Cybersecurity Curricular Guidance for Associate-Degree Programs

IronDog DRAFT

5 July 2019
Available for public review and comment

Association for Computing Machinery (ACM)
Committee for Computing Education in Community Colleges (CCECC)

Copyright © 2019 by ACM CCECC. All rights reserved.
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

CSEC2Y Task Group  

Table of Contents  

Introduction  

- Overview of the Curricular Development Process  
- How to Use These Guidelines  
  - Conducting program reviews to update and create curriculum  
  - Facilitating program and course articulation  
  - Complying with government-sponsored frameworks  
  - Interacting with local advisory boards  

Two-Year/Community College Environment  

Career and Transfer Programs  

Diversity in the Computing Profession  

Ethics and Professionalism  

Mathematics Requirements  

The Cybersecurity Discipline  

Acknowledgements  

Cybersecurity Curricular Framework  

<p>| Essential | 16 |
| Cross-Cutting Competencies | 16 |
| Data Security | 16 |
| Cryptography | 17 |
| Digital Forensics | 17 |
| Data Integrity and Authentication | 17 |
| Access Control | 18 |
| Secure Communication Protocols | 18 |
| Cryptanalysis | 18 |
| Data Privacy | 18 |
| Information Storage Security | 18 |
| Software Security | 19 |
| Fundamental Principles | 19 |
| Design | 19 |
| Implementation | 19 |
| Analysis and Testing | 20 |
| Deployment and Maintenance | 20 |
| Documentation | 20 |</p>
<table>
<thead>
<tr>
<th>Component</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethics</td>
<td>20</td>
</tr>
<tr>
<td>Component Security</td>
<td>20</td>
</tr>
<tr>
<td>Component Design</td>
<td>20</td>
</tr>
<tr>
<td>Component Procurement</td>
<td>21</td>
</tr>
<tr>
<td>Component Testing</td>
<td>21</td>
</tr>
<tr>
<td>Component Reverse Engineering</td>
<td>21</td>
</tr>
<tr>
<td>Connection Security</td>
<td>21</td>
</tr>
<tr>
<td>Physical Media</td>
<td>21</td>
</tr>
<tr>
<td>Hardware and Physical Component Interfaces and Connectors</td>
<td>21</td>
</tr>
<tr>
<td>Distributed Systems Architecture</td>
<td>22</td>
</tr>
<tr>
<td>Network Architecture</td>
<td>22</td>
</tr>
<tr>
<td>Network Implementations</td>
<td>22</td>
</tr>
<tr>
<td>Network Services</td>
<td>22</td>
</tr>
<tr>
<td>Network Defense</td>
<td>22</td>
</tr>
<tr>
<td>System Security</td>
<td>23</td>
</tr>
<tr>
<td>System Thinking</td>
<td>23</td>
</tr>
<tr>
<td>System Management</td>
<td>23</td>
</tr>
<tr>
<td>System Access</td>
<td>24</td>
</tr>
<tr>
<td>System Control</td>
<td>24</td>
</tr>
<tr>
<td>System Testing</td>
<td>24</td>
</tr>
<tr>
<td>Common System Architectures</td>
<td>24</td>
</tr>
<tr>
<td>Human Security</td>
<td>24</td>
</tr>
<tr>
<td>Identity Management</td>
<td>24</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>25</td>
</tr>
<tr>
<td>Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms</td>
<td>25</td>
</tr>
<tr>
<td>Awareness and Understanding</td>
<td>25</td>
</tr>
<tr>
<td>Personal Data Privacy and Security</td>
<td>25</td>
</tr>
<tr>
<td>Usable Security and Privacy</td>
<td>25</td>
</tr>
<tr>
<td>Organizational Security</td>
<td>25</td>
</tr>
<tr>
<td>Risk Management</td>
<td>26</td>
</tr>
<tr>
<td>Security Governance &amp; Policy</td>
<td>26</td>
</tr>
<tr>
<td>Analytical Tools</td>
<td>26</td>
</tr>
<tr>
<td>Systems Administration</td>
<td>26</td>
</tr>
<tr>
<td>Cybersecurity Planning</td>
<td>26</td>
</tr>
<tr>
<td>Business Continuity, Disaster Recovery, and Incident Management</td>
<td>26</td>
</tr>
<tr>
<td>Security Program Management</td>
<td>27</td>
</tr>
<tr>
<td>Personnel Security</td>
<td>27</td>
</tr>
<tr>
<td>Societal Security</td>
<td>27</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>27</td>
</tr>
</tbody>
</table>
Cyber Law 27
Cyber Ethics 27
Cyber Policy 28
Privacy 28
Supplemental 28
Data Security 28
Cryptography 28
Digital Forensics 29
Data Integrity and Authentication 29
Access Control 29
Secure Communication Protocols 30
Cryptanalysis 30
Data Privacy 30
Information Storage Security 30
Software Security 30
Fundamental Principles 31
Design 31
Implementation 31
Analysis and Testing 31
Deployment and Maintenance 31
Documentation 31
Ethics 31
Component Security 31
Component Design 32
Component Procurement 32
Component Testing 32
Component Reverse Engineering 32
Connection Security 32
Physical Media 32
Physical Interfaces and Connectors 33
Hardware Architecture 33
Distributed Systems Architecture 33
Network Architecture 33
Network Implementations 33
Network Services 34
Network Defense 34
System Security 35
System Thinking 35
System Management 35
System Access 36
System Control 36
System Testing 36
Common System Architectures 36

