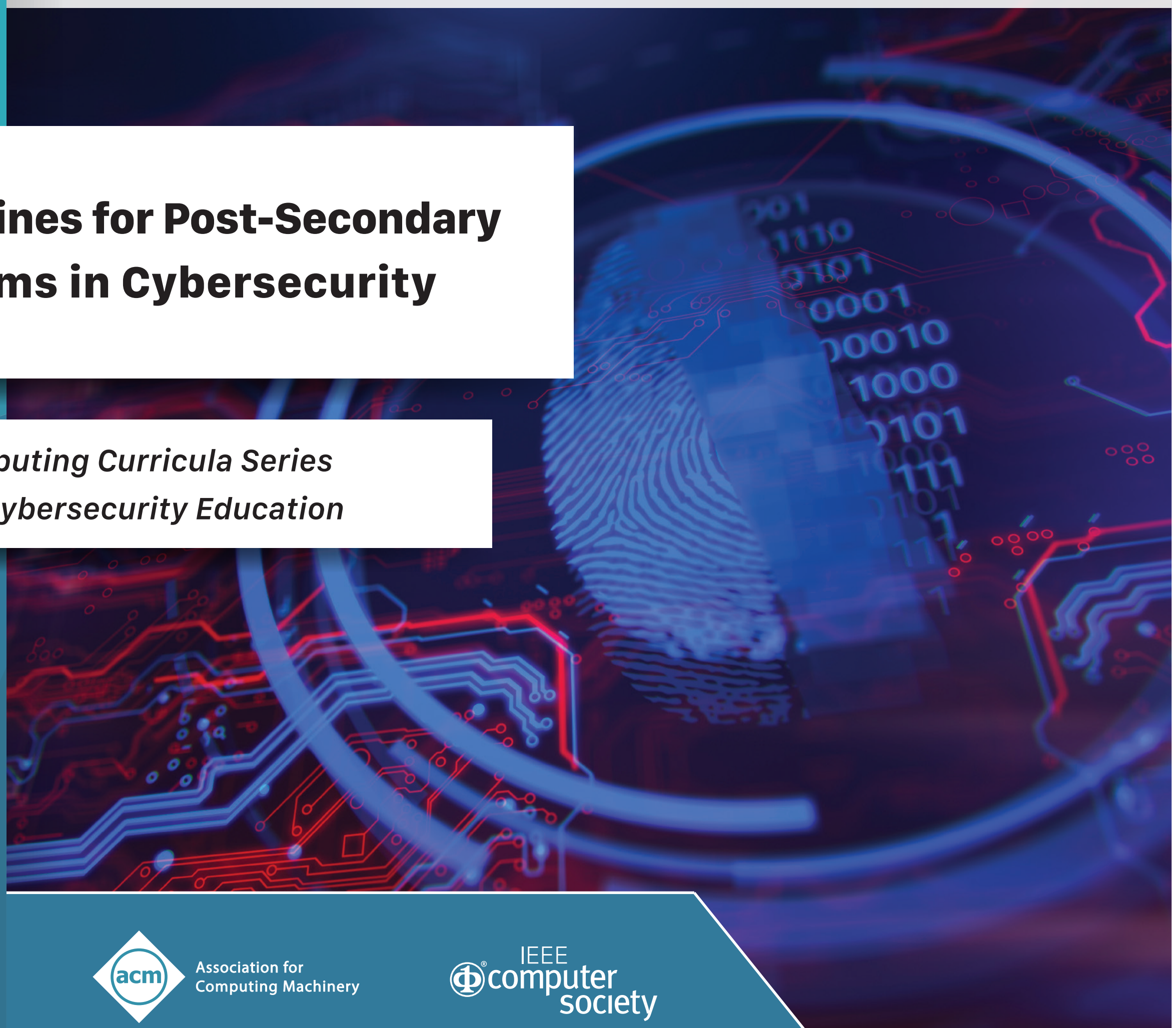
CYBERSECURITY CURRICULA 2017



Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity

A Report in the Computing Curricula Series
Joint Task Force on Cybersecurity Education

Association for Computing Machinery

IEEE computer society

ASSOCIATION FOR INFORMATION SYSTEMS

ifip

- Association for Computing Machinery (ACM)
- IEEE Computer Society (IEEE-CS)
- Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC)
- International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)

Version 1.0 Report
31 December 2017

Cybersecurity Curricula 2017

Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity

A Report in the Computing Curricula Series
Joint Task Force on Cybersecurity Education

Association for Computing Machinery (ACM)
IEEE Computer Society (IEEE-CS)
Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC)
International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)

Version 1.0 Report
31 December 2017

ISBN: 978-1-4503-5278-9
DOI: 10.1145/3184594
Web link: https://dl.acm.org/citation.cfm?id=3184594

When available, you may order additional copies from:

ACM Order Department
P.O. Box 30777
New York, NY 10087-0777

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros
P.O. Box 3014
Los Alamitos, CA 90720-1314

Sponsors:

This report was made possible by financial support from the following:
Association for Computing Machinery (ACM)
IEEE Computer Society (IEEE-CS)
Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC)

U.S. National Science Foundation (Award# 1623104)
Intel Corporation
U.S. National Security Agency (Grant# H98230-17-1-0219)

The CSEC2017 Final Report has been endorsed by ACM, IEEE-CS, AIS SIGSEC, and IFIP WG 11.8.

Cover designed by Nelly Group, LLC.

Cybersecurity Curricula 2017

Version 1.0 Report
31 December 2017

A Report in the Computing Curricula Series
Joint Task Force on Cybersecurity Education

Association for Computing Machinery (ACM)
IEEE Computer Society (IEEE-CS)
Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC)
International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)

CSEC2017 Joint Task Force

Diana L. Burley, Ph.D. (JTF Co-Chair, ACM)
Professor, Human & Organizational Learning
Executive Director, Institute for Information Infrastructure Protection
The George Washington University, USA

Matt Bishop, Ph.D. (JTF Co-Chair, ACM/IFIP)
Professor, Computer Science
Co-Director, Computer Security Laboratory
University of California, Davis, USA

Scott Buck (ACM)
University Program Director
Intel Labs, Intel, USA

Joseph J. Ekstrom, Ph.D. (IEEE CS)
Associate Professor Emeritus, Information Technology
Brigham Young University, USA

Lynn Futcher, Ph.D. (ACM/IFIP)
Associate Professor
Nelson Mandela University, South Africa

David Gibson, Ph.D. (ACM)
Professor Emeritus, Computer Science
Department of Computer and Cyber Science
United States Air Force Academy, USA

Elizabeth K. Hawthorne, Ph.D. (ACM)
Senior Professor, Computer Science and Cybersecurity
Union County College, USA

Siddharth Kaza, Ph.D. (ACM)
Associate Professor, Computer & Information Sciences
Chair, Department of Computer & Information Sciences
Towson University, USA

Yair Levy, Ph.D. (AIS SIGSEC)
Professor, Information Systems and Cybersecurity
Director, Center for Information Protection, Education, and Research (CIPhER)
Nova Southeastern University, USA

Herbert Mattord, Ph.D. (AIS SIGSEC)
Associate Professor, Information Systems
Director of Education, Institute for Cybersecurity Workforce Development
Kennesaw State University, USA

Allen Parrish, Ph.D. (IEEE CS)
Professor, Cyber Science
Chair, Department of Cyber Science
United States Naval Academy, USA

Table of Contents

Table of Figures

Chapter 1: Introduction to Cybersecurity Education

By all accounts, the world faces a current and growing workforce shortage of qualified cybersecurity professionals and practitioners. In fact, both government and non-government sources project nearly 1.8 million cybersecurity-related positions going unfilled by 2022[1]. The workforce demand is acute, immediate, and growing[2]. In order to develop the required talent, academic departments across the spectrum of computing disciplines are launching initiatives to establish new cybersecurity programs or courses of study within existing programs. Whether developing full new programs, defining new concentrations within existing programs, or augmenting existing course content, these institutions need curricular guidance based on a comprehensive view of the cybersecurity field, the specific demands of the base discipline, and the relationship between the curriculum and cybersecurity workforce frameworks.

In August 2015, the Association for Computing Machinery (ACM) Education Board recognized this urgent need and took measures to assemble a Joint Task Force on Cybersecurity Education (CSEC2017) with other professional and scientific computing societies to develop comprehensive curricular guidance in cybersecurity education.

For nearly five decades, starting with Computer Science 1968[3], the ACM education initiative has collaborated with other professional and scientific societies to establish curricular guidelines for academic program development in the computing disciplines. Currently, ACM curricular volumes provide recommendations in computer science, computer engineering, information systems, information technology, and software engineering. The ACM Computing Curricula 2005 Report (CC2005), currently being updated, provides an overview of the curriculum guidelines for each of these five computing disciplines[4]. This volume, CSEC2017, represents an expansion of the ACM education initiative to include the first set of global curricular recommendations in cybersecurity education.

Due to the highly dynamic nature of cybersecurity, it is strongly recommended that these curricular guidelines be reviewed within five years of the publication date.

1.1 The Joint Task Force

The CSEC2017 Joint Task Force on Cybersecurity Education (JTF) was officially launched in September 2015 as a collaboration between major international computing societies: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS)[5], Association for Information Systems Special Interest Group on Information

---

[1] See, for example, CSO Online: http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

[2] (ISC)2 Report available here: https://www.boozallen.com/content/dam/boozallen/documents/Viewpoints/2015/04/frostsullivan-ISC2-global-information-security-workforce-2015.pdf

[3] ACM Curriculum Committee on Computer Science. 1968. Curriculum 68: Recommendations for Academic Programs in Computer Science. *Comm. ACM* 11, 3 (Mar. 1968), 151-197.

[4] ACM Computing Disciplines Overview: http://acm.org/education/curricula-recommendations

[5] IEEE CS website: https://www.computer.org/

Security and Privacy (AIS SIGSEC)[6], and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)[7].

The ACM Education Board appointed the CSEC2017 JTF co-chairs. In addition to the co-chairs, the CSEC2017 JTF includes nine leading cybersecurity professionals selected by the participating professional societies to represent their constituencies and to provide a diverse set of perspectives. The JTF members are listed along with their affiliations at the beginning of this document.

