissler* | Cosumnes River College, Sacramento, CA
Melissa Stange* | Lord Fairfax Community College, Middletown, VA
Nancy Jones | Coastline Community College, Garden Grove, CA
James Kolasa | Bluegrass Community and Technical College, Lexington, KY
Amelia Phillips | Highline College, Des Moines, WA
Lambros Piskopos | Wilbur Wright College, Chicago, IL
Pam Schmelz | Ivy Tech Community College, Columbus, IN

* Steering Committee
+ Task Group Chair
# Table of Contents

## Introduction
- Overview of the Curricular Development Process 4
- How to Use These Guidelines 4
- Two-Year/Community College Environment 4
- Career and Transfer Programs 6
- Diversity in the Computing Profession 7
- Ethics and Professionalism 7
- Mathematics Requirements 8
- The Cybersecurity Discipline 8

## Cybersecurity Curricular Framework

### Knowledge Areas

#### Essential
- Data Security 10
- Software Security 12
- Component Security 13
- Connection Security 14
- System Security 15
- Human Security 16
- Organizational Security 17
- Societal Security 18

#### Supplemental
- Data Security 19
- Software Security 21
- Component Security 22
- Connection Security 23
- System Security 25
- Human Security 26
- Organizational Security 27
- Societal Security 29
Introduction

Overview of the Curricular Development Process

In early 2018 the Association for Computing Machinery (ACM) endorsed their first curricular volume for Cybersecurity designed for four-year institutions, Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, referred to as CSEC2017 (cybered.acm.org). The ACM Committee for Computing Education in Community Colleges (CCECC) formed a task force in early 2019 to create similar cybersecurity curriculum guidance for two-year programs. The content of these guidelines, known as CSEC2Y, is based on CSEC2017, and considers other inputs including the CAE-CD 2Y 2019 knowledge units (requirements of the NSA and DHS National Centers of Academic Excellence in Cyber Defense) and the NICE cybersecurity workforce framework.

[In a future draft we will provide more details on how other frameworks (CAE KUs, NICE framework) influenced and align with these guidelines.]

The ten-member CSEC2Y task force is made up of community college educators with varying expertise in cybersecurity from community and technical colleges across the country. The task force has been meeting online since April 2019, with one in-person meeting during 3CS in August 2019. In addition to the focused work and contributions of these ten educators, input was incorporated from breakout groups at a pre-NICE event in November 2019. The result is this StrawDog draft, an early draft being presented publicly to the community for review and comment. We hope to get significant feedback from the community that will help improve the guidance and make it as useful as possible.

After StrawDog closes for public comment, the task force will work to incorporate the feedback appropriately and further improve the guidance. A second draft called IronDog will be released for public review and comment in Summer 2019, with the final guidelines expected at the end of 2019.

How to Use These Guidelines

[In a future draft we will provide guidance on how to use these guidelines for activities such as program review.]

Two-Year/Community College Environment

According to the American Association of Community Colleges, nearly one-half of all undergraduates in the United States are enrolled in two-year colleges, and more than half of all
first-time college freshman attend community and technical colleges. “Community colleges are centers of educational opportunity. They are an American invention that put publicly funded higher education at close-to-home facilities, beginning nearly 100 years ago with Joliet Junior College (in Joliet, Illinois). Since then, they have been inclusive institutions that welcome all who desire to learn, regardless of wealth, heritage, or previous academic experience. The process of making higher education available to the maximum number of people continues to evolve” (www.aacc.nche.edu).

The community college environment is uniquely positioned, resulting from the threefold mission of these institutions to provide a learning environment for:

- transfer into baccalaureate programs;
- entrance into the local workforce; and
- lifelong learning for personal and professional enrichment.

In addition, many two-year colleges are drivers of local economic development, providing workforce development and skills training, as well as offering noncredit programs ranging from English as a second language to skills retraining to community enrichment programs and cultural activities.

Two-year colleges serve high school graduates proceeding directly into college, workers needing to upgrade skill sets or master new ones in order to re-enter the workforce, immigrants seeking to become integrated into the local culture and master a new language, individuals leaving the workplace to engage college-level coursework for the first time, returning students with college degrees who have decided to pursue an alternate career path, and many individuals in need of ongoing training and skill updating. This diversity is addressed in numerous ways, including targeted career counseling, remediation of basic skills, specialized course offerings, individualized instruction and attention, flexible scheduling and delivery methodologies, and a strong emphasis on retention and successful completion. Furthermore, because two-year colleges have less restrictive entrance requirements, faculty must be prepared to instruct students exhibiting a broad range of academic preparations, aptitudes, and learning styles. The mission of two-year college faculty is to focus their full-time attention on effective pedagogy for educating a diverse student population, as well as remaining current in their discipline and in the scholarship of teaching and learning, and fostering student success.

Two-year, community or technical colleges, as well as certain four-year colleges, award associate degrees to students completing between 60 to 66 higher education semester credits in a specific program of study. It is often the case that an associate-degree requires approximately half the college credit of a bachelor’s degree. Associate-degree programs are complete, whether designed specifically to enable graduates to transfer into the upper division of a baccalaureate program or to gain entry into the workforce. Additionally, these institutions also offer certificate programs, intended to be fulfilled in less time than a complete degree
program; such programs are often designed for targeted student audiences and focused on specific content.