Human Security 36
Identity Management 37
Social Engineering 37
Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms 37
Awareness and Understanding 37
Personal Data Privacy and Security 37
Usable Security and Privacy 37

Organizational Security 38
Risk Management 38
Security Governance & Policy 38
Analytical Tools 38
Systems Administration 38
Cybersecurity Planning 39
Business Continuity, Disaster Recovery, and Incident Management 39
Security Program Management 39
Personnel Security 39

Societal Security 39
Cybercrime 40
Cyber Law 40
Cyber Ethics 40
Cyber Policy 40
Privacy 40

References 41

Appendix A: Competencies 43
Cross-Cutting Competencies 43
Data Security Competencies 44
Software Security Competencies 45
Component Security Competencies 46
Connection Security Competencies 47
System Security Competencies 48
Human Security Competencies 49
Organizational Security Competencies 50
Societal Security Competencies 51
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 [10], referred to as CSEC2017 (cybered.acm.org). The ACM Committee for Computing Education in Community Colleges (CCECC) formed a task force in early 2018 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 [12] (requirements of the NSA and DHS National Centers of Academic Excellence in Cyber Defense) and the NICE Cybersecurity Workforce Framework [11].

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 United States. The task force has been meeting online since April 2018, with one in-person meeting during 3CS in August 2018. In addition to the focused work and contributions of these ten educators, input into the first draft, known as StrawDog, was incorporated from breakout groups at a pre-NICE event in November 2018. The StrawDog draft was released in February 2019, and presented publicly to the community for review and comment during the period February 25 - April 17, 2019. This period began with a special session presentation and discussion at the SIGCSE Symposium 2019, and included dissemination through a variety of venues, newsletters, and mailing lists. Feedback was collected via notes during feedback sessions, emails received, as well as through a survey. Those providing input represent both 2-year and 4-year educators as well as industry professionals.

The feedback on the StrawDog draft has been reviewed by the task group and was very valuable in informing the current draft, known as IronDog. In response to this feedback, the committee crafted competencies for each knowledge area, bringing together the knowledge, skills, and dispositions expected of students in the cybersecurity context [7]. These competencies have been mapped to categories in the NICE Cybersecurity Workforce Framework. With the IronDog draft, we again present the curriculum document to the community for public review and comment, and look forward to any additional feedback that will help further improve the guidance and make it as useful as possible. After IronDog closes for public comment, the task force will work to incorporate the final feedback appropriately, with the final guidelines expected in late 2019 or early 2020.
How to Use These Guidelines

The competencies and learning outcomes itemized in the Cybersecurity Curricular Framework section of this document can be used but are not limited to the following.

Conducting program reviews to update and create curriculum

For example, the cybersecurity learning outcomes can be used by colleges to conduct periodic program reviews with the intent of validating existing cybersecurity courses, certificates, and degrees, as well as to create new cybersecurity curriculum. A collection of exemplars correlated to the cybersecurity learning outcomes makes it easy for colleges to compare and develop new courses, certificates and degree programs in cybersecurity. Actual course and program examples from across the nation will be collected and be available at ccecc.acm.org/guidance/cybersecurity. If you are interested in submitting a program example, contact the CCECC at ccecc.acm.org/contact.

Facilitating program and course articulation

Two-year cybersecurity programs may utilize these guidelines in articulation conversations with four-year transfer partners whose programs use CSEC2017. For example, the cybersecurity competencies and learning outcomes are being used by ABET to develop criteria for two-year cybersecurity programs. ABET’s program-specific criteria for cybersecurity at the baccalaureate level (four-year programs) were guided by CSEC2017 [1]. Once the two-year criteria are completed, the CCECC will map those criteria to the CSEC2Y competencies and learning outcomes at which time you can view the ABET mapping and others at ccecc.acm.org/guidance/cybersecurity.

Complying with government-sponsored frameworks

For example, the ACM CCECC cybersecurity competencies map to the NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [10] and the learning outcomes map to the Centers of Academic Excellence – Cyber Defense (CAE-CD) Two-Year Knowledge Units [12]. Mappings will also be established between the cybersecurity competencies and the U.S. Department of Labor Cybersecurity Industry Model. The mappings will be available at ccecc.acm.org/guidance/cybersecurity.

Interacting with local advisory boards

For example, cybersecurity program advisory boards may review the CSEC2Y competencies and learning outcomes and compare with local needs and a given local two-year college’s cybersecurity courses, certificates, and degrees with the specific intent of strengthening the local program of study.
Two-Year/Community College Environment

According to the American Association of Community Colleges, over 40% of all undergraduates in the United States are enrolled in two-year colleges, and more than half of undergraduates from some demographic groups attend community and technical colleges [1]. “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...” [3].

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 and 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 computing, 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” [3]. 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.