The CSEC2017 JTF is an outcome of the Cyber Education Project (CEP)[8]. The CEP initiative was organized in July 2014 by a group of computing professionals who represented a diverse cross-section of academic institutions and professional societies. The CEP mission was two-fold: to initiate the processes for (1) developing undergraduate curricular guidance; and (2) establishing a case for the accreditation of educational programs in the cyber sciences.

The CSEC2017 JTF is advancing the first mission of the CEP:

> *To develop comprehensive curricular guidance in cybersecurity education that will support future program development and associated educational efforts at the post-secondary level.*

While the CSEC2017 JTF has chosen to use the more generally accepted term *cybersecurity* instead of the term *cyber sciences* advanced by the CEP[8], conceptually the terms are consistent.

1.1.1 The Vision

The CSEC2017 JTF has worked actively since its inception in September of 2015 to define project parameters and establish a foundational vision, mission and goals. The project vision is:

> *The CSEC2017 curricular volume will be the leading resource of comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity offerings at the post-secondary level.*

1.1.2 The Mission

The CSEC2017 mission is twofold:

- To develop comprehensive and flexible curricular guidance in cybersecurity education that will support future program development and associated educational efforts at the post-secondary level, and
- To produce a curricular volume that structures the cybersecurity discipline and provides guidance to institutions seeking to develop or modify a broad range of programs, concentrations and/or courses rather than a prescriptive document to support a single program type.

---

[6] AIS SIGSEC website: http://aisnet.org/group/SIGSEC
[7] IFIP WG 11.8 website: https://www.ifiptc11.org/wg118
[8] Cyber Education Project website: http://cybereducationproject.org/about/

1.1.3 The Goals

Based on this mission, the CSEC2017 JTF established the following goals for the curricular volume:

- To describe a vision of proficiency in cybersecurity,
- To define a structure for the cybersecurity discipline by developing a thought model that defines the boundaries of the discipline and outlines key dimensions of the curricular structure,
- To support the alignment of academic programs with industry needs in cybersecurity,
- To involve broad global audience of stakeholders through continuous community engagement during the development process,
- To develop curricular guidance that is comprehensive enough to support a wide range of program types, and
- To develop curricular guidance that is grounded in fundamental principles that provide stability, yet is structured to provide flexibility to support evolving program needs.

1.2 The Audience

The CSEC2017 JTF defines the primary and secondary audiences for this cybersecurity guidance below.

Primary audience:

- Faculty members in computing-based disciplines at academic institutions around the world who are interested in developing cybersecurity programs, defining new cybersecurity concentrations within existing programs, or augmenting existing programs (including existing concentrations and courses) to incorporate cybersecurity content.

Secondary audience:

- Industry members who will assist with cybersecurity program development within academic institutions, develop industry-based programs, and be consumers of the student outcomes of these programs,
- Training and professional development providers,
- Faculty members in non-computing based disciplines who are developing or intend to develop allied programs that teach cybersecurity concepts and skills,
- Academic administrators with oversight for program and course development and revision,
- Workforce framework developers (government and non-government),
- Policymakers,
- Members of the K-12 educational community who are preparing students to enter post-secondary education in cybersecurity, and

- Other stakeholders involved with cybersecurity workforce development initiatives.

1.3 Sources

The curricular guidelines developed in this document build upon prior work in computer security, information assurance and cyber security education, training, and workforce development. In addition to the sources listed later in this document under References, major sources used in the development of this document include:

- Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science,
- Global IT Skills Framework for the Information Age (SFIA),
- Requirements of the U.S. National Security Agency and U.S. Department of Homeland Security National Centers of Academic Excellence in Cyber Defense and Cyber Operations,
- Information Technology Curricula 2017: Curriculum Guidelines for Baccalaureate Degree Programs in Information Technology,
- Guide to the Systems Engineering Body of Knowledge, and
- U.S. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

1.4 Global Community Engagement

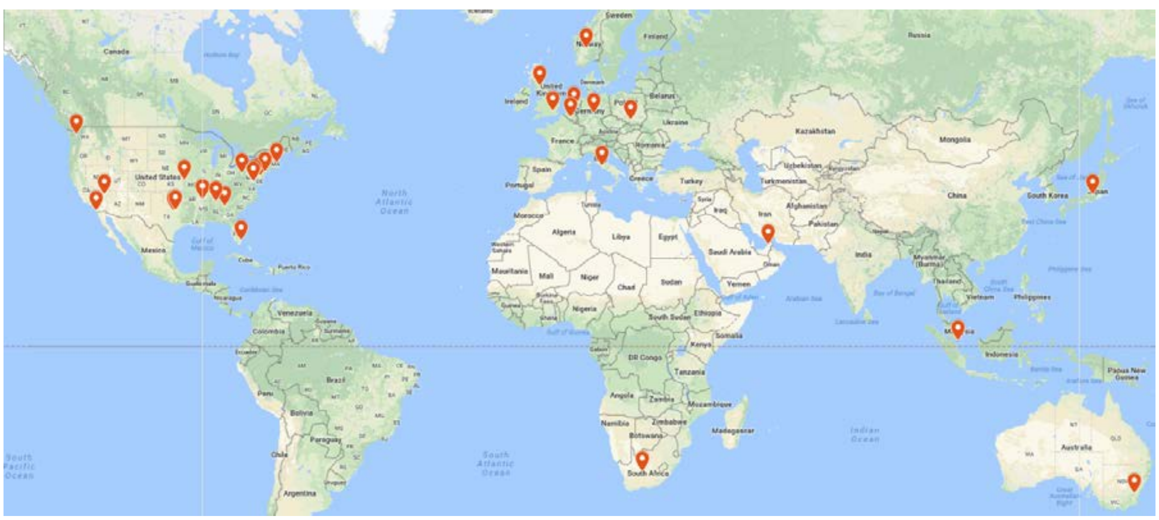


Figure 1. Global engagement activities.

The CSEC2017 JTF continuously engaged the broad stakeholder community throughout the development process. Community members provided input to shape the approach, content and organizational structure of the CSEC report. Community engagement activities have included: special sessions, panels and workshops at conferences affiliated with participating professional societies, international conferences, keynote addresses, webinars, working group meetings, government briefings, and advisory board briefings.

As shown in Figure 1, community engagement activities were held in a variety of locations around the world. These activities were positioned as regional convening opportunities to gather insights from a cross-section of subject matter experts. Among these activities, key milestones in the development process included international workshops and a global stakeholder survey.

1.4.1 International Workshops

In 2016, with the support of the Intel Corporation and the U.S. National Science Foundation, the JTF organized and hosted the International Security Education Workshop (ISEW), which was held June 13-15, 2016, in Philadelphia, PA[9]. The workshop was structured to advance the CSEC2017 development process. Through panel discussions and working group sessions, approximately 75 stakeholders from the global cybersecurity education community provided input on the curricular content and structure by debating two key questions:

- What should be included in a cybersecurity degree program?
- How should the volume of curricular recommendations be organized and disseminated?

The full meeting report is available on the CSEC2017 website. The input gathered from participants of the ISEW informed the first version of the CSEC2017 thought model and served as the basis of the global stakeholder survey.

In August 2016, government representatives from 10 of the Association of South East Asian Nations (ASEAN), along with leaders from Japan and Australia, participated in a 2016 project briefing in Singapore. ASEAN representatives included: Brunei, Malaysia, Laos, Thailand, Singapore, Cambodia, Myanmar, Vietnam, Indonesia, and Philippines.

Approximately one year following the ISEW, on May 29-31, 2017, the JTF organized a community engagement session at the 10th World Information Security Education Conference (WISE 10) in Rome, Italy. Participants from countries such as Germany, Norway, Russia Sweden, South Africa, and the United States gathered to discuss the CSEC2017 v. 0.05 draft document and to advance the development process. A report on the workshop structure and purpose was published in the WISE 10 proceedings.

1.4.2 Global Stakeholder Survey

In September 2016, after a year of community engagement and developmental work, the JTF launched a global stakeholder survey to solicit feedback on the proposed curricular thought model. Stakeholders were invited to participate in the survey through direct invitations, announcements in public educational and scientific forums, social media outreach via the JTF website and LinkedIn, and invitations sent through the distribution lists of participating professional associations. The survey yielded 231 responses from

[9] The ISEW was co-located with the Colloquium for Information Systems Security Education (CISSE), and sponsored by the Intel Corporation, the National Science Foundation (NSF), and the Institute for Information and Infrastructure Protection (I3P) at the George Washington University (GW).

stakeholders located in 20 countries; working across academia, industry and government; and representing all five computing disciplines.

In summary, survey respondents suggested that the JTF clarify the intended audience of the curricular volume; refine the definitions and distinguish between the curricular elements of the thought model; provide additional information on the content of each of the knowledge categories; simplify the thought model; and adapt the structure to allow for placement of emerging topics. The JTF used these comments to revise the thought model. The full survey report is available on the CSEC2017 website.

1.4.3 Contributor Acknowledgement

The JTF gratefully acknowledges the valuable contributions of all participants in our community engagement efforts. We specifically recognize the global subject matter experts who provide advice as members of our advisory boards and working groups. Throughout the development process, members of the Global Advisory Board and Industry Advisory Board provided advice on the development process, global community engagement strategies and specific curricular content. Members of our Knowledge Area Working Groups assisted task force members with the development of knowledge area curricular content.

We carefully considered all comments and critiques from community members, and we are particularly appreciative of the many comments provided as feedback. A comprehensive list of contributors (including participants in the global workshops), along with a graphical depiction of the breadth of global participation, appears in Appendix A at the end of this document.[10]

1.5 Cybersecurity as a Discipline

In the CC2005 Overview Report, the ACM identifies five primary computing disciplines, and recognizes a category of computing disciplines that highlights the increasing number of hybrid or interdisciplinary courses of study.