At the earliest opportunity, faculty and academic advisors must help each student determine which type of program best serves the student’s educational and career goals. Such considerations include the distinctions between certificate, career and transfer programs, the academic requirements of each, and the associated employment options. Career-oriented associate-degree programs (typically A.A.S.) provide the specific knowledge, skills, and abilities necessary to proceed directly into the workplace, while transfer-oriented degree programs (typically A.S.) provide the academic foundation and pathway to continue a program of study at a four-year college or university.

**Career and Transfer Programs**

Typically, associate-degree computing programs fall into two categories: those designed to prepare graduates for immediate entry into career paths, usually an Associate of Applied Science (A.A.S), and those designed for transfer into baccalaureate-degree programs, usually an Associate of Science (A.S.) or Associate of Arts (A.A.) or in some cases with no degree awarded.

Colleges should make students aware at the onset of their studies of the distinctions between career and transfer programs, the academic requirements of each, and the resultant employment options.

Career-oriented associate-degree programs provide students with the specific knowledge, skills and abilities necessary to proceed directly into employment in a targeted work environment. The program of study may include professional development coursework as well as courses that emphasize communication skills, mathematical reasoning and other general education requirements. In addition, many students will augment their formal studies with technical industry certifications to enhance their immediate employability.

It is important to note that a career-oriented associate-degree program is not intended to facilitate transfer into a baccalaureate program, but rather to provide entry into a career that requires specialized post-secondary skills and an advanced level of expertise and education. Nevertheless, many students graduating from career-oriented programs subsequently elect to further their education at the baccalaureate level.

Articulation is a key consideration in associate-degree programs which are designed as transfer curricula. Articulation of courses and programs between academic institutions is a process that facilitates transfer by students from one institution to another. The goal is to enable students to transfer in as seamless a manner as possible. Efficient and effective articulation requires accurate assessment of courses and programs as well as meaningful communication and cooperation among institutions. Both students and faculty have responsibilities and obligations
for successful articulation. Ultimately, students are best served when educational institutions establish well defined articulation agreements that actively promote transfer.

Diversity in the Computing Profession

Across the globe there is a high demand for computing and cybersecurity professionals and a significant shortfall in job vacancies in many locations. The growth of new and emerging roles in computer, technology, and engineering fields exceeds the rate that underrepresented groups enter these fields. Academic research continues to bear light on the pressing need to increase the diversity of students pursuing computing degrees and the numerous benefits of doing so. To help fulfill the increasing shortage of computer professionals, computing faculty should increase efforts to effectively recruit and retain a wider range of students and build and provide effective support structures so that all students can successfully graduate.

Ethics and Professionalism

Ethical reasoning and professional conduct are important concepts in the overall curricula for computing disciplines, including cybersecurity, and must be integrated throughout the programs of study. This ethical and professional context should be established at the onset and should appear routinely in discussions and learning activities throughout the curriculum. Updated in 2018, the ACM Code of Ethics notes that “Computing professionals' actions change the world. To act responsibly, they should reflect upon the wider impacts of their work, consistently supporting the public good.” The Code goes on to provide an excellent framework for conduct that should be fostered beginning early in students’ experiences (www.acm.org/code-of-ethics).

As computing technologies become ubiquitous in society, ethical behavior and adherence to codes of conduct for computing professionals are imperative; therefore, careful consideration of legal, ethical, and societal issues involving computing, the Internet and databases are essential to the education of computing professionals. Students who realize the potential uses and abuses of technology will, as citizens, be able to contribute to public policy debate from a knowledgeable perspective on issues such as property rights and privacy concerns that affect everyone.

Computer systems have substantial social impact in nearly every setting including applications such as healthcare, finance, transportation, defense, government, education, and communications. Engaging students in the consideration of the ethical aspects involved in decisions about technology and computing systems enables them to make more judicious choices. It is crucial that students pursuing careers in cybersecurity or computing more generally be made aware of and properly equipped to handle the complexities of professional judgments - as computing professionals, graduates must follow codes of conduct and take responsibility for their actions and be accountable for the systems that they develop, support, and protect.
[In a future draft we will discuss the importance of ethics in cybersecurity more specifically, including reference to cybersecurity-related codes of ethics such as EC-Council’s Code of Ethics (https://www.eccouncil.org/code-of-ethics/)]

Mathematics Requirements

Mathematics provides a language for working with ideas relevant to computing, specific tools for analysis and verification, and a theoretical framework for understanding important concepts. For these reasons, mathematics content must be initiated early in the student’s academic career, reinforced frequently, and integrated into the student’s course of study. Curriculum content, pre- and co-requisite structures, and learning activities and laboratory assignments must be designed to reflect and support this framework. Many students enter two-year colleges with insufficient mathematics preparation for a computing program. Such students must devote additional semesters to achieve the mathematical maturity and problem-solving skills required to be successful in computing coursework.

A variety of mathematics courses and embedded content may be appropriate for undergraduate cybersecurity majors. This may include discrete mathematics, statistics, linear algebra, among others. Transfer programs may have more extensive mathematics requirements to align with 4-year partner programs. This curricular guidance does not include specific student learning outcomes for mathematics.

The Cybersecurity Discipline

Cybersecurity has only recently emerged as an identifiable discipline, and cybersecurity degree programs are still relatively young. CSEC2017 defines cybersecurity as: “A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management.”