Cybersecurity in particular is a discipline in which ethics play a critical role, and ethics should be incorporated throughout a cybersecurity curriculum. Cybersecurity codes of ethics offer dictates such as “Promote generally accepted information security current best practices and standards” found in the ISSA (Information Systems Security Association) Code of Ethics [9] and “Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks” found in the EC-Council Code of Ethics [7].

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 and logic courses and embedded content may be appropriate for undergraduate cybersecurity majors. This may include discrete mathematics, statistics, and 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, but supports the inclusion of sufficient mathematics to meet the cybersecurity outcomes for a given program.

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 [5] and Information Technology [6] programs have cybersecurity infused throughout the content.

Acknowledgements

The task force would like to thank the following reviewers for their valuable feedback on the StrawDog draft:

Daniel Sehnal, Rappahannock Community College (RCC), Glenns Campus, Saluda, VA
Alvin Brewer, Lord Fairfax Community College, VA
Henry Coffman, Lord Fairfax Community College, Middletown VA
Crystal Dye, Southwest Virginia Community College, Richlands, VA
John Impagliazzo, Hofstra University, Hempstead, NY
Michael McKeever, Santa Rosa Junior College, Petaluma, CA
Margaret, Montgomery College, Montgomery College
Trang D. Nguyen, Prince George's Community College, Largo, MD
Tony Vargas, El Paso Community College, El Paso, TX
Virginia Carneiro de Paula, Ph.D., Palm Beach State College, Lake Worth, FL
Jacob Miller, Pennsylvania College of Technology, Williamsport, PA
James Walden, Northern Kentucky University, Highland Heights, KY
Tim Preuss, Minnesota State Community and Technical College, Moorhead, MN
John Cook, Herkimer College, Herkimer, NY
Sepi Hejazi Moghadam, Google, CA
Suvineetha Herath, Carl Sandburg College, Galesburg, IL
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. The terms “domain” and “subdomain” would be preferred to “knowledge area” and “knowledge unit” respectively since our focus is on competencies and outcomes, which go beyond knowledge to include skills and dispositions in context. To maintain consistency with CSEC2017 and allow easy comparison of sections of the curricular framework, the structure and terms used in organizing CSEC2017 are maintained in this document, though the content focuses on competencies and outcomes as discussed below.

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>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>Focuses on the protection of data at rest, during processing, and in transit.</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>

Several pervasive themes, referred to as cross-cutting concepts in CSEC2017, are woven throughout the knowledge areas, including
- **Confidentiality**, rules that limit access to system data and information to authorized persons;
- **Integrity**, assurance that the data and information are accurate and trustworthy;
- **Availability**, the data, information, and system are accessible;
- **Risk**, potential for gain or loss;
- **Adversarial thinking**, a thinking process that considers the potential actions of the opposing force working against the desired result; and
- **Systems thinking**, a thinking process that considers the interplay between social and technical constraints to enable assured operations.

These pervasive themes can be found in all eight knowledge areas. They help students explore connections among the knowledge areas and reinforce the security mindset conveyed throughout each knowledge area.

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 associate-degree cybersecurity program. The content in Supplemental is content that is likely to appear in some flavor of associate-degree cybersecurity program, but not in other flavors of associate-degree cybersecurity program.

The heart of this curricular framework is a small set of competencies for each knowledge area, along with a variety of student learning outcomes organized by knowledge unit within each knowledge area. The competencies follow the definition presented in *Modelling Competencies for Computing Education beyond 2020: A Research Based Approach to Defining Competencies in the Computing Disciplines* [8]: “Competency integrates knowledge, skills, and dispositions and is context-situated.” Knowledge (“know-that”) refers to “mastery of core concepts and content knowledge.” Skills (“know-how”) are “qualities that people develop and learn over time with practice and through interactions with others.” Dispositions (“know-why” and “know-yourself”) include “attitudinal, behavioral, and socio-emotional qualities of how disposed people are to apply knowledge and skills to solve problems.” Context is the setting in which competencies manifest, the “authentic situations related to problems/issues and aspects of work.”

The student learning outcomes represent more detailed outcomes than the competencies and may be seen as course or lesson learning outcomes. Learning outcomes emphasize what students *can do* over merely what students *know*. Both competencies and learning outcomes are expressed using action verbs from Bloom’s Revised Taxonomy. The Bloom’s level - Remembering, Understanding, Applying, Analyzing, Evaluating, or Creating - represents the depth of cognition for a given competency or learning outcome.

In this document the Essential content is presented first, with competencies representing the cross-cutting concepts that span knowledge areas at the beginning of the section, and the
remaining competencies and learning outcomes organized by knowledge area. The Supplemental content is presented next, organized in the same manner. The Bloom’s level of each competency and learning outcome is indicated after it in italics. In addition, one or more NICE Cybersecurity Workforce Framework [11] categories are indicated after each competency.