- Computer Engineering,
- Computer Science,
- Information Systems,
- Information Technology,
- Software Engineering,
- Mixed Disciplinary Majors *(xx Informatics or Computational xx).*

The CSEC2017 JTF advances cybersecurity as a new computing discipline and positions the cybersecurity curricular guidance within the context of the current set of defined computing disciplines. These five disciplines (listed above) often serve as the foundation of new cybersecurity programs (or courses of study). As a result, the disciplinary lens shapes the depth of coverage and the desired student learning outcomes. The manner in

[10] While we tried to accurately capture all contributors, if we missed or misrepresented your participation, please contact us for corrections.

which the disciplinary lenses shape the curricular content will be fully described in chapter 3 of this document.

1.6 Report Structure

This report, CSEC2017 v.1.0, presents the work of the JTF. The CSEC2017 report provides an overview of the cybersecurity discipline to frame the curricular model. The document then presents the curricular framework and outlines the recommended curricular content. Next, and in order to place the content within the larger context, the report highlights industry perspectives on cybersecurity. Finally, to aid with implementation, the report discusses issues related to the educational practice, suggests a process for developing roadmaps that link the curricular model to workforce frameworks, and references course, curricular and workforce exemplars that highlight how global institutions could implement the curricular guidelines.

The roadmaps and exemplars will be continuously received through the community engagement website: http://cybered.acm.org *(coming soon).*

Chapter 2: The Cybersecurity Discipline

The CSEC2017 JTF 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.*

Cybersecurity is a computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It draws from the foundational fields of information security and information assurance; and began with more narrowly focused field of computer security.

The need for cybersecurity arose when the first mainframe computers were developed. Multiple levels of security were implemented to protect these devices and the missions they served. The growing need to maintain national security eventually led to more complex and technologically sophisticated security safeguards. During the early years, cybersecurity as practiced, even if not specifically identified as such, was a straightforward process composed predominantly of physical security and document classification. The primary threats to security were physical theft of equipment, espionage against products of the systems, and sabotage. As society's reliance on broad cyber infrastructure has expanded, so too has the threat environment.

2.1 The Rise of Cyberthreats

An agency of the U.S. Department of Defense, the Advanced Research Projects Agency (ARPA) was created in 1958 and began examining the feasibility of a redundant, networked communications system to support the exchange of computer data. The resulting network, called ARPANET, was created in the late 1960s and saw wide use, increasing the potential for its misuse.

Security that went beyond protecting the physical location of computing devices effectively began with a single paper published by the RAND Corporation in February 1970 for the Department of Defense. That report, RAND Report R-609, attempted to define the multiple controls and mechanisms necessary for the protection of a computerized data-processing system.

In the 1970s, the development of TCP (the Transmission Control Protocol) and IP (the Internet Protocol) led to the emergence of the Internet. The development of the World Wide Web in the 1980s brought the Internet to wide use, which significantly increased the importance of cybersecurity. The U.S. Government passed several key pieces of legislation that formalized the recognition of computer security as a critical issue for federal information systems including the Computer Fraud and Abuse Act of 1986 and the Computer Security Act of 1987. The Internet eventually brought ubiquitous connectivity to virtually all computers, where integrity and confidentiality were a lower priority than the drive for availability. Many problems that plague the Internet today result from this early lack of focus on security awareness.

Early computing approaches relied on security that was built into the physical environment of the data center that housed the computers. As networked computers became the dominant style of computing, the ability to physically secure a networked computer was lost, and the stored information became more exposed to security threats. Larger organizations began integrating security into their computing strategies. Anti-virus products became extremely popular, and cybersecurity began to emerge as an independent discipline.

The Internet brings unsecured computer networks and billions of connected devices into continuous communication with each other. The security of each computer's stored information is contingent upon awareness, learning, and applying cybersecurity principles. Securing a computer's stored information can be accomplished by first determining a value for the information. Choosing security controls to apply and protect the information as it is transmitted, processed and stored should be commensurate with that value and its threat environment.

Recent years have seen a growing awareness of the need to improve cybersecurity, as well as a realization that cybersecurity is important to the national defense of every country. The growing threat of cyberattacks has made governments and companies more aware of the need to defend the computerized control systems of utilities and other critical infrastructure. Another growing concern is the threat of nation-states engaging in cyberwarfare, and the possibility that business and personal information systems could become casualties if they are undefended.

2.2 The Emergence of Cybersecurity as a Discipline

Given society's increasing dependence on the global cyber infrastructure, it is no surprise that cybersecurity is emerging as an identifiable discipline with a breadth and depth of content that encompasses many of the subfields (e.g., software development, networking, database management) that form the modern computing ecosystem. Underlying this emergence is the need to prepare specialists across a range of work roles for the complexities associated with assuring the security of system operations from a holistic view. Assuring secure operations involves the creation, operation, defense, analysis, and testing of secure computer systems.

While cybersecurity is an interdisciplinary course of study including aspects of law, policy, human factors, ethics, and risk management, it is fundamentally a computing-based discipline. As such, and as depicted in Figure 2, academic programs in cybersecurity are both informed by the interdisciplinary content, and driven by the needs and perspectives of the computing discipline that forms the programmatic foundation.

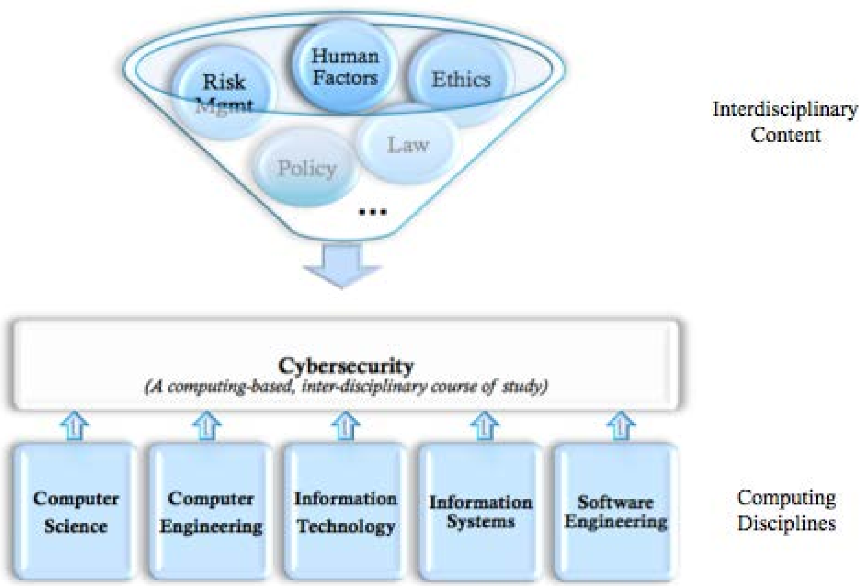


Figure 2. Structure of the cybersecurity discipline.

Cybersecurity as an identifiable degree field is still in its infancy. Driven by significant workforce needs, global academic institutions are developing a range of educational programs in the field while others are adjusting existing programs to incorporate cybersecurity content. The curricular recommendations provided in this volume are framed by the computing disciplines: computer science, computer engineering, information technology, information systems, and software engineering.

2.3 Characteristics of a Cybersecurity Program

Each graduate of a cybersecurity program of study should have a cybersecurity curriculum that includes:

- A computing-based foundation (e.g., computer science, information technology),
- Crosscutting concepts that are broadly applicable across the range of cybersecurity specializations (e.g., cybersecurity's inherent adversarial mindset),
- A body of knowledge containing essential cybersecurity knowledge and skills,
- A direct relationship to the range of specializations meeting the in-demand workforce domains, and
- A strong emphasis on the ethical conduct and professional responsibilities associated with the field.

The curricular framework advanced in this volume will help academic institutions develop cybersecurity programs that meet each of these criteria.

Chapter 3: Cybersecurity Curricular Framework

To promote proficiency in the field, cybersecurity programs require curricular content that includes:

- The theoretical and conceptual knowledge essential to understanding the discipline, and
- Opportunities to develop the practical skills that support the application of that knowledge.

The content included in any cybersecurity program requires a delicate balance of breadth and depth, along with an alignment to workforce needs. It also demands a structure that simultaneously provides for consistency across programs of similar types while allowing for the flexibility necessitated by both constituent needs and advancements in the body of knowledge. The curricular framework presented in this chapter supports and balances the achievement of these goals.

3.1 Philosophy and Approach

The CSEC thought model (hereafter thought model) is based on a rigorous review of existing curricular frameworks in science education, computing education, and cybersecurity education. Our philosophy, shaped in part by the U.S. National Research Council Next Generation Science Standards[11], views cybersecurity as a body of knowledge grounded in enduring principles that is continuously extended, refined, and revised through evidence-based practice.

3.2 Thought Model

The thought model shown in Figure 3 has three dimensions: knowledge areas, crosscutting concepts, and disciplinary lenses.

While not explicitly identified as a model dimension, foundational requirements underlie and support all of the curricular content. These requirements include competencies such as communication, numeracy, analytical and problem-solving skills, critical thinking, and teamwork which are developed through general education. Along with technological literacy and ethical conduct, these requirements lead students to become contributing members of society.

[11] U.S. National Research Council Next Generation Science Standards website: http://nextgenscience.org

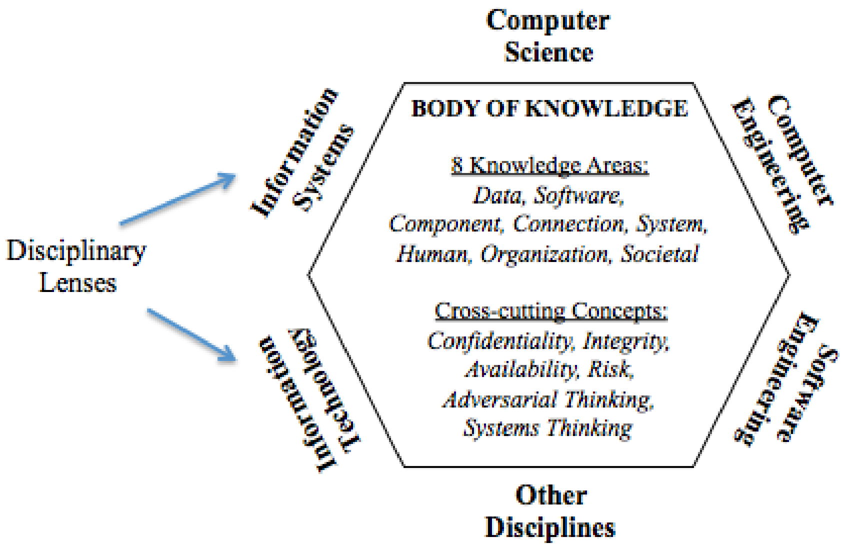


Figure 3. CSEC thought model.