In addition to being an important discipline in its own right, cybersecurity is becoming an increasingly important element of all computing programs. Curriculum content in creating and maintaining secure computing environments is a critical component in associate-degree computing programs. Almost every career path open to a computing student encompasses some aspect of security. System administrators and engineers must be able to properly design, configure, and maintain a secure system; programmers and application developers must know how to design and build secure, fault-tolerant software systems from the bottom up; web specialists must be capable of assessing risks and determining how best to reduce the potential impact of breached systems; user support technicians must be knowledgeable in security concerns surrounding desktop computing; and project managers must be able to calculate the cost/benefit tradeoffs involved with implementing secure systems.
It is the responsibility of faculty to ensure that students are well prepared for the cybersecurity challenges they will inevitably encounter in their careers as computing professionals. ACM CCECC curricular guidelines for associate-degree Computer Science and Information Technology programs have cybersecurity infused throughout the content.

Cybersecurity Curricular Framework

These guidelines for associate-degree cybersecurity programs maintain the high-level structure of the CSEC2017 curricular framework, including the division into eight knowledge areas, with each knowledge area having a number of knowledge units. Following is a table showing the eight knowledge areas and their definitions from CSEC2017, which applies in these guidelines as well:

<table>
<thead>
<tr>
<th>Knowledge Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>Focuses on the protection of data at rest, during processing, and in transit. This knowledge area requires the application of mathematical and analytical algorithms to fully implement.</td>
</tr>
<tr>
<td>Software Security</td>
<td>Focuses on the development and use of software that reliably preserves the security properties of the information and systems it protects.</td>
</tr>
<tr>
<td>Component Security</td>
<td>Focuses on the design, procurement, testing, analysis and maintenance of components integrated into larger systems.</td>
</tr>
<tr>
<td>Connection Security</td>
<td>Focuses on the security of the connections between components including both physical and logical connections.</td>
</tr>
<tr>
<td>System Security</td>
<td>Focuses on the security aspects of systems that are composed of components and connections, and use software.</td>
</tr>
<tr>
<td>Human Security</td>
<td>Focuses on protecting individuals' data and privacy in the context of organizations (i.e., as employees) and personal life, in addition to the study of human behavior as it relates to cybersecurity.</td>
</tr>
<tr>
<td>Organizational Security</td>
<td>Focuses on protecting organizations from cybersecurity threats and managing risk to support the successful accomplishment of the organization's mission.</td>
</tr>
<tr>
<td>Societal Security</td>
<td>Focuses on aspects of cybersecurity that broadly impact society as a whole for better or for worse</td>
</tr>
</tbody>
</table>

These associate-degree guidelines are divided into Essential and Supplemental portions. This recognizes the fact that there can be a variety of flavors of associate-degree cybersecurity programs. The content in Essential is content that may be expected to appear in any and every associate-degree cybersecurity program. The content in Supplemental is content that is likely to
appear in some flavor of associate-degree cybersecurity program, but would not be expected in all flavors of associate-degree cybersecurity program.

In this curricular framework the Essential content is presented first, organized by knowledge area and knowledge unit. The Supplemental content is presented next, also organized by knowledge area and knowledge unit.

The heart of the "content" is student learning outcomes, emphasizing what students can do over what students know. Learning outcomes are expressed using action verbs from Bloom’s Revised Taxonomy. The Bloom’s level - Remembering, Understanding, Applying, Analyzing, Evaluating, or Creating - is indicated in italics after each learning outcome.

Knowledge Areas

This section comprises the content of the curricular framework.

Essential

Data Security

Cryptography

- Analyze which cryptographic protocols, tools, and techniques are appropriate for providing confidentiality, data protection, data integrity, authentication, non-repudiation, and obfuscation. Analyzing
- Outline the differences between symmetric and asymmetric algorithms. Analyzing
- Examine hash functions for integrity checking and protecting authentication data. Analyzing
- Use historical ciphers, such as shift cipher, affine cipher, substitution cipher, Vigenere cipher, ROT-13, Hill cipher, Enigma machine, and others, to encrypt and decrypt data. Applying
- Deduce the strengths and weaknesses of historical ciphers. Analyzing

Digital Forensics

- Describe what a digital investigation is, the sources of digital evidence, and the limitations of forensics. Understanding
- Contrast a variety of forensics tools. Analyzing
- Discuss the concept and value of the digital forensics science. Understanding
- Demonstrate the benefits of digital forensic readiness and planning. Understanding
- Discuss key rules, laws, policies, and procedures that affect digital forensics. Understanding
- Examine legal issues, authorities, and processes related to digital evidence. Analyzing
Describe the forensic examiner ethical responsibilities. *Understanding*

Data Integrity and Authentication

- Contrast the concepts and techniques to achieve authentication, authorization, access control, and data integrity. *Analyzing*
- Summarize the benefits and challenges of multifactor (n-factor) authentication. *Understanding*
- Implement multifactor (n-factor) authentication using one or more of cryptographic tokens, cryptographic devices, biometric authentication, one-time passwords, knowledge-based authentication. *Applying*
- Describe different types of password attack techniques and the motivation behind them (Dictionary attack, Brute force attack, Rainbow table attack, Phishing and social engineering, Malware-based attack, Spidering, Off-line analysis, and Password cracking tools). *Understanding*
- Illustrate one or more password attack techniques. *Applying*
- Apply basic functions associated with password storage techniques, including cryptographic hash functions, salting, iteration count, and password-based key derivation. *Applying*