Essential

Cross-Cutting Competencies

Cross-Cutting Competencies

- Outline via appropriate methods, and using industry standard terminology, cybersecurity-related issues within an organization as they pertain to Confidentiality, Integrity, and Availability. Analyzing NICE Analyze, Operate and Maintain
- Assess and respond appropriately to various risks which can affect the expected operation of information systems. Evaluating NICE Protect and Defend
- Investigate current and emerging cyberthreats and incorporate best practices to mitigate them. Applying NICE Operate and Maintain, Collect and Operate
- Apply appropriate countermeasures to help protect organizational resources based on an understanding of how bad actors think and operate. Applying NICE Protect and Defend
- Discuss how changes in one part of a system may impact other parts of a cybersecurity ecosystem. Understanding NICE Protect and Defend

Data Security

Essential Data Security Competencies

- Carry out collection and acquisition of digital evidence in a forensically sound manner. Applying NICE Protect and Defend, Investigate
- Implement data security by selecting appropriate cryptographic procedures, algorithms, and tools based on security policy and level of risk in an organization. Applying NICE Protect and Defend, Operate and Maintain, Securely Provision
- Infer gaps in data security considering current and emerging technologies and the current state and prevailing trends in cybercrime. Understanding NICE Protect and Defend
- Perform actions to maintain data integrity for information systems and networks using appropriate levels of authentication, authorization, and access control. Applying NICE Operate and Maintain, Protect and Defend, Securely Provision
Essential Data Security Learning Outcomes

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**
- Perform fundamental incident response functions including detecting, reporting, responding, and handling of security incidents. **Applying**
- Carry out containment, eradication, and recovery, and post-incident activities. **Applying**
- 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, such as dictionary attacks, brute force attacks, rainbow table attacks, phishing and social engineering, malware-based attacks, 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

#### Essential Software Security Competencies

- Analyze the security of a software system and its related data and apply secure programming practices. **Analyzing NICE Securely Provision, Operate and Maintain**
- Demonstrate techniques of defensive programming and secure coding in a software system. **Understanding NICE Securely Provision, Operate and Maintain**
- Analyze the software development life cycle and explain and discuss how security can be incorporated into the software development life cycle. **Analyzing NICE Securely Provision**
- Use documentation or a knowledge base to resolve a security challenge in an identified computing scenario. **Applying NICE Protect and Defend**

#### Essential Software Security Learning Outcomes

### Fundamental Principles

- Apply fundamental design principles, including least privilege, open design, and abstraction, to system and application software. **Applying**
- Execute access decisions and permissions based on explicit need. **Applying**
- Diagram a simple secure application design. **Applying**
- Explain software security controls in an open design. **Understanding**
- Modify the levels of abstraction in a given piece of software to provide single layer abstraction. **Applying**
- Implement software as a collection of secure 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**
- Explain what it means for a programming language to be type-safe. **Understanding**

### Implementation

- Discuss significant implementation issues in a secure software life cycle. **Understanding**
• Write secure code to implement input validation and 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
• Develop a secure small application using defensive programming techniques. Creating
• Describe methods of protecting code in various environments. Understanding

Analysis and Testing
• Explain the difference between static and dynamic software testing. Understanding
• Test the security of a given piece of software, including granting access one layer at a time, reducing access points, using top-down or bottom-up approach. 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

<table>
<thead>
<tr>
<th>Essential Component Security Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Distinguish and mitigate vulnerabilities of system components throughout their lifecycle. Analyzing NICE Protect and Defend</td>
</tr>
<tr>
<td>• Analyze how security design impacts components throughout their lifecycle, especially related software and firmware updates. Analyzing NICE Protect and Defend</td>
</tr>
</tbody>
</table>

Essential Component Security Learning Outcomes

Component Design
• Distinguish different vulnerabilities which can apply to system components. Analyzing
- Describe the various phases of the component lifecycle. *Understanding*
- Compare various secure component design principles. *Analyzing*

**Component Procurement**
- Discuss vulnerabilities, risks, and mitigations for components of an organizational network at various points in a 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 for an organizational network. *Applying*
- Describe unit testing tools and techniques, as distinguished from those used in system-level testing. *Understanding*

**Component Reverse Engineering**
- Describe common reverse engineering scenarios for components of a system. *Understanding*

**Connection Security**

**Essential Connection Security Competencies**
- Construct and properly configure computer networks which adhere to current industry standards and organizational guidelines. *Creating NICE Operate and Maintain*
- Investigate the impact of various connection and transmission attacks on network hardware and software. *Applying NICE Protect and Defend, Analyze*

**Essential Connection Security Learning Outcomes**

**Physical Media**

[Supplemental only]

**Hardware and Physical Component Interfaces and Connectors**
- Manipulate physical components of an organizational network and their interfaces, such as network cables, motherboards, memory, current CPU chips, and buses. *Applying*
- Explain various standards for network connector hardware, such as RJ-11, RJ-45, ST, and SC. *Understanding*
- Install and configure device drivers for network components in an organization. *Applying*
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 commonly used network protocols based on the layers of the OSI model. **Analyzing**
- Explain common protocols used in the world-wide-web and the TCP/IP Internet protocol suite, including HTTPS, DNS, DHCP, ARP, etc. **Understanding**
- Distinguish various cloud system implementations, such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). **Analyzing**
- Perform an operating system installation for a virtual machine in a Type 1 or Type 2 hypervisor environment. **Applying**
- Perform configuration tasks in a Type 1 or Type 2 hypervisor environment. **Applying**