3.2.1 Knowledge Areas

Knowledge areas (KAs) serve as the basic organizing structure for cybersecurity content. Each knowledge area is made up of critical knowledge with broad importance within and across multiple computing-based disciplines. The knowledge areas are structured as flexible buckets in the thought model to allow for the expansion and contraction of content as needed. Collectively, knowledge areas represent the full body of knowledge within the field of cybersecurity.

The essentials of cybersecurity. The essential concepts of each knowledge area capture the cybersecurity proficiency that every student needs to achieve regardless of program focus. Essentials should be introduced early and reinforced throughout every cybersecurity program.

The knowledge units (KUs) are thematic groupings that encompass multiple, related topics; the topics cover the required curricular content for each KU. The learning outcomes are a description of what students should know or be able to do. As shown in Figure 4, The KAs may contain multiple knowledge units, topics and learning outcomes. Specific learning outcomes for topics contained in each KA are provided in the exemplars.

The essential concepts are explicitly identified in each knowledge area. These concepts may also appear as specific knowledge units, as topics within knowledge units, or as aggregates of topics across knowledge units. Taken together, the essential concepts in all of the knowledge areas should be covered in every cybersecurity program. Specific learning outcomes for the essential concepts are included in the curricular framework described in Chapter 4.

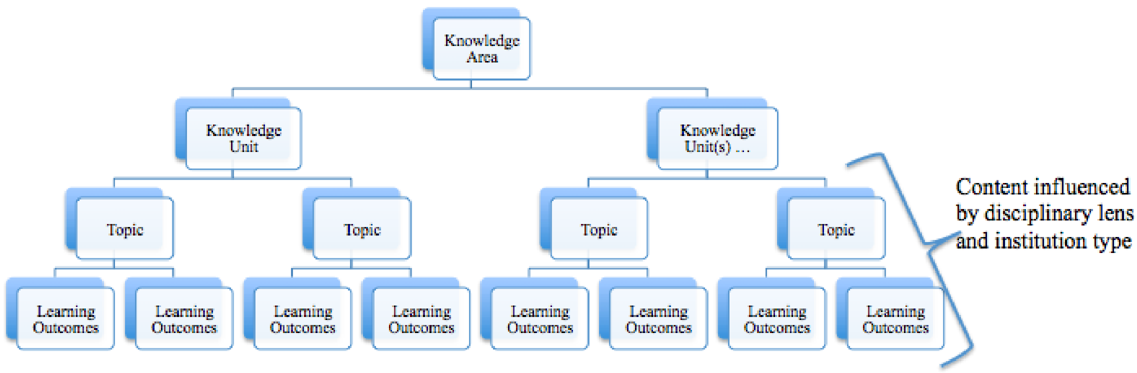


Figure 4. Knowledge area structure.

In the thought model, each knowledge unit meets the following criteria:

- Has broad (though variable, based on the disciplinary lens) importance across multiple computing-based disciplines,
- Provides a key tool for understanding or investigating complex cybersecurity ideas, and
- Is both teachable and learnable over time and at increasing levels of depth and sophistication.

While the primary emphasis of each knowledge area is on development, protection and maintenance of security properties, some programs may choose to include the study of tools and techniques for circumventing protection mechanisms, such as a course on penetration testing. Due to the adversarial nature of cybersecurity, the study of *offensive* or *hacking* techniques is often a good way to develop stronger *defensive* cyber skills. All the knowledge areas include knowledge units that can be taught from both cyber-defense and cyber-offense perspectives.

Knowledge areas are *not* structured to be mutually exclusive. Accordingly, some knowledge units will have relevance to, and could be logically placed in, multiple knowledge areas. While the associated curricular guidance will differ, knowledge units are intentionally repeated in multiple knowledge areas (with cross-references). Since knowledge units do not necessarily correspond to courses or course units, cybersecurity courses will typically contain topics from multiple knowledge units. Therefore, placement of a knowledge unit under one knowledge area should not preclude its coverage in other knowledge areas.

3.2.2 Crosscutting Concepts

Crosscutting concepts help students explore connections among the knowledge areas, and are fundamental to an individual's ability to understand the knowledge area regardless of the disciplinary lens. These concepts "*provide an organizational schema for interrelating* *knowledge"*[12] into a coherent view of cybersecurity. The crosscutting concepts also reinforce the security mindset conveyed through each of the knowledge areas.

The thought model includes the following six crosscutting concepts:

- **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.
- **Systems Thinking.** A thinking process that considers the interplay between social and technical constraints to enable assured operations.

3.2.3 Disciplinary Lens

The disciplinary lens is the third dimension of the thought model. It represents the underlying computing discipline from which the cybersecurity program can be developed. The disciplinary lens drives the approach, depth of content, and learning outcomes resulting from the interplay among the topics, essential and crosscutting concepts. The thought model encompasses the current computing disciplines identified by the ACM: computer science, computer engineering, information systems, information technology, and software engineering.

The application of the crosscutting concept and/or the level of depth taught within each knowledge unit may differ depending upon the disciplinary lens. For instance, coverage of *Risk* in the context of *Data Security* may differ for students in a computer science cybersecurity program and those in an information systems cybersecurity program. The exemplars illustrate this interplay.

[12] U.S. National Research Council. 2013. *Next Generation Science Standards: For States, By States*. Washington, DC: The National Academies Press.

Chapter 4: Content of the Cybersecurity Curricular Framework

The curricular content was gathered and synthesized from a variety of sources including (in no particular order): ACM/IEEE CS2013; ACM/IEEE IT2017; U.S. National Security Agency and Department of Homeland Security Centers of Academic Excellence (CAE); $(ISC)^2$; workforce frameworks such as the U.S. National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NCWF); Global IT Skills Framework for the Information Age (SFIA); course exemplars sponsored by the Intel University Programs Office; the U.S. National Science Foundation; U.K. Government Communications Headquarters (GCHQ); industry sector working groups; and other sources provided by the stakeholder community.

The sections in this chapter provide an overview of the curricular content for each knowledge area. The table for each knowledge area lists the essentials, knowledge units and the topics within each knowledge unit. In many cases, specific curricular guidance on topic coverage has been included. To refine the knowledge units and topics, the JTF convened subject matter experts in Knowledge Area Working Groups (KAWGs). KAWG members are listed by knowledge area in Appendix A.

As described above, the essentials across the knowledge areas capture the cybersecurity proficiency that every student needs to achieve regardless of program focus. The essentials are listed within each KA section and are presented as a collective in Appendix B.

Note: Several of the knowledge units and topics in the knowledge areas are seemingly redundant. This is purposeful redundancy that serves both to permit specificity in the coverage in each specific knowledge area, and also to emphasize the importance of these essentials knowledge units and topics in the totality of the cybersecurity discipline knowledge domain.

Within the knowledge area tables are cross references to other knowledge area tables that contain important related information. Theses cross references are in the leftmost column under "Knowledge Units," and they are in italics within brackets [ ].

See Appendix C for an overview of the exemplars that map knowledge areas and knowledge units to different types of curricula. The curricular exemplars demonstrate how the curricula from specific institutions cover the knowledge area *essentials* and some subset of knowledge units. The exemplars are provided on the community engagement website (http://cybered.acm.org/) to show how the cybersecurity content can be organized in a variety of ways.

The information in the tables provides guidance for developers of an entire curriculum or a course syllabus. Those developers must instantiate the topics with specific material that their course is to cover. For example, the description/curricular guidance for the "Logical data access controls" topic in the "Access Control" knowledge unit of the "Data Security" knowledge area lists several types of controls, including access control lists, mandatory access controls, and so forth. A class on the security of mobile devices will have access controls for Android in its syllabus, even though that is not listed in the Description/Curricular Guidance column. The Android system does not provide attribute-based access control at the time this is written; therefore, the syllabus for this class would omit it at this time. Similarly, a syllabus on modern cryptography would include “Modes of operation for block ciphers” (a discussion/curricular guidance in the “Symmetric (private key) ciphers” topic of the knowledge unit “Cryptography” in the knowledge area “Data Security”) such as GCM even though the discussion/curricular guidance does not explicitly mention that mode. These two examples emphasize that the curricular guidance presents the topics a curriculum might include. The specific content of those topics is left to the curriculum developer because she knows the goals of the class and the needs of the students, and so can tailor how each topic is covered to meet those goals and needs.

4.1 Knowledge Area: Data Security

The Data Security knowledge area 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.

4.1.1 Knowledge Units and Topics

The following table lists the essentials, knowledge units, and topics of the Data Security knowledge area.