Access Control

- Demonstrate the applicability and value of physical data security controls, such as data center security, including keyed access, man trips, key cards and video surveillance, rack-level security, and data destruction. *Understanding*
- Implement data access control to manage identities, credentials, privileges, and related access. *Applying*
- Differentiate among the different types of identities and their associated access controls and services, such as AAA, federated identities, access control lists, group policies, and passwords. *Understanding*
- Investigate access control models, such as role-based, rule-based, and attribute-based. *Applying*
- Describe access control best practices, such as separation of duties, job rotation, and clean desk policy. *Understanding*

Secure Communication Protocols

- Explain the goals of end-to-end data security. *Understanding*
- Investigate key application and transport layer protocols, such as HTTP, HTTPS, SSH, and SSL/TLS. *Applying*
- Investigate key application and transport layer protocols, such as IPsec and VPN technologies. *Applying*
- Explain security threats and mitigations to data at the data link layer. *Understanding*
Cryptanalysis
- Contrast different well-known cryptanalysis attacks. *Analyzing*

Data Privacy
- Evaluate different ways to jeopardize privacy by using contemporary technology, including social media. *Evaluating*

Information Storage Security
- Discuss prevention techniques implemented on software level vs hardware level. *Understanding*
- Contrast techniques about data erasure and their limitations in implementation. *Analyzing*
- Implement a procedure that authenticates a user and records access. *Applying*
- Discuss a data security policy such as HIPAA for a given scenario. *Understanding*

Software Security

Fundamental Principles
- Apply fundamental design principles including least privilege, open design, and abstraction. *Applying*
- Apply the least privilege concept to system and application software. *Applying*
- Execute access decisions and permissions based on explicit need. *Applying*
- Diagram a simple and small application design. *Applying*
- Explain software security controls in an open design. *Understanding*
- Illustrate the levels of abstraction in software security to allow single layer modification. *Applying*
- Implement software as a collection of co-operating components. *Applying*

Design
- Explain the importance of security requirements in software design. *Understanding*
- Interpret fundamental security requirements in a software system. *Understanding*
- Examine the waterfall and agile development models' relationship to software security. *Analyzing*

Implementation
- Discuss significant implementation issues in a secure software life cycle. *Understanding*
- Implement input validation to prevent buffer overflow, integer range violations, and input type violations. *Applying*
- Apply restrictions to process privileges. *Applying*
• Use cryptographic randomness appropriately in a cryptography system. *Applying*
• Implement proper error handling and user notification. *Applying*
• Implement defensive programming techniques. *Applying*
• Describe methods of protecting code in various environments. *Understanding*

**Analysis and Testing**

• Explain the difference between static and dynamic software testing. *Understanding*
• Test modules as they are developed. *Evaluating*

**Deployment and Maintenance**

• Perform common software configuration and patching tasks. *Applying*
• Explain the requirements for secure software decommissioning and retiring. *Understanding*

**Documentation**

• Discuss the need for including security in all documentation. *Understanding*

**Ethics**

• Defend an ethical approach to software security, especially in development, testing and vulnerability disclosure. *Evaluating*
• Explain various ethical aspects in software development. *Understanding*

**Component Security**

**Component Design**

• Distinguish vulnerabilities of system components. *Analyzing*
• Describe the component lifecycle. *Understanding*
• Compare various secure component design principles. *Analyzing*

**Component Procurement**

• Discuss vulnerabilities, risks, and mitigations at various points in a component supply chain. *Understanding*
• Discuss security threats and risks to both hardware and software in component procurement, such as malware attached during manufacturing or transportation. *Understanding*

**Component Testing**

• Perform common component security testing. *Applying*
• Describe unit testing tools and techniques as distinguished from system-level testing in the context of Cybersecurity. Understanding

Component Reverse Engineering
• Describe common reverse engineering scenarios for components. Understanding

Connection Security

Physical Media
[Supplemental only]

Hardware and Physical Component Interfaces and Connectors
• Manipulate physical components and their interfaces, such as network cables, motherboards, memory, current CPU chips, and buses. Applying
• Explain various standards for connectors, such as RJ-11, RJ-45, ST, and SC. Understanding
• Explain why every physical interface has a corresponding software component to provide a corresponding software interface. Understanding

Distributed Systems Architecture
• Describe architectures for running processes in a distributed system and enabling communication between them. Understanding
• Summarize the evolution of the Internet as a distributed platform, including the role of the world-wide-web. Understanding
• Compare the OSI model and the TCP/IP model. Analyzing
• Categorize protocols, based on the layers of the OSI model. Analyzing
• Explain protocols used in the world-wide-web and the TCP/IP Internet protocol suite, including HTTPS, DNS, DHCP, ARP, etc. Understanding
• Distinguish cloud system implementations, such as Infrastructure as a service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS), and all of their relatives. Analyzing
• Perform an operating system installation in a Type 1 or Type 2 hypervisor environment. Applying
• Perform configuration tasks using a Type 1 or Type 2 hypervisor environment. Applying

Network Architecture
• Diagram common architecture models to describe simple, secure systems including components and interfaces while adhering to current standards, including properly configuring internetworking devices, such as routers and switches. Applying
• Distinguish the various topologies and their transmission characteristics. Analyzing
Illustrate the ideas of nodes, edges, and topologies using a network diagram. Applying