Network Architecture

- Diagram common architecture models to describe simple secure systems, including components and interfaces of internetworking devices, according to current standards. **Applying**
- Distinguish various network topologies and their transmission characteristics. **Analyzing**
- Illustrate the ideas of nodes, edges, and topologies using a network diagram. **Applying**
- Explain the characteristics of various 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, and how they can affect an organization’s network. **Understanding**
- Differentiate between various transmission attacks, such as Ping of Death and Denial of Service, and associated vulnerabilities, and how they can affect an organization’s network. **Understanding**

Network Services

- Describe the concept of an operating system service or daemon, and how it could be vulnerable to exploitation. **Understanding**

Network Defense

- Explain how network defenses should be layered to achieve maximum confidentiality, integrity, and availability (CIA). **Understanding**
Describe how various connectivity devices can interoperate to provide layered defenses against attacks on organizational networks. *Understanding*

**System Security**

**Essential System Security Competencies**

- Discuss the components of a secure system, and how they work together. *Understanding NICE Operate and Maintain*
- Outline a security threat model and how system monitoring tools and mechanisms can be used. *Analyzing NICE Protect and Defend*
- Analyze procedures for system recovery that maintain business continuity in the face of system attack. *Analyzing NICE Operate and Maintain*
- Contrast various methods for authentication and access control in an enterprise, and why one might choose one over another. *Analyzing NICE Operate and Maintain*
- Execute testing protocols on a system with an understanding of normal, secure operation, and document results. *Applying NICE Operate and Maintain*
- Discuss system security issues related to common system architectures such as virtual machines, industrial control systems, embedded systems, autonomous systems, mobile systems and general-purpose systems. *Understanding NICE Operate and Maintain*

**Essential System Security Learning Outcomes**

**System Thinking**

- Explain a holistic approach to system security. *Understanding*
- Describe what a system is, including how components work together. *Understanding*
- Discuss the components of a secure system. *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 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*

**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 such as virtual machines, industrial control systems, embedded systems, autonomous systems, mobile systems and general-purpose systems.  
  *Understanding*

**Human Security**

---

**Essential Human Security Competencies**

- Analyze the security of an individual’s data and privacy in the context of an organization and in their personal lives.  
  *Analyzing NICE Analyze*
- Evaluate organizational policies, rules, and norms with security implications.  
  *Evaluating NICE Oversee and Govern*
- Describe trends in human behavior which pose risks to individual and organizational privacy and security.  
  *Analyzing NICE Analyze*
- Summarize applicable national and global security policies and legislation.  
  *Understanding NICE Oversee and Govern*

---

**Essential Human Security Learning Outcomes**

**Identity Management**
- Compare various methods of identity management, identification, authentication, and access authorization, such as roles, biometrics, and multi-method systems.  
  *Analyzing*
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**
- Compare various social engineering risks and suitable mitigations. **Analyzing**
- Distinguish various types of social engineering attacks, including phishing, vishing, email compromise, and baiting. **Analyzing**
- 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**

**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**
- Evaluate security education, training, and awareness program tasks. **Evaluating**
- 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**
- Compare various types of security and privacy policies, such as HIPAA, FERPA, and PII, along with techniques for user education. **Analyzing**

**Organizational Security**
**Essential Organizational Security Competencies**

- Implement policies and procedures in accordance with national and international laws to protect information security. *Applying NICE Operate and Maintain*
- Describe security features in operating system and database administration in a local or cloud environment. *Understanding NICE Operate and Maintain*
- Summarize the components of a business continuity plan that ensures minimal down time and quick recovery in the face of cybersecurity incidents or natural disasters. *Understanding NICE Operate and Maintain*

**Essential Organizational Security Learning Outcomes**

**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 security features that are embedded within a cloud environment. *Understanding*

**Cybersecurity Planning**
* [Supplemental only]

**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 the 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

Essential Societal Security Competencies
• Illustrate the use of foreign disclosure policies and import/export control regulations as related to cybersecurity. Applying NICE Oversee and Govern
• Categorize applicable cyber policies for a given scenario. Analyzing NICE Oversee and Govern
• Distinguish laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. Analyzing NICE Oversee and Govern

Essential Societal Security Learning Outcomes

Cybercrime
• Categorize different types 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

Supplemental Data Security Competencies

● Perform a forensic analysis on a local network, on stored data within a system as well as mobile devices for an enterprise environment. *Applying NICE Investigate*
● Outline complex technical concepts to technical and non-technical audiences as they relate to data security. *Analyzing NICE Oversee and Govern*

Supplemental Data Security Learning Outcomes

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.  Applying
- Perform acquisition of digital evidence from non-PC devices, such as smart phones, tablets, GPS, games consoles, Smart TVs, and IoT devices.  Applying
- Analyze key computer operating systems files and artifacts, including computer memory forensics acquisition and analysis.  Analyzing
- Analyze digital evidence from non-PC devices, such as smart phones, tablets, GPS, games consoles, Smart TVs, and IoT devices.  Analyzing
- Apply documentation techniques and reporting of findings using industry standard and technically accurate terminology and format.  Applying
- Outline complex technical concepts and processes so that they are easily understood by non-technical audiences.  Analyzing
- Carry out verification and validation of evidence during forensic acquisition, preservation, and analysis, including the use of hashes.  Applying
- Summarize the best practices in collecting and isolating mobile devices when part of digital evidence.  Understanding
- Summarize key features of mobile operating systems (OS) and applications.  Understanding
- Describe key mobile artifacts.  Understanding