<table>
<tr><th colspan="3">DATA SECURITY</th></tr>
<tr><td colspan="3">Essentials
- Basic cryptography concepts,
- Digital forensics,
- End-to-end secure communications,
- Data integrity and authentication, and
- Information storage security.</td></tr>
<tr><td>Knowledge Units</td><td>Topics</td><td>Description/Curricular Guidance</td></tr>
<tr><td>Cryptography</td><td></td><td></td></tr>
<tr><td></td><td>Basic concepts</td><td>This topic covers basic concepts in cryptography to build the base for other sections in the knowledge unit. This topic includes:
● Encryption/decryption, sender authentication, data integrity, non-repudiation,
● Attack classification (ciphertext-only, known plaintext, chosen plaintext, chosen ciphertext),
● Secret key (symmetric), cryptography and public-key (asymmetric) cryptography,
● Information-theoretic security (one-time pad, Shannon Theorem), and
● Computational security.</td></tr>
<tr><td></td><td>Advanced concepts</td><td>This topic includes:
● Advanced protocols:</td></tr>
</table>

		o Zero-knowledge proofs, and protocols, o Secret sharing, o Commitment, o Oblivious transfer, o Secure multiparty computation, ● Advanced recent developments: fully homomorphic encryption, obfuscation, quantum cryptography, and KLJN scheme.
	Mathematical background	This topic is essential in understanding encryption algorithms. More advanced concepts may be included, if needed. This topic includes: ● Modular arithmetic, ● Fermat, Euler theorems, ● Primitive roots, discrete log problem, ● Primality testing, factoring large integers, ● Elliptic curves, lattices and hard lattice problems, ● Abstract algebra, finite fields, and ● Information theory.
	Historical ciphers	This topic includes the following and their current applications (if any): ● Shift cipher, affine cipher, substitution cipher, Vigenere cipher, ROT-13, and ● Hill cipher, Enigma machine, and others.
	Symmetric (private key) ciphers	This topic includes: ● B block ciphers and stream ciphers (pseudo-random permutations, pseudo-random generators), ● Feistel networks, Data Encryption Standard (DES), ● Advanced Encryption Standard (AES), ● Modes of operation for block ciphers, ● Differential attack, linear attack, and ● Stream ciphers, linear feedback shift registers, RC4.
	Asymmetric (public-key) ciphers	This topic includes: ● Theoretical concepts (Computational complexity, one-way trapdoor functions), ● Naive RSA, ● Weakness of Naive RSA, padded RSA, ● Diffie-Hellman protocol, ● El Gamal cipher, ● Other public-key ciphers, including Goldwasser-Micali, Rabin, Paillier, McEliece, and ● Elliptic curves ciphers.
Digital Forensics [*See also System Security KA for related content, p. 39.*]		

	Introduction	This topic includes: ● Definition, and ● Limits and types of tools (open source versus closed source).
	Legal Issues	This topic includes: ● Right to privacy, ● Fourth and Fifth Amendments, ● Protection of encryption keys under the Fifth Amendment, ● Types of legal authority (owner consent, search warrant, FISA, Title III (wiretap), abandonment, exigent circumstances, plain sight, etc.), ● Protection from legal processes (e.g., ISP subscriber information via subpoena, e-mail server transactional data from 2703(d) court order, full content via search warrant, etc.), ● Legal request for preservation of digital evidence (e.g., via 2703(f) preservation letter), and ● Affidavits, testimony and testifying,
	Digital forensic tools	This topic includes: ● Types, ● Artifact-focused versus all-in-one tools, ● Requirements, and ● Limitations.
	Investigatory process	This topic includes: ● Alerts, ● Identification of evidence, ● Collection and preservation of evidence, ● Timelines, reporting, chain of custody, and ● Authentication of evidence.
	Acquisition and preservation of evidence	This topic includes: ● Pull-the-plug versus triage, ● Write-blocking, ● Forensically-prepared destination media, ● Imaging procedures, ● Acquisition of volatile evidence, ● Live forensics analysis, and ● Chain of custody.
	Analysis of evidence	This topic focuses on knowledge (awareness the artifact exists), attributes (components and possible variations of the artifact), origin/cause (emphasis on why the artifact exists), discoverability (how the artifact is located/viewed with tools), relevance (significance in the context of the specific investigation). Includes: ● Sources of digital evidence, ● Deleted and undeleted files, temporary files, ● Metadata, ● Print spool files,

		● Slack space, ● Hibernation files, ● Windows registry, ● Browser history, ● Log files, ● File systems, ● File recovery, and ● File carving.
	Presentation of results	This topic includes: ● Timeline analysis, ● Attribution, ● Lay versus technical explanations, ● Executive summaries, ● Detailed reports, and ● Limitations.
	Authentication of evidence	This topic includes: ● Hashing algorithms (MD5, SHA-1, etc.), ● Hashing entire media vs individual files, and ● Pre-exam and post-exam verification hashing.
	Reporting, incident response and handling	This topic includes: ● Report structures, ● Incident detection and analysis, ● Containment, eradication and recovery, ● Post-incident activities, and ● Information sharing,
	Mobile forensics	This topic includes: ● Wireless technologies, ● Mobile device technology, ● Collection/Isolation of mobile device, ● Mobile operating systems (OS) and Apps, and ● Mobile artifacts.
Data Integrity and Authentication		
	Authentication strength	This topic includes: ● Multifactor authentication, ● Cryptographic tokens, ● Cryptographic devices, ● Biometric authentication, ● One-time passwords, and ● Knowledge-based authentication.
	Password attack techniques	This topic includes: ● Dictionary attack, ● Brute force attack, ● Rainbow table attack, ● Phishing and social engineering, ● Malware-based attack, ● Spidering, ● Off-line analysis, and ● Password cracking tools.

	Password storage techniques	This topic includes: ● Cryptographic hash functions (SHA-256, SHA-3, collision resistance), ● Salting, ● Iteration count, and ● Password-based key derivation.
	Data integrity	This topic includes: ● Message authentication codes (HMAC, CBC-MAC), ● Digital signatures, ● Authenticated encryption, and ● Hash trees.
Access Control		
	Physical data security	This topic includes: ● Data center security, including keyed access, man trips, key cards and video surveillance, ● Rack-level security, and ● Data destruction.
	Logical data access control	This topic includes: ● Access control lists, group policies, passwords, ● Discretionary Access Control (DAC), ● Mandatory Access Control (MAC), ● Role-based Access Control (RBAC), ● Attribute-based Access Control (ABAC), ● Rule-based Access Control (RAC), ● History-based Access Control (HBAC), ● Identity-based Access Control (IBAC), ● Organization-based Access Control (OrBAC), and ● Federated identities and access control.
	Secure architecture design	This topic includes: ● Principles of a security architecture, and ● Protection of information in computer systems.
	Data leak prevention techniques	This topic includes: ● Controlling authorized boundaries, ● Channels, ● Destinations, and ● Methods of data sharing.
Secure Communication Protocols		
	Application and transport layer protocols	This topic includes: ● HTTP, ● HTTPS, ● SSH, and ● SSL/TLS.
	Attacks on TLS	This topic includes: ● Downgrade attacks, ● Certificate forgery,

		● Implications of stolen root certificates, and ● Certificate transparency.
	Internet/Network layer	This topic includes IPsec and VPN.
	Privacy preserving protocols	This topic includes Mixnet, Tor, Off-the-record message, and Signal.
	Data link layer	This topic includes L2TP, PPP and RADIUS.
Cryptanalysis		
	Classical attacks	This topic includes: ● Brute-force attack, ● Frequency-based attacks, ● Attacks on the Enigma machine, and ● Birthday-paradox attack.
	Side-channel attacks	This topic includes: ● Timing attacks, ● Power-consumption attacks, and ● Differential fault analysis.
	Attacks against private-key ciphers	This topic includes: ● Differential attack, ● Linear attack, and ● Meet-in-the-middle attack.
	Attacks against public-key ciphers	This topic includes factoring algorithms (Pollard's p-1 and rho methods, quadratic sieve, and number field sieve).
	Algorithms for solving the Discrete Log Problem	This topic includes: ● Pohlig-Hellman, ● Baby Step/Giant Step, and ● Pollard's rho method.
	Attacks on RSA	This topic includes: ● Shared modulus, ● Small public exponent, and ● Partially exposed prime factors.
Data Privacy [*See also Human Security KA, p. 44, Organizational Security KA, p. 51, and Societal Security KA, p. 62, for related content.*]		
	Overview	This topic includes: ● Definitions (Brandeis, Solove), ● Legal (HIPAA, FERPA, GLBA), ● Data collection, ● Data aggregation, ● Data dissemination, ● Privacy invasions,

		● Social engineering, and ● Social media.
Information Storage Security		
	Disk and file encryption	This topic includes hardware-level versus software encryption.
	Data erasure	This topic includes: ● Overwriting, degaussing, ● Physical destruction methods, and ● Memory remanence.
	Data masking	For this topic, include the need and techniques for data masking. The following is a non-exhaustive list of subtopics to be covered: ● Data masking for testing, ● Data masking for obfuscation, and ● Data masking for privacy.
	Database security	This topic includes: ● Access/authentication, auditing, and ● App integration paradigms.
	Data security law	This topic introduces the legal aspects of data security, laws and policies that govern data (e.g., HIPAA). It also provides an introduction to other law-related topics in the Organizational Security knowledge area.

4.1.2 Essentials and Learning Outcomes

Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes. Typically, the learning outcomes lie within the *understanding* and *applying* levels in the Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms).

Essentials	Learning outcomes
Basic cryptography concepts	
	Describe the purpose of cryptography and list ways it is used in data communications.
	Describe the following terms: cipher, cryptanalysis, cryptographic algorithm, and cryptology, and describe the two basic methods (ciphers) for transforming plaintext in ciphertext.
	Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities.
	Discuss the dangers of inventing one's own cryptographic methods.
	Describe which cryptographic protocols, tools and techniques are appropriate for a given situation.

End-to-end secure communications [*See also* *Connection Security KA for related content, p. 32*.]	
	Explain the goals of end-to-end data security.
Digital forensics	
	Describe what a digital investigation is, the sources of digital evidence, and the limitations of forensics.
	Compare and contrast variety of forensics tools.
Data integrity and authentication	
	Explain the concepts of authentication, authorization, access control, and data integrity.
	Explain the various authentication techniques and their strengths and weaknesses.
	Explain the various possible attacks on passwords.
Data erasure	Describe the various techniques for data erasure.

4.2 Knowledge Area: Software Security

The Software Security knowledge area focuses on the development and use of software that reliably preserves the security properties of the information and systems it protects. The security of a system, and of the data it stores and manages, depends in large part on the security of its software. The security of software depends on how well the requirements match the needs that the software is to address, how well the software is designed, implemented, tested, and deployed and maintained. The documentation is critical for everyone to understand these considerations, and ethical considerations arise throughout the creation, deployment, use, and retirement of software.

The Software Security knowledge area addresses these security issues. The knowledge units within this knowledge area are comprised of fundamental principles and practices.

4.2.1 Knowledge Units and Topics

The following table lists the principles essentials, knowledge units, and topics of the Software Security knowledge area. These knowledge units have been validated by the Software Security Working Group using the Open Web Application Security Project (OWASP) Top 10 and the IEEE "Avoiding the Top 10 Software Security Design Flaws."