Explain types of virtualization including native virtualization (type 1) and hosted virtualization (type 2). Understanding

Network Implementations

- Differentiate between various connection attacks, such as SYN-scanning, and associated vulnerabilities. Understanding
- Differentiate between various transmission attacks, such as Ping of Death and Denial of Service, and associated vulnerabilities. Understanding

Network Services

- Describe the concept of an operating system service, and how a service could be vulnerable to exploitation. Understanding

Network Defense

- Explain how defenses must be layered to achieve maximum confidentiality, integrity, and availability (CIA). Understanding
- Describe how various connectivity devices interoperate in providing layered defenses. Understanding

System Security

System Thinking

- Explain a holistic approach to system security. Understanding
- Describe what a system is, including how components work together. Understanding
- Describe how system engineering is used to accomplish tasks. Understanding
- Discuss the components of a secure system. Understanding
- Discuss the components that secure special-purpose systems. Understanding
- Contrast various security threat models. Analyzing
- Explain fundamental principles of secure systems. Understanding

System Management

- Describe the components of a security policy for a system. Understanding
- Contrast various system monitoring tools and mechanisms. Analyzing
- Evaluate various system recovery methods. Evaluating
- Describe the importance of patching systems and describe how patching can protect systems against attacks at various steps in the vulnerability life cycle. Understanding
- Illustrate how different management components protect the operating system from attack. Applying
• Outline procedures for maintaining business continuity in the face of a system attack.  
  Analyzing

System Access
• Contrast various authentication methods. Analyzing
• Categorize different access control systems. Analyzing
• Explain various authentication methods and how they protect the operating system from attack. Understanding
• Describe different ways to verify a user's identity. Understanding

System Control
• Use documentation to securely operate a system. Applying
• Develop documentation for a system with security considerations in mind. Creating
• Differentiate among types of malware. Understanding

System Testing
• Execute common testing protocols. Applying
• Discuss the differences between unit testing and system testing. Understanding

Common System Architectures
• Discuss system security issues related to common system architectures including virtual machines, industrial control systems, embedded systems, autonomous systems, mobile systems and general-purpose systems. Understanding

Human Security

Identity Management
• Compare various methods of identity management, identification, authentication, and access authorization, such as roles, biometrics, and multi-method systems. Analyzing

Social Engineering
• Compare various social engineering risks and suitable mitigations. Analyzing
• Distinguish various types of social engineering attacks, including phishing, vishing, email compromise, and baiting. Analyzing

Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms
• Investigate privacy theories from social psychology and social science, including tradeoffs and risks. Applying
• Debate social media privacy and security. Evaluating
Awareness and Understanding

- Carry out security education, training, and awareness program tasks. Applying
- Appraise individual responsibilities related to cyber hygiene, such as password creation, maintenance, and storage; mitigation tools; identification and use of safe websites; and identifying and using appropriate privacy settings. Evaluating

Personal Data Privacy and Security

- Evaluate personal data privacy and security for a given scenario. Evaluating

Usable Security and Privacy

- Describe the impact usability and user experience have on security and privacy. Understanding
- Describe human factors which impact privacy and security, such as the psychology of adversarial thinking when developing security policies, resistance to biometric authentication, and the economics of security. Understanding

Organizational Security

Risk Management

- Classify various organizational risk factors. Understanding

Security Governance & Policy

- Implement information security governance and policy. Applying
- Summarize significant national and international laws that relate to cybersecurity. Understanding
- Discuss the importance of ethical codes of conduct for cybersecurity professionals and their organizations. Understanding

Analytical Tools

[Supplemental only]

Systems Administration

- Describe security components that are integrated into the operating system administration functions. Understanding
- Describe components that secure the system database from vulnerabilities. Understanding
- Demonstrate the use of group membership to assign permissions. Understanding
Discuss the security features that are embedded within the cloud environment.

*Understanding*

Cybersecurity Planning

* Describe the use of Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis in an organization. *Understanding*

Business Continuity, Disaster Recovery, and Incident Management

* Summarize incident response steps to be taken to ensure the chain of evidence is preserved. *Understanding*
* Describe a disaster recovery plan that ensures minimal down time and quick recovery. *Understanding*
* Explain components of a business continuity plan, such as contingency planning, incident response, emergency response, backup and recovery efforts. *Understanding*

Security Program Management

[Supplemental only]

Personnel Security

[Supplemental only]

Societal Security

Cybercrime

* Categorize different type of cybercrime. *Analyzing*
* Investigate the economic implications of a society influenced by cybercrimes, including crimes that involve cryptocurrencies. *Applying*

Cyber Law

* Interpret relevant cyber laws, including computer hacking laws. *Understanding*
* Explain how to preserve the chain of custody for digital evidence. *Understanding*
* Explain how digital contracts are used in cyber law. *Understanding*

Cyber Ethics

* Analyze various cyber ethics scenarios, including topics on codes of conduct and professional ethics. *Analyzing*
* Distinguish among ethical hacking, nuisance hacking, activist hacking, criminal hacking, and acts of war. *Analyzing*
Cyber Policy
- Discuss various cyber policy issues. *Understanding*

Privacy
- Contrast privacy and transparency, including goals and tradeoffs. *Analyzing*
- Investigate cultural differences in the existence of privacy norms and boundaries. *Applying*