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.  Applying

Access Control

- Illustrate the fundamental value and benefits of security architectures used to protect information in computer systems.  Applying
Secure Communication Protocols

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

Cryptanalysis

- Demonstrate timing attacks and their effects on well-known algorithms such as RSA, ElGamal, and the Digital Signature Algorithm. *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

<table>
<thead>
<tr>
<th>Supplemental Software Security Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Implement isolation to secure a process or application. <em>Applying NICE Securely Provision</em></td>
</tr>
<tr>
<td>- Discuss the relationship between an organization’s mission and secure software design. <em>Understanding NICE Securely Provision</em></td>
</tr>
<tr>
<td>- Write software specifications, including security specifications, for a given process or application. <em>Applying NICE Securely Provision</em></td>
</tr>
<tr>
<td>- Assess a given test plan, from a security perspective. <em>Evaluating NICE Securely Provision</em></td>
</tr>
<tr>
<td>- Describe social and legal aspects of software development from a security perspective. <em>Understanding NICE Oversee and Govern</em></td>
</tr>
<tr>
<td>- Develop user documentation for software installation and software configuration including security safeguards. <em>Creating NICE Securely Provision</em></td>
</tr>
</tbody>
</table>

Supplemental Software Security Learning Outcomes
Fundamental Principles

- Test authorization and access control for a given class. Applying
- Develop software for a specific process among multiple secure modules. Applying
- Illustrate isolation through a virtual machine or sandbox. Applying
- Write software specifications that include security specifications infused in the design and implementation 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

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

- 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
Supplemental Component Security Competencies

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

Supplemental Component Security Learning Outcomes

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

Supplemental Connection Security Competencies

- Examine characteristics of commonly used physical networking media. *Analyzing NICE Operate and Maintain*
- Distinguish vulnerabilities and example exploits as they apply to interfaces used in hypervisors, virtual networking, physical networking, and interprocess communication. *Analyzing NICE Protect and Defend*
- Analyze the security risks presented by various network protocols and services. *Analyzing NICE Protect and Defend*
- Implement appropriate defenses throughout an enterprise to harden the network against attackers. *Applying NICE Operate and Maintain, Protect and Defend*

Supplemental Connection Security Learning Outcomes

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*
- 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**

<table>
<thead>
<tr>
<th>Supplemental System Security Competencies</th>
</tr>
</thead>
</table>
| - Critique security throughout the system lifecycle, including security requirements, system management, system testing, and system disposal.  
  *Evaluating NICE Operate and Maintain* |
| - Examine appropriate models for managing authentication, access control and authorization across systems in an organization.  
  *Analyzing NICE Operate and Maintain* |
| - Apply cyber defense methods to prepare a system against attacks, including penetration testing, log analysis, resilience mechanisms, and the use of intrusion detection systems.  
  *Applying NICE Operate and Maintain, Protect and Defend* |
| - Discuss legal aspects of system and network requirements, such as support for litigation holds and forensic analysis.  
  *Understanding NICE Operate and Maintain* |
| - Construct virtual environments including disk and memory structures to meet organization needs.  
  *Creating NICE Operate and Maintain, Securely Provision* |

**Supplemental System Security Learning Outcomes**

**System Thinking**

- Discuss the components that secure special-purpose systems.  
  *Understanding*
- 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
- Critique the strengths and weaknesses of various access control models and mechanisms. *Evaluating*

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*
- Paraphrase legal ramifications that can affect day-to-day network administration, such as litigation holds. *Understanding*
- 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

**Supplemental Human Security Competencies**
- Analyze a variety of physical access controls. *Analyzing NICE Protect and Defend*
- Use a variety of tools and techniques to detect and mitigate social engineering threats. *Applying NICE Protect and Defend*
Supplemental Human Security Learning Outcomes

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

Social Engineering

- 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

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

- 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

Supplemental Organizational Security Competencies

- Analyze risks to information assets in an organization and communicate them to stakeholders. *Analyzing NICE Analyze*
- Analyze the meaning and use of various security metrics and data with the aid of tools, to ensure quality control and security of data. *Analyzing NICE Operate and Maintain*
- Assess administrative procedures for protecting systems from attack and ensuring the availability of system access and functions in an organization. *Evaluating NICE Operate and Maintain*
- Discuss issues related to personnel security in an organization, including the protection of personally identifiable information, and proper use or avoidance of fear, uncertainty, and doubt (FUD) as an awareness tool. *Understanding NICE Oversee and Govern*

Supplemental Organizational Security Learning Outcomes

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

- Critique administrative procedures for protecting the physical system from attack. *Evaluating*
Implement hardening techniques to protect the operating system. \textit{Applying}

Assess processes that ensure availability of system access and functions. \textit{Evaluating}