SOFTWARE SECURITY		
Essentials - Fundamental design principles including least privilege, open design, and abstraction, - Security requirements and their role in design, - Implementation issues, - Static and dynamic testing, - Configuring and patching, and - Ethics, especially in development, testing and vulnerability disclosure.		
Knowledge Units	**Topics**	**Description/Curricular Guidance**
Fundamental Principles [*See also Component Security KA for related content, p. 29*.]		This knowledge unit introduces the principles that underlie both design and implementation. The first five are restrictiveness principles, the next three are simplicity principles, and the rest are methodology principles.
	Least privilege	Software should be given only those privileges that it needs to complete its task.
	Fail-safe defaults	The initial state should be to deny access unless access is explicitly required. Then, unless software is given explicit access to an object, it should be denied access to that object and the protection state of the system should remain unchanged.
	Complete mediation	Software should validate every access to objects to ensure that the access is allowed.
	Separation	Software should not grant access to a resource, or take a security-relevant action, based on a single condition.
	Minimize trust	Software should check all inputs and the results of all security-relevant actions.
	Economy of mechanism	Security features of software should be as simple as possible.
	Minimize common mechanism	The sharing of resources should be reduced as much as possible.
	Least astonishment	Security features of software, and security mechanisms it implements, should be designed so that their operation is as logical and simple as possible.
	Open design	Security of software, and of what that software provides, should not depend on the secrecy of its design or implementation.

	Layering	Organize software in layers so that modules at a given layer interact only with modules in the layers immediately above and below it. This allows you to test the software one layer at a time, using either top-down or bottom-up techniques, and reduces the access points, enforcing the principle of separation.
	Abstraction	Hide the internals of each layer, making only the interfaces available; this enables you to change how a layer carries out its tasks without affecting components at other layers.
	Modularity	Design and implement the software as a collection of co-operating components (modules); indeed, each module interface is an abstraction.
	Complete linkage	Tie software security design and implementation to the security specifications for that software.
	Design for iteration	Plan the design in such a way that it can be changed, if needed. This minimizes the effects with respect to the security of changing the design if the specifications do not match an environment that the software is used in.
Design		This knowledge unit describes techniques for including security considerations throughout the design of software.
	Derivation of security requirements	Beginning with business, mission, or other objectives, determine what security requirements are necessary to succeed. These may also be derived, or changed, as the software evolves.
	Specification of security requirements	Translate the security requirements into a form that can be used (formal specification, informal specifications, specifications for testing).
	Software development lifecycle/Security development lifecycle	Include the following examples: waterfall model, agile development and security.
	Programming languages and type-safe languages	Discuss the problems that programming languages introduce, what type-safety does, and why it is important.
Implementation		This knowledge unit describes techniques for including security considerations throughout the implementation of software.
	Validating input and checking its representation	For this topic: ● Check bounds of buffers and values of integers to be sure they are in range, and ● Check inputs to make sure they are what is expected and will be processed/interpreted correctly.
	Using APIs correctly	For this topic: ● Ensure parameters and environments are

		validated and controlled so that the API enforces the security policy properly, and ● Check the results of using the API for problems.
	Using security features	For this topic: ● Use cryptographic randomness, and ● Properly restrict process privileges.
	Checking time and state relationships	For this topic: ● Check that the file acted upon is the one for which the relevant attributes are checked, and ● Check that processes run.
	Handling exceptions and errors properly	For this topic: ● Block or queue signals during signal processing, if necessary, and ● Determine what information should be given to the user, balancing usability with any need to hide some information, and how and to whom to report that information.
	Programming robustly	This topic is sometimes called secure or defensive programming. Curricular content should include: ● Only deallocate allocated memory, ● Initialize variables before use, and ● Don't rely on undefined behavior.
	Encapsulating structures and modules	This topic includes classes and other instantiations. Example: isolating processes.
	Taking environment into account	Example: don't put sensitive information in the source code.
Analysis and Testing [*See also Component Security KA for related content, p. 29.*]		This knowledge unit introduces testing considerations for validating that the software meets stated (and unstated) security requirements and specifications. Unstated requirements include those related to robustness in general.
	Static and dynamic analysis	This topic describes the different methods for each of these, includes how static and dynamic analysis work together, and the limits and benefits of each, as well as how to perform these types of analyses on very large software systems.
	Unit testing	This topic describes how to test component parts of the software, like modules.
	Integration testing	This topic describes how to test the software components as they are integrated
	Software testing	This topic describes how to test the software as a whole, and place unit and integration testing in a proper framework.
Deployment and		This knowledge unit discusses security

Maintenance		considerations in the use of software, and in its deployment, maintenance, and removal.
	Configuring	This topic covers how to set up the software system to make it function correctly.
	Patching and the vulnerability lifecycle	This topic includes managing vulnerability reports, fixing the vulnerabilities, testing the patch and patch distribution.
	Checking environment	This topic covers ensuring the environment matches the assumptions made in the software, and if not, how to handle the conflict
	DevOps	This topic combines development and operation, and the automation and monitoring of both.
	Decommissioning/Retiring	This topic describes what happens when the software is removed, and how to remove it without causing security problems.
Documentation		This knowledge unit describes how to introduce and include information about security considerations in configuration, use, and other aspects of using the software and maintaining it (including modifying it when needed).
	Installation documents	This topic includes installation and configuration documentation.
	User guides and manuals	This topic includes tutorials and cheat sheets (brief guides); these should emphasize any potential security problems the users can cause.
	Assurance documentation	This topic focuses on how correctness was established, and what *correctness* means here.
	Security documentation	This topic focuses on potential security problems, how to avoid them, and if they occur, what the effects might be and how to deal with them.
Ethics [*See also* *Organizational Security KA*, *p. 51, and* *Societal Security KA*, *p. 62, for related content.*]		This knowledge unit introduces ethical considerations in all of the above areas, so students will be able to reason about the consequences of security-related choices and effects.
	Ethical issues in software development	This topic covers code reuse (licensing), professional responsibility, codes of ethics such as the ACM/IEEE-CS Software Engineering Code of Ethics and Professional Practice.
	Social aspects of software development	This topic covers considerations of the effects of software under development, both when the software works properly and the consequences of poor or non-

		secure programming practices.
	Legal aspects of software development	This topic discusses the liability aspects of software, regulations; also compliance and issues related to it.
	Vulnerability disclosure	This topic covers how to disclose, to whom to disclose, and when to disclose ("responsible disclosure").
	What, when and why to test	This topic describes the ethical implications of testing, especially including corner cases.

4.2.2 Essentials and Learning Outcomes

Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes. Typically, the learning outcomes lie within the *understanding* and *applying* levels in the Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms).

Essentials	Learning outcomes
Fundamental Design Principles; Least Privilege, Open Design, and Abstraction	
	Discuss the implications of relying on open design or the secrecy of design for security.
	List the three principles of security.
	Describe why each principle is important to security.
	Identify the needed design principle.
Security requirements and the roles they play in design	
	Explain why security requirements are important.
	Identify common attack vectors.
	Describe the importance of writing secure and robust programs.
	Describe the concept of privacy including personally identifiable information.
Implementation issues	
	Explain why input validation and data sanitization are necessary.
	Explain the difference between pseudorandom numbers and random numbers.
	Differentiate between secure coding and patching and explain the advantage of using secure coding techniques.
	Describe a buffer overflow and why it is a potential security problem.
Static, dynamic analysis	
	Explain the difference between static and dynamic analysis.
	Discuss a problem that static analysis cannot reveal.
	Discuss a problem that dynamic analysis cannot reveal.
Configuring, patching	
	Discuss the need to update software to fix security vulnerabilities.
	Explain the need to test software after an update but before the patch is distributed.
	Explain the importance of correctly configuring software.

Ethics, especially in development, testing, and vulnerability disclosure	
	Explain the concept that because you can do it, it doesn't mean you should do it.
	Discuss the ethical issues in disclosing vulnerabilities.
	Discuss the ethics of thorough testing, especially corner cases.
	Identify the ethical effects and impacts of design decisions.

4.3 Knowledge Area: Component Security

The Component Security knowledge area focuses on the design, procurement, testing, analysis and maintenance of components integrated into larger systems.

The security of a system depends, in part, on the security of its components. The security of a component depends on how it is designed, fabricated, procured, tested, connected to other components, used and maintained. This knowledge area is primarily concerned with the security aspects of the design, fabrication, procurement, testing and analysis of components. Together with the Connection Security and System Security KAs, the Component Security KA addresses the security issues of connecting components and using them within larger systems.

4.3.1 Knowledge Units and Topics

The following table lists the essentials, knowledge units, and topics of the Component Security knowledge area.

COMPONENT SECURITY

Essentials
- Vulnerabilities of system components,
- Component lifecycle,
- Secure component design principles,
- Supply chain management security,
- Security testing, and
- Reverse engineering.

Knowledge Units	**Topics**	**Description/Curricula Guidance**
Component Design [*See also Software Security KA for related content, p. 23.*]		This knowledge unit introduces design principles and techniques which increase the security of components.
	Component design security	This topic covers threats to the security of component design artifacts (e.g., schematics, netlists, and masks) such as hardware Trojans, intellectual property piracy, reverse engineering, tampering,

		side-channel analysis and counterfeiting. It also introduces techniques for protecting components from unauthorized access and use.
	Principles of secure component design	This topic covers principles such as establishing a sound security policy, treating security as an integral part of system design, trusted computing platforms, chain of trust, reducing risk, layered security, simplicity of design, minimizing system elements to be trusted, and avoiding unnecessary security mechanisms.
	Component identification	This topic covers techniques such as watermarking, fingerprinting, metering, encrypted IDs, and physical unclonable functions for protecting components against intellectual property theft and ensuring component authenticity.
	Anti-reverse engineering techniques	This topic covers techniques such as design obfuscation and camouflaging for making component designs and implementations difficult to reverse engineer.
	Side-channel attack mitigation	This topic covers techniques for defending against side-channel attacks primarily targeted at cryptographic algorithms. Defensive techniques include leakage reduction, noise injection, frequent key updates, physical random functions, and secure scan chains.
	Anti-tamper technologies	This topic covers techniques for making components resistant to physical and electronic attacks including physical protection techniques, tamper evident systems and tamper responding systems.
Component Procurement		This knowledge unit describes techniques for ensuring that the security of system components is maintained throughout the procurement process.
	Supply chain risks	This topic describes security threats and risks to both hardware and software in component procurement.
	Supply chain security	This topic describes strategies such as physical security, split manufacturing, traceability, cargo screening and validation, and inspections to detect and prevent compromises of component security during the procurement process.
	Supplier vetting	This topic includes strategies such as supplier credentialing to establish trusted suppliers and transporters of components.
Component Testing [*See also Software Security KA for related content,*		This knowledge unit introduces unit testing techniques and describes tools and techniques used to test the security properties of a component.

p. 23.]		
	Principles of unit testing	This topic describes unit testing tools and techniques as distinguished from system-level testing.
	Security testing	This topic describes tools and techniques such as fuzz testing for testing the security properties of a component beyond its functional correctness.
Component Reverse Engineering		This knowledge unit describes techniques for discovering the design and functionality of a component with incomplete information.
	Design reverse engineering	This topic describes tools and techniques for discovering the design of a component at some level of abstraction.
	Hardware reverse engineering	This topic describes tools and techniques for discovering the functionality and other properties of a component's hardware, such as the functions of an integrated circuit.
	Software reverse engineering	This topic describes tools and techniques such as static and dynamic analysis for discovering the functionality and properties of a component's software.