Supplemental

Data Security

Cryptography
- Compare the benefits and drawbacks of applying cryptography in hardware vs software. *Analyzing*
- Demonstrate the importance of mathematical theory in the application of cryptography. *Understanding*
- Apply symmetric cryptography, such as DES, Twofish, AES, in a given scenario. *Applying*
- Explain the evolution from DES to 3DES to AES. *Understanding*
- Deduce minimum key strength for symmetric algorithms to be effective. *Analyzing*
- Apply asymmetric cryptography, such as Diffie-Hellman, RSA, ECC, ElGamal, and DSA. *Applying*
- Contrast trust models in PKI, such as hierarchical, distributed, bridge, web of trust. *Analyzing*
- Explain how symmetric and asymmetric encryption are used in tandem to secure electronic communications and transactions. *Understanding*

Digital Forensics
- Outline a variety of digital forensic tools (open source vs. closed source) and their limits. *Analyzing*
- Use common digital forensics tools, such as EnCase, FTK, ProDiscover, Xways, SleuthKit. *Applying*
- Describe digital forensics investigative procedures, such as identification of evidence, collection and preservation of evidence, timelines, reporting, chain of custody, and authentication of evidence. *Understanding*
- Summarize the relationship between digital forensics and traditional techniques in responding to events of interest including incidents and breaches. *Understanding*
- Carry out forensically sound acquiring and handling of digital evidence following chain of custody best practices. \textit{Applying}
- Perform acquisition of digital evidence from non-PC devices, such as smart phones, tablets, GPS, games consoles, Smart TVs, and IoT devices. \textit{Applying}
- Analyze key computer operating systems files and artifacts, including computer memory forensics acquisition and analysis. \textit{Analyzing}
- Analyze digital evidence from non-PC devices, such as smart phones, tablets, GPS, games consoles, Smart TVs, and IoT devices. \textit{Analyzing}
- Apply documentation techniques and reporting of findings using industry standard and technically accurate terminology and format. \textit{Applying}
- Outline complex technical concepts and processes so that they are easily understood by non-technical audiences. \textit{Analyzing}
- Carry out verification and validation of evidence during forensic acquisition, preservation, and analysis, including the use of hashes. \textit{Applying}
- Perform fundamental incident response functions including detecting, reporting, responding, and handling of security incidents. \textit{Applying}
- Carry out containment, eradication, and recovery, and post-incident activities. \textit{Applying}
- Summarize the best practices in collecting and isolating mobile devices when part of digital evidence. \textit{Understanding}
- Summarize key features of mobile operating systems (OS) and applications. \textit{Understanding}
- Describe key mobile artifacts. \textit{Understanding}

\textbf{Data Integrity and Authentication}

- Illustrate the use of cryptography to provide data integrity, such as message authentication codes, digital signatures, authenticated encryption, and hash trees. \textit{Applying}

\textbf{Access Control}

- Illustrate the fundamental value and benefits of security architectures used to protect information in computer systems. \textit{Applying}

\textbf{Secure Communication Protocols}

- Illustrate attacks and countermeasures on TLS, such as downgrade attacks, certificate forgery, implications of stolen root certificates, and certificate transparency. \textit{Applying}
- Investigate privacy preserving protocols, such as Mixnet, Tor, Off-the-record message, and Signal. \textit{Applying}

\textbf{Cryptanalysis}

- Demonstrate timing attacks and their effects on well-known algorithms such as RSA, ElGamal, and the Digital Signature Algorithm. \textit{Understanding}
Describe how meet-in-the-middle attacks affect the privacy aspect of data.

Understanding

Categorize in terms of complexity different techniques for attacks against public key ciphers, such as Pollard's p-1 and rho methods, quadratic sieve, and number field sieve.

Analyzing

Data Privacy

[Essential only]

Information Storage Security

[Essential only]

Software Security

Fundamental Principles

- Manipulate object access to validate accessibility. Applying
- Develop software that disseminates the tasks and associated privileges for a specific security process among multiple modules. Applying
- Perform input validation and action verification. Applying
- Illustrate isolation through a virtual machine or sandbox. Applying
- Execute software in a logical and simple approach. Applying
- Execute a software test that grants access to one layer at a time, reduces access points, and uses either a top-down or bottom-up approach. Applying
- Write software specifications that connect design and implementation to security specifications. Applying
- Diagram a software design that is adjustable to environmental changes. Applying

Design

- Explain the relationship between software security requirements and a business’ mission. Understanding
- Translate software security requirements into written formal, informal, and testing specifications. Understanding
- Explain what it means for a programming language to be type-safe. Understanding

Implementation

- Use an API to detect errors and implement security policy. Applying
- Implement process and resource checking. Applying
- Implement process isolation. Applying
Analysis and Testing

- Distinguish different methods of static and dynamic analysis. **Analyzing**
- Test software components as they are integrated. **Evaluating**
- Test software as a whole while incorporating unit testing and software testing. **Evaluating**

Deployment and Maintenance

- Modify a software system to compensate for assumptions that do not match the deployment environment. **Applying**
- Summarize software development and operations. **Understanding**

Documentation

- Write documentation for software installation and configuration. **Applying**
- Write user documentation emphasizing user security dangers. **Applying**

Ethics

- Describe social aspects related to software development. **Understanding**
- Summarize legal aspects and regulations regarding software development. **Understanding**