Cybersecurity Planning

- Apply Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis in an organization. \textit{Applying}

Business Continuity, Disaster Recovery, and Incident Management

[Essential only]

Security Program Management

- Perform project management tasks that provide for security of data. \textit{Applying}
- Analyze the meaning and use of various security metrics used in protecting the network. \textit{Analyzing}
- Describe the use of quality assurance and quality control to prevent mistakes and increase the quality of a system. \textit{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. \textit{Understanding}
- Classify components of third party security services. \textit{Understanding}
- Discuss components that ensure the protection of personally identifiable information. \textit{Understanding}

Societal Security

\begin{tcolorbox}[title=Supplemental Societal Security Competencies]
- Apply corresponding cyber laws according to a given situation and circumstances. \textit{Applying NICE Oversee and Govern}
- Distinguish social dynamics of computer attackers in a global context. \textit{Analyzing NICE Investigate}
- Compare different cyber ethics theories that impact on individuals and society. \textit{Analyzing NICE Investigate}
\end{tcolorbox}

Supplemental Societal Security Learning Outcomes
Cybercrime
- Categorize challenges associated with the enforcement and prosecution of cybercrime. \textit{Analyzing}

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

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

Cyber Policy
- Examine the cost of cybersecurity to a nation. \textit{Analyzing}

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


Appendix A: Competencies

All the competencies presented in this guidance are collected together here organized by knowledge area.

Cross-Cutting Competencies

<table>
<thead>
<tr>
<th>Cross-Cutting Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Outline via appropriate methods, and using industry standard terminology, cybersecurity-related issues within an organization as they pertain to Confidentiality, Integrity, and Availability. <em>Analyzing NICE Analyze, Operate and Maintain</em></td>
</tr>
<tr>
<td>● Assess and respond appropriately to various risks which can affect the expected operation of information systems. <em>Evaluating NICE Protect and Defend</em></td>
</tr>
<tr>
<td>● Investigate current and emerging cyberthreats and incorporate best practices to mitigate them. <em>Applying NICE Operate and Maintain, Collect and Operate</em></td>
</tr>
<tr>
<td>● Apply appropriate countermeasures to help protect organizational resources based on an understanding of how bad actors think and operate. <em>Applying NICE Protect and Defend</em></td>
</tr>
<tr>
<td>● Discuss how changes in one part of a system may impact other parts of a cybersecurity ecosystem. <em>Understanding NICE Protect and Defend</em></td>
</tr>
</tbody>
</table>
Data Security Competencies

Essential Data Security Competencies

- Carry out collection and acquisition of digital evidence in a forensically sound manner. 
  Applying NICE Protect and Defend, Investigate
- Implement data security by selecting appropriate cryptographic procedures, algorithms, and tools based on security policy and level of risk in an organization. 
  Applying NICE Protect and Defend, Operate and Maintain, Securely Provision
- Infer gaps in data security considering current and emerging technologies and the current state and prevailing trends in cybercrime. Understanding NICE Protect and Defend
- Perform actions to maintain data integrity for information systems and networks using appropriate levels of authentication, authorization, and access control. Applying NICE Operate and Maintain, Protect and Defend, Securely Provision
- Demonstrate knowledge of the principles, processes, tools and techniques used in responding to security incidents. Understanding NICE Protect and Defend, Investigate
- Execute appropriate mitigation procedures and apply necessary countermeasures in response to security threats. Applying NICE Protect and Defend

Supplemental Data Security Competencies

- Perform a forensic analysis on a local network, on stored data within a system as well as mobile devices for an enterprise environment. Applying NICE Investigate
- Outline complex technical concepts to technical and non-technical audiences as they relate to data security. Analyzing NICE Oversee and Govern
Software Security Competencies

Essential Software Security Competencies

- Analyze the security of a software system and its related data and apply secure programming practices. *Analyzing NICE Securely Provision, Operate and Maintain*
- Demonstrate techniques of defensive programming and secure coding in a software system. *Understanding NICE Securely Provision, Operate and Maintain*
- Analyze the software development life cycle and explain and discuss how security can be incorporated into the software development life cycle. *Analyzing NICE Securely Provision*
- Use documentation or a knowledge base to resolve a security challenge in an identified computing scenario. *Applying NICE Protect and Defend*

Supplemental Software Security Competencies

- Implement isolation to secure a process or application. *Applying NICE Securely Provision*
- Discuss the relationship between an organization’s mission and secure software design. *Understanding NICE Securely Provision*
- Write software specifications, including security specifications, for a given process or application. *Applying NICE Securely Provision*
- Assess a given test plan, from a security perspective. *Evaluating NICE Securely Provision*
- Describe social and legal aspects of software development from a security perspective. *Understanding NICE Oversee and Govern*
- Develop user documentation for software installation and software configuration including security safeguards. *Creating NICE Securely Provision*
Component Security Competencies

Essential Component Security Competencies

- Distinguish and mitigate vulnerabilities of system components throughout their lifecycle. *Analyzing NICE Protect and Defend*
- Analyze how security design impacts components throughout their lifecycle, especially related software and firmware updates. *Analyzing NICE Protect and Defend*