4.3.2 Essentials and Learning Outcomes

Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes. Typically, the learning outcomes lie within the *understanding* and *applying* levels in the Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms).

Essentials	Learning outcomes
Vulnerabilities of system components	
	Explain how the security of a system's components might impact the security of the system.
	Describe ways in which the confidentiality of a component's design may be compromised.
	Describe ways to learn information about component's functionality with limited information about its design and implementation.
Component lifecycle	
	List the phases of a component's lifecycle.
Secure component design principles	List component design artifacts which may require protection.
	Give examples of several secure component design principles and explain how each protects the security of components.
	Describe several techniques for protecting the design elements of an integrated circuit.
Supply chain management	
	List common points of vulnerability in a component's supply chain.
	Describe security risks in a component supply chain.
	Describe ways to mitigate supply chain risks.
Security testing	
	Differentiate between unit and system testing.

	List several techniques for testing security properties of a component.
Reverse engineering	
	List reasons why someone would reverse engineer a component.
	Explain the difference between static and dynamic analysis in reverse engineering software.
	Describe a technique for reverse engineering the functionality of an integrated circuit.

4.4 Knowledge Area: Connection Security

The Connection Security knowledge area focuses on the security of the connections between components including both physical and logical connections.

It is critical that every cybersecurity professional have a basic knowledge of digital communications and networking. Connections are how components interact. Much of this material could be introduced through examples, and then abstracting to the essentials and introducing the appropriate vocabulary. Together with the Component Security and System Security KAs, the Connection Security KA addresses the security issues of connecting components and using them within larger systems.

4.4.1 Knowledge Units and Topics

The following table lists the essentials, knowledge units, and topics of the Connection Security knowledge area.

<table>
<tr><th colspan="3">CONNECTION SECURITY</th></tr>
<tr><td colspan="3">Essentials
- Systems, architecture, models, and standards,
- Physical component interfaces,
- Software component interfaces,
- Connection attacks, and
- Transmission attacks.</td></tr>
<tr><th>Knowledge Units</th><th>Topics</th><th>Description/Curricular Guidance</th></tr>
<tr><td>Physical Media</td><td></td><td>This knowledge unit introduces the concepts of physical signaling and transmission. These general concepts could be introduced through presenting the history of Ethernet protocols and 802.11 wireless. Starting with a coax broadcast domain and CSMA/CD, moving to hubs and then switches without changing the addressing and payload. The introduction of switching required simulating broadcast behavior to simulate the coax broadcast behavior. Wireless is a shared medium but physical characteristics of the medium required different collision avoidance mechanisms than coax.</td></tr>
<tr><td></td><td>Transmission in a medium</td><td>This topic covers signals in coax, twisted pair,</td></tr>
</table>

		optical fiber, and air.
	Shared and point-to-point media	This topic discusses the communication characteristic of the media.
	Sharing models	This topic describes the various schemes for sharing media between multiple clients. For example: 802.1 MAC addressing and PPP.
	Common technologies	This topic examines various implementations of the models covered above. IEEE 802.3 (Ethernet), IEEE 802.11 (Wi-Fi), IEEE 802.16 (fixed wireless broadband).
Physical Interfaces and Connectors		This knowledge unit describes the characteristics of connectors, their materials, and standards that define the characteristics of the connectors. Different materials have different characteristics and signal transmission capability. Even non-technical security people need to understand that optical fiber is different than twisted pair and that each has different standards and specific standard connectors.
	Hardware characteristics and materials	This topic introduces the connection characteristics of various media and the requirements for physical connections.
	Standards	This topic examines various standards for connectors.
	Common connectors	RJ 11, Rj 45, ST, SC, MTRJ, SFF ISA Buss, etc.
Hardware Architecture		This knowledge unit introduces the advantages and potential vulnerabilities of standard hardware architectures.
	Standard architectures	This topic should introduce the idea of standard architectures and the advantages of standardization. The history of PC motherboards could be used as an example showing the evolution from ISA through PCI and beyond. The ability for cards to add functionality without changing the base architecture is important. Adding Multiport Ethernet ports in a card allows a PC to become a router.
	Hardware interface standards	This topic introduces various hardware interface standards starting with IC package design, through busses such as ISA and PCI for integration platforms and on to networking standards like IEEE 802.3.
	Common architectures	This topic should examine the current technologies learners will face (CPU chips, PC motherboard, Ethernet standards).
Distributed Systems Architecture		This knowledge unit introduces the general concepts of distributed systems and how they are connected together. The Internet is not the only network and TCP/IP is not the only protocol for system

		interconnection. Each implementation has specific characteristics and different potential vulnerabilities. The focus of the curriculum should be on similarities, differences, and why design choices are made. Each architecture has advantages and disadvantages for particular use cases and each has particular vulnerabilities and strengths from a security perspective. One cannot assume that a mitigation strategy for the Internet will be appropriate for a supercomputer infrastructure.
	General concepts	This topic should start with the idea of a process in and operating system and then introduce the various architectures for running processes and enabling their communication. Symmetric multiprocessing and shared memory, network based with an interprocess communication model.
	World-wide-web	This topic covers the HTTP/HTTPS protocol and demonstrates how it is an example of a distributed processing standard.
	The Internet	This topic covers the evolution of the Internet as a distributed processing platform. Learners should be clear as to why the world-wide-web and the Internet are not equivalent.
	Protocols and layering	This topic covers the 7 layer OSI model along with the 5 layer Internet model and compares them as an example of encapsulation and layering to enable services that build on each other.
	High performance computing (supercomputers)	This topic introduces HPC and use cases that distinguish HPC from the standard Internet.
	Hypervisors and cloud computing implementations	This topic introduces the concepts of providing infrastructure as a service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS), and all of their relatives relevant to the learners should be covered.
	Vulnerabilities and example exploits	This topic examines the attack surfaces of the various distributed computing models emphasizing the fact that every interface introduces potential vulnerabilities. The hypervisor, virtual networking, physical network, and interprocess communication should all be covered.
Network Architecture		This knowledge unit introduces the concepts typically covered in a computer networking course. It provides the foundation for the more specialized KUs.
	General concepts	This topic should cover the ideas of nodes and edges with the names of the various topologies and the transmission characteristics of the topologies.
	Common architectures	This topic covers the IEEE 802 network architecture

		and how the various networks are named based on the physical characteristics (LANs, MANs, etc.).
	Forwarding	This topic covers packet forwarding in general. Since similar switching silicone is now used in routers and switches, and SDN treats forwarding separate from building the forwarding table, this is its own topic.
	Routing	This topic covers routing algorithms and explains how forwarding tables are built using graph analysis algorithms such as link-state and distance vector.
	Switching/Bridging	This topic covers learning algorithms and IEEE 802.1 bridging along with Spanning Tree Protocol and its relationship to routing. It is not currently clear how this topic will evolve with STP being replaced through the emergence of Trill and STP.
	Emerging trends	This topic covers emerging technologies and their impact as they emerge. Currently the impact of SDN and adding routing to layer 2 with enhanced learning bridges would be the content. This is evolving rapidly.
[*See also System Security KA for related content, p. 39*]	Virtualization and virtual hypervisor architecture	Virtualization has provided ways to design architecture using either native virtualization (type 1) or virtualization under the control of a host operating system (type 2).
Network Implementations		This knowledge unit explores specific technologies that implement the general concepts of networking. Network architecture concepts may be illustrated by specific implementations but it should be made clear that there are other possibilities. It should be emphasized that vulnerabilities are exploited in implementations. Often an architecture can be proven correct theoretically, but implemented in a way that has vulnerabilities. Also seams between technologies often open vulnerabilities. ARP poisoning is a perfect example of how a seam between technologies opens vulnerabilities.
	IEEE 802/ISO networks	This topic is a deep dive into the ISO standards. It is expected that this topic will be introduced other places.
	IETF networks and TCP/IP	This is a deep dive into the basic infrastructure of the Internet and TCP.
	Practical integration and glue protocols	This topic looks at the problem of integrating technologies through the implementation of what could be called interface shims or glue code. ARP is the obvious example. A mechanism was required to map the IP addresses of the IETF internetworking model to the MAC addresses of the underlying networks. ARP is the glue. Similarly, Infiniband needs a shim to carry IP traffic. Other examples