Component Security

Component Design

[Essential only]

Component Procurement

[Essential only]

Component Testing

- Use tools and techniques, such as fuzz testing, for testing the security properties of a component beyond its functional correctness. **Applying**

Component Reverse Engineering

[Essential only]
Connection Security

Physical Media
- Diagram transmission flow in a medium. *Applying*
- Contrast the communications characteristics of shared and point-to-point media. *Analyzing*
- Explain various schemes for sharing media between multiple clients, including PPP and CSMA/CD. *Understanding*
- Examine characteristics of common networking standards including frame structure, including IEEE 802.3 and 802.11. *Analyzing*

Physical Interfaces and Connectors
*Essential only*

Hardware Architecture
*Essential only*

Distributed Systems Architecture
- Describe use cases for high performance computing (HPC). *Understanding*
- Discuss vulnerabilities and example exploits as they apply to interfaces used in hypervisors, virtual networking, physical networking, and interprocess communication. *Understanding*

Network Architecture
- Compare the various IEEE 802 network architecture implementations. *Analyzing*
- Distinguish various networks based on their physical characteristics (LANs, MANs, etc.). *Analyzing*
- Explain packet forwarding in general and in the context of Software-Defined Networking. *Understanding*
- Examine routing algorithms, such as link-state and distance vector, and how they populate forwarding tables. *Analyzing*
- Discuss emerging technologies and their impact as they emerge, such as Software-Defined Networking, the Internet of Things, and adding routing to layer 2 with enhanced learning bridges. *Understanding*

Network Implementations
- Analyze the various fields available in Internet Protocol packets at various layers of the Open Systems Interconnection (OSI) and TCP/IP models. *Analyzing*
- Demonstrate examples of network vulnerabilities, such as ARP poisoning as a MitM attack. *Understanding*
• Discuss examples of physical security vulnerabilities, including Universal Serial Bus (USB) and other serial connections. Understanding

Network Services
• Differentiate network service models, including client-server and peer-to-peer. Understanding
• Describe methods by which components connect, including procedure calls, IPC requests, Interface Definition Languages with stub code, and private protocols over a socket. Understanding
• Explain specific services and how their protocols are implemented, including SMTP, HTTP, SNMP, REST, CORBA, and Application layer protocols for specialty devices. Understanding
• Describe service virtualization as a method to emulate the behavior of specific components, such as cloud-based applications and service-oriented architecture. Understanding
• Demonstrate examples of network vulnerabilities of client-server, peer-to-peer, and virtualization network services, such as common service signatures. Understanding

Network Defense
• Implement configuration settings on devices throughout an enterprise to harden the network against attackers. Applying
• Demonstrate how intrusion detection and intrusion prevention services can be used to protect a network and audit network traffic. Understanding
• Discuss appropriate uses of host-, server-, and internetworking device-based firewalls. Understanding
• Implement a simple virtual private network. Applying
• Describe the purpose and function of honeypots and honeynets within an overall network defense strategy. Understanding
• Operate commonly used monitoring network tools and devices. Applying
• Analyze logs associated with commonly used monitoring network tools and devices. Analyzing
• Manipulate a commonly used network protocol analyzer to capture and analyze packets flowing through the network. Applying
• Discuss threat hunting, attack pattern detection, and similar network traffic analysis techniques. Understanding
• Use tools and techniques for finding and mitigating vulnerabilities through looking at potential weaknesses. Applying
• Discuss tools and techniques for limiting the flow of packets based upon rules for packet content, including network admission control techniques; machine certificates; machine profiling techniques; and probing with SNMP, DHCP, HTTP, DNS, LDAP, and NMAP. Understanding

24
Diagram a Demilitarized Zone (DMZ) and its components, including isolated networks and special servers, such as proxy servers, mail servers, and web servers. **Applying**

Write a security policy that provides guidance and requirements for the services provided by the network along with the measures to be used to see that the policies are followed. **Applying**

Develop procedures that are used to operate the network in light of applicable security policies and business requirements. **Creating**

Use tools and techniques to test the network by actually attempting to exploit vulnerabilities. **Applying**

Discuss the role of machine learning to detect patterns in attack vectors, such as in proactive threat hunting. **Understanding**

**System Security**

**System Thinking**

- Justify security requirements throughout the system development lifecycle. **Evaluating**
- Critique plans for testing secure systems in a given scenario. **Evaluating**

**System Management**

- Carry out elements of an automation plan, such as data mining, machine learning, and related techniques. **Applying**
- Examine reasons for commissioning, decommissioning, and disposing of a system under attack. **Analyzing**
- Defend a system against an insider threat. **Evaluating**
- Describe a process to document baseline system functions. **Understanding**

**System Access**

- Analyze the strengths and weaknesses of various access control models and mechanisms. **Analyzing**

**System Control**

- Investigate models for managing authorization across systems. **Applying**
- Contrast authentication and authorization. **Analyzing**
- Describe how malicious activity can be detected, including the use of intrusion detection systems. **Understanding**
- Describe potential system attacks and the actors that might perform them. **Understanding**
- Apply cyber defense methods to prepare a system to repel attacks. **Applying**
- Analyze logs to detect intruders. **Analyzing**
- Carry out a penetration test on a system. **Applying**
• Analyze system requirements for performing forensic analysis. *Analyzing*
• Investigate legal ramifications that affect day-to-day network administration, such as litigation holds. *Applying*
• Discuss recovery and resilience mechanisms that help ensure system availability. *Understanding*