Supplemental Component Security Competencies

- Use tools and techniques, such as fuzz testing, for testing the security properties of a component beyond its functional correctness. *Applying NICE Operate and Maintain*
### Connection Security Competencies

#### Essential Connection Security Competencies

- Construct and properly configure computer networks which adhere to current industry standards and organizational guidelines. *Creating NICE Operate and Maintain*
- Investigate the impact of various connection and transmission attacks on network hardware and software. *Applying NICE Protect and Defend, Analyze*

#### Supplemental Connection Security Competencies

- Examine characteristics of commonly used physical networking media. *Analyzing NICE Operate and Maintain*
- Distinguish vulnerabilities and example exploits as they apply to interfaces used in hypervisors, virtual networking, physical networking, and interprocess communication. *Analyzing NICE Protect and Defend*
- Analyze the security risks presented by various network protocols and services. *Analyzing NICE Protect and Defend*
- Implement appropriate defenses throughout an enterprise to harden the network against attackers. *Applying NICE Operate and Maintain, Protect and Defend*
System Security Competencies

Essential System Security Competencies

- Discuss the components of a secure system, and how they work together. *Understanding NICE Operate and Maintain*
- Outline a security threat model and how system monitoring tools and mechanisms can be used. *Analyzing NICE Protect and Defend*
- Analyze procedures for system recovery that maintain business continuity in the face of system attack. *Analyzing NICE Operate and Maintain*
- Contrast various methods for authentication and access control in an enterprise, and why one might choose one over another. *Analyzing NICE Operate and Maintain*
- Execute testing protocols on a system with an understanding of normal, secure operation, and document results. *Applying NICE Operate and Maintain*
- Discuss system security issues related to common system architectures such as virtual machines, industrial control systems, embedded systems, autonomous systems, mobile systems and general-purpose systems. *Understanding NICE Operate and Maintain*

Supplemental System Security Competencies

- Critique security throughout the system lifecycle, including security requirements, system management, system testing, and system disposal. *Evaluating NICE Operate and Maintain*
- Examine appropriate models for managing authentication, access control and authorization across systems in an organization. *Analyzing NICE Operate and Maintain*
- Apply cyber defense methods to prepare a system against attacks, including penetration testing, log analysis, resilience mechanisms, and the use of intrusion detection systems. *Applying NICE Operate and Maintain, Protect and Defend*
- Discuss legal aspects of system and network requirements, such as support for litigation holds and forensic analysis. *Understanding NICE Operate and Maintain*
- Construct virtual environments including disk and memory structures to meet organization needs. *Creating NICE Operate and Maintain, Securely Provision*
Human Security Competencies

Essential Human Security Competencies

- Analyze the security of an individual’s data and privacy in the context of an organization and in their personal lives. Analyzing NICE Analyze
- Evaluate organizational policies, rules, and norms with security implications. Evaluating NICE Oversee and Govern
- Describe trends in human behavior which pose risks to individual and organizational privacy and security. Analyzing NICE Analyze
- Summarize applicable national and global security policies and legislation. Understanding NICE Oversee and Govern

Supplemental Human Security Competencies

- Analyze a variety of physical access controls. Analyzing NICE Protect and Defend
- Use a variety of tools and techniques to detect and mitigate social engineering threats. Applying NICE Protect and Defend
- Summarize techniques to encourage personal compliance with cybersecurity rules, policies, and ethical norms. Understanding NICE Oversee and Govern
## Organizational Security Competencies

### Essential Organizational Security Competencies

- Implement policies and procedures in accordance with national and international laws to protect information security. *Applying NICE Operate and Maintain*
- Describe security features in operating system and database administration in a local or cloud environment. *Understanding NICE Operate and Maintain*
- Summarize the components of a business continuity plan that ensures minimal down time and quick recovery in the face of cybersecurity incidents or natural disasters. *Understanding NICE Operate and Maintain*

### Supplemental Organizational Security Competencies

- Analyze risks to information assets in an organization and communicate them to stakeholders. *Analyzing NICE Analyze*
- Analyze the meaning and use of various security metrics and data with the aid of tools, to ensure quality control and security of data. *Analyzing NICE Operate and Maintain*
- Assess administrative procedures for protecting systems from attack and ensuring the availability of system access and functions in an organization. *Evaluating NICE Operate and Maintain*
- Discuss issues related to personnel security in an organization, including the protection of personally identifiable information, and proper use or avoidance of fear, uncertainty, and doubt (FUD) as an awareness tool. *Understanding NICE Oversee and Govern*
Societal Security Competencies

Essential Societal Security Competencies

- Illustrate the use of foreign disclosure policies and import/export control regulations as related to cybersecurity. *Applying NICE Oversee and Govern*
- Categorize applicable cyber policies for a given scenario. *Analyzing NICE Oversee and Govern*
- Distinguish laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. *Analyzing NICE Oversee and Govern*

Supplemental Societal Security Competencies

- Apply corresponding cyber laws according to a given situation and circumstances. *Applying NICE Oversee and Govern*
- Distinguish social dynamics of computer attackers in a global context. *Analyzing NICE Investigate*
- Compare different cyber ethics theories that impact on individuals and society. *Analyzing NICE Investigate*