System Testing
• Examine system requirements to determine whether they meet system objectives. *Analyzing*

Common System Architectures
• Construct virtual environments including disk and memory structures. *Creating*
• Describe the components of a SCADA industrial control system. *Understanding*
• Diagram an Internet of Things system. *Applying*

Human Security

Identity Management
• Examine various physical assets access controls, such as Network Access Control (NAC), Identity Access Management (IAM), Rules-based Access Control (RAC), and Roles-based Access Control (RBAC). *Analyzing*
• Explain the benefits and challenges of identity management as a service (IaaS). *Understanding*
• Categorize types of data and user credential access control attacks and mitigations, such as brute force attacks, spoofing attacks, strong password policies, and restricted access systems. *Analyzing*

Social Engineering
• Describe psychological and behavioral factors which contribute to social engineering attacks, such as adversarial thinking, cognitive biases, and trust building. *Understanding*
• Describe ways in which message systems, browser interfaces, and user interaction can be exploited to mislead users. *Understanding*
• Use various tools and approaches to detect and/or mitigate different social engineering threats, such as using email filtering, blacklists, instruction detection systems and intrusion prevention systems (IDS/IPS). *Applying*

Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms
• Summarize various ways in which systems are misused and users misbehave to cause intentional and unintentional threats and attacks, such as unintentional system misuse, naïve behavior, and cyber bullying. *Understanding*
• Debate methods and techniques to persuade individuals to follow rules, policies, and ethical norms related to cybersecurity. *Evaluating*

• Summarize methods and techniques to employ when an individual is uncertain how to respond to a given cybersecurity situation. *Understanding*

**Awareness and Understanding**

• Compare various mental models and their impact on how users perceive, judge, communicate, and respond to cybersecurity risks. *Analyzing*

• Evaluate a Security Education, Training, and Awareness (SETA) program. *Evaluating*

• Describe ways to improve cybersecurity vulnerabilities and threats awareness, such as warning signs of internal employee vulnerabilities and threats, awareness of identity theft, email compromise, and free/open Wi-Fi networks. *Understanding*

**Personal Data Privacy and Security**

• Examine various types of sensitive personal data (SPD) and associated risks and impact of misuse. *Analyzing*

• Evaluate how personal tracking techniques and an individual’s digital footprint impact privacy and security. *Evaluating*

**Usable Security and Privacy**

• Compare various types of security and privacy policies, such as HIPAA, FERPA, and PII, along with techniques for user education. *Analyzing*

• Describe the benefits and challenges of following cybersecurity design guidelines, such as providing secure defaults, and reducing unintentional security and privacy errors. *Understanding*

**Organizational Security**

**Risk Management**

• Distinguish information assets in an organization and threats to those assets. *Analyzing*

• Analyze risks in an organization including the potential for both accidental and intentional losses. *Analyzing*

• Describe the risk of insider threat in an organization, including motive-means-opportunity behaviors. *Understanding*

• Apply a risk management model to measure, evaluate, and communicate risk to stakeholders. *Applying*

• Outline risk control in an organization using the categories of Avoid, Reduce, Transfer, and Accept. *Analyzing*
Security Governance & Policy
[Essential only]

Analytical Tools
- Use tools to collect and analyze data to generate security intelligence including threats and adversary capabilities. Applying

Systems Administration
- Design administrative procedures for protecting the physical system from attack. Creating
- Implement hardening techniques to protect the operating system. Applying
- Describe processes that ensure availability of system access and functions. Understanding

Cybersecurity Planning
[Essential only]

Business Continuity, Disaster Recovery, and Incident Management
[Essential only]

Security Program Management
- Perform project management tasks that provide for security of data. Applying
- Analyze the meaning and use of various security metrics used in protecting the network. Analyzing
- Describe the use of quality assurance and quality control to prevent mistakes and increase the quality of a system. Understanding

Personnel Security
- Describe the proper use or avoidance of fear, uncertainty, and doubt (FUD) as an awareness tool in various contexts, such as physical security, password security, and social engineering. Understanding
- Classify components of third party security services. Understanding
- Discuss components that ensure the protection of personally identifiable information. Understanding
Societal Security

Cybercrime
- Categorize challenges associated with the enforcement and prosecution of cybercrime. Analyzing

Cyber Law
- Investigate legislative and executive powers relevant to cyber law, along with those addressed in constitutional amendments. Applying
- Examine the core doctrines of intellectual property in cyber law. Analyzing
- Describe privacy law into contemporary dilemmas involving social media, electronic surveillance, and Internet privacy. Understanding
- Explain a data security law that has been discussed on recent event. Understanding
- Apply case law and common law to current legal dilemmas in the computer hacking. Applying

Cyber Ethics
- Compare ethical practices and legal codes. Analyzing
- Discuss ethical issues related to nation-state conflicts, including cyber espionage and Just War Theory. Understanding

Cyber Policy
- Examine the cost of cybersecurity to a nation. Analyzing

Privacy
- Debate human right to privacy contrasting the need of transparency. Evaluating
- Explain conditions for ethical and lawful use of privacy enhancing technology. Understanding
- Analyze potential solutions that address circumstances when data privacy is compromised. Analyzing