		abound.
	Vulnerabilities and example exploits	This topic should provide examples from the technologies important to the program. If ARP is chosen as an example, ARP poisoning as a MitM attach works well. USB and other serial connections could also provide examples.
Network Services		This knowledge unit explores different models used to implement connectivity between the consumer of a service and the provider of a service. Each topic can be explored at many levels with many examples (e.g., wireless issues surrounding biomedical devices). This area is broken out because the service models can be implemented in so many ways with so many different architectures. Remote procedure calls (RPC) are implemented over many different connection technologies varying from process-to-process in a single processor to across the Internet. The security concerns are different and the design tradeoffs change based on implementations and requirements.
	Concept of a service	This topic is a network-centric dive into one model of distributed computing. A service is a process that provides something to another process based on a request.
	Service models (client-server, peer-to-peer)	This topic is a network-centric look at how services are modelled. From a network perspective, the client initiates a connection and a server responds. With P2P either side can initiate the request.
	Service protocol concepts (IPC, APIs, IDLs)	This topic describes all of the ways components connect. Procedure calls, IPC requests, Interface Definition Languages with stub code, private protocols over a socket, everything.
	Common service communication architectures	This topic looks at specific services and how their protocols are implemented. Examples are SMTP, HTTP, SNMP, REST, CORBA, etc. Specialty connections such as wireless control of implanted medical devices can also be examined.
	Service virtualization	This topic covers service virtualization as a method to emulate the behavior of specific components such as cloud-based applications and service-oriented architecture.
	Vulnerabilities and example exploits	This topic looks at the vulnerabilities and exploits of client-server, peer-to-peer, and virtualization network services. Common service signatures are often used for vulnerability profiling.
Network Defense		This knowledge unit captures current concepts in network protection. It is likely that the vocabulary and technology will evolve significantly over time. The key ideas should include connection

		vulnerabilities like inserting a tap into a connector and enabling eavesdropping. All of these provide vulnerabilities that can be exploited for man-in-the-middle attacks. The idea of base-line capture and monitoring for deviations from the base needs to be covered as it applies in several of the specific topics.
	Network hardening	This topic covers ways to help the network defend itself from unauthorized access.
	Implementing IDS/IPS	This topic covers intrusion detection and intrusion prevention services. These services audit the network traffic.
	Implementing firewalls and virtual private networks (VPNs)	This topic covers the installation and use of firewalls and virtual private networks.
	Defense in depth	This topic introduces the idea that defenses must be layered.
	Honeypots and honeynets	This topic introduces the idea of providing intentionally vulnerable networks and devices in isolated networks so that they can be watched and analyzed as they are attacked.
	Network monitoring	This topic covers the tools and techniques for monitoring network devices and their associated logs.
	Network traffic analysis	This topic covers the tools and techniques for capturing and analyzing the packets flowing through the network. Research topic in this area include threat hunting and attack pattern detection.
	Minimizing exposure (attack surface and vectors)	This topic covers the tools and techniques for finding and mitigating vulnerabilities through looking at potential weaknesses.
	Network access control (internal and external)	This topic covers tools and techniques for limiting the flow of packets based upon rules for packet content. Examples include network admission control techniques; machine certificates; machine profiling techniques; probing with SNMP, DHCP, HTTP, DNS, LDAP, and NMAP.
	Perimeter networks (also known as demilitarized zones or DMZs) / Proxy Servers	This topic covers tools and techniques for implementing Defense in Depth using isolated networks and special servers.
	Network policy development and enforcement	This topic covers the creation of policies that provide guidance and requirements for the services provided by the network along with the measures to be used to see that the policies are followed.
	Network operational procedures	This topic discusses the creation of procedures that are used to operate the network.
	Network attacks (e.g., session	This topic covers the tools and techniques used to

	hijacking, man-in-the-middle)	test the network by actually attempting to exploit vulnerabilities.
	Threat hunting and machine learning	This topic covers how proactive threat hunting uses machine learning to detect patterns in attack vectors.

4.4.2 Essentials and Learning Outcomes

Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes. Typically, the learning outcomes lie within the *understanding* and *applying* levels in the Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms).

Essentials	Learning outcomes
Systems, architecture, models, and standards	
	Discuss the need for common models and architectures in order to describe systems.
	Describe a model of systems that consists of components and interfaces for connections.
	Explain why a component requires at least one interface.
	List several standards that define models consisting of systems of components and interfaces.
	Describe the components and interfaces of a networking standard provided.
Physical component interfaces	
	Explain why a hardware device is always modeled a physical component.
	List several examples of physical component interfaces with their associated vulnerabilities.
	Describe an exploit for a vulnerability of a physical interface provided.
Software component interfaces	
	Explain why every physical interface has a corresponding software component to provide a corresponding software interface.
	Explain how software components are organized to represent logical layers in a standard model.
	Discuss how the Internet 5 layer model can be viewed as software components and interfaces that represent levels of services encapsulated by lower-level services.
	Discuss how TCP/IP as a service is represented by different interfaces in different software systems.
Connection attacks	
	Explain how connection attacks can be understood in terms of attacks on software component interfaces.
	Describe how a specified standard interface could expose vulnerabilities in a software component that implements the interface.
	Describe how an implementation could protect itself from a

	specified vulnerability in a specified standard interface.
Transmission attacks [*See also* Data Security KA *for related content, p. 16.*]	
	Explain how transmission attacks are often implemented as attacks on components that provide the service of relaying information.
	Describe an attack on a specified node in a TCP/IP network given the description of a vulnerability.
	Explain why transmission attacks can often be viewed as connection attacks on network components (physical or software).

4.5 Knowledge Area: System Security

The System Security knowledge area focuses on the security aspects of systems that are composed of components and connections, and use software. Understanding the security of a system requires viewing it not only as a set of components and connections, but also as a complete unit in and of itself. This requires a holistic view of the system. Together with the Component Security and Connection Security KAs, the System Security KA addresses the security issues of connecting components and using them within larger systems

4.5.1 Knowledge Units and Topics

The following table lists the essentials, knowledge units, and topics of the System Security knowledge area.

SYSTEM SECURITY

Essentials

- Holistic approach,
- Security policy,
- Authentication,
- Access control,
- Monitoring,
- Recovery,
- Testing, and
- Documentation.

Knowledge Units	Topics	Description/Curricular Guidance
System Thinking		This knowledge unit introduces the student to thinking of the system as a whole, rather than simply a number of connected components.
	What is a system?	This topic discusses the definition of *system* and how it depends on context.
	What is systems engineering?	This topic focuses on the value of having good systems engineering artifacts in order to inform security risk management.

	Holistic approaches	This topic covers viewing the system as a whole rather than as simply a collection of interconnected components. For example, viewing the human, organizational and environmental considerations of the whole as opposed to viewing each individual component and connection and how they affect the view of risk.
	Security of general-purpose systems	This topic covers the security considerations of computing and of systems in general.
	Security of special-purposes systems	This topic covers security considerations derived from the purposes to which the system is put.
	Threat models	This topic covers what security problems can arise and how they might be realized, detected, and mitigated.
	Requirements analysis	This topic presents requirements derivation and validation throughout the system lifecycle, including in various methodologies such as the waterfall and agile development methodologies.
[*See also Software Security KA for related content, p. 23.*]	Fundamental principles	The Software Security knowledge area covers these principles in detail, but they also apply here.
	Development for testing	This topic covers designing systems for ease and effectiveness of testing.
System Management		This knowledge unit describes techniques for including security considerations throughout the management of the system.
	Policy models	This topic includes examples such as Bell-LaPadula, Clark-Wilson, Chinese Wall, and Clinical Information Systems Security.
	Policy composition	This topic covers restrictiveness.
	Use of automation	This topic includes data mining, machine learning and related techniques, and their benefits and limitations.
[*See also Software Security KA for related content, p. 23.*]	Patching and the vulnerability life cycle	This topic includes the security issues patching raises such as whether to patch a system, and patching a running system, as well as how to handle vulnerability reports.
	Operation	This topic includes security in operation, and the importance of usability considerations.
	Commissioning and decommissioning	This topic describes the security considerations when installing and removing a system.
	Insider threat	This topic includes examples of insider threats such as data exfiltration and sabotage, and covers countermeasures.

	Documentation	This topic covers security and assurance documentation as well as installation and user guides focused on the system itself.
	Systems and procedures	This topic discusses procedures that are used to manage systems.
System Access [*See also Human Security KA for related content, p. 44.*]		This knowledge unit introduces security considerations about controlling access to systems. It deals with the identification of entities, and confirmation of that identification to the desired level of granularity. Topics overlap with the Human Security knowledge area, but the focus here is on the system elements and not the human ones.
	Authentication methods	Authentication methods refers to human-to-system or system-to-system authentication; examples include passwords, biometrics, dongles, and single sign-on.
	Identity	How is identity represented to the system? This topic includes roles as well as names, etc.
System Control		This knowledge unit examines the security considerations involved in controlling the system itself. It includes detecting, compensating for, defending against, and preventing attacks.
[*See also Data Security KA for related content, p. 16.*]	Access control	This topic focuses on controlling access to resources, and the integrity of the controls, rather than their controlling access to data, which is covered in the Data Security knowledge area.
	Authorization models	This topic covers the management of authorization across many systems, and the distinction between authentication and authorization.
	Intrusion detection	This topic covers anomaly, misuse (rule-based, signature-based) and specification-based techniques.
	Attacks	This topic covers attack models (such as attack trees and graphs) and specific attacks.
	Defenses	This topic includes examples such as ASLR, IP hopping, and intrusion tolerance.
	Audit	This topic covers logging, log analysis, and relationship to intrusion detection.
	Malware	This topic includes examples such as computer viruses, worms, ransomware, and other forms of malware.
	Vulnerabilities models	This topic includes examples such as RISOS and PA; and enumerations such as CVE and CWE.
	Penetration testing	This topic covers the Flaw Hypothesis Methodology and other forms (ISSAF, OSSTMM, GISTA, PTES, etc.).

[*See also Data Security KA for related content, p. 16.]*	Forensics	This topic focuses on the system requirements for forensics**.**
	Recovery, resilience	This topic includes availability mechanisms.
System Retirement		This knowledge unit examines how retiring a system at or before its end of life may affect the security of other systems, or of the organization that used the system.
	Decommissioning	This topic examines how retiring a system at or before its end of life may affect the security of other systems, or of the organization that used the system. The student should understand the effects of removing a system, or components or connections within a system, upon the security of the system as a whole.
	Disposal	This topic includes wiping media and other forms of destruction to prevent sensitive information (such as PII) from being recovered.
System Testing [*See also Software Security KA, p. 23, and Component Security KA, p. 29, for related content.*]		This knowledge unit covers considerations of testing systems to ensure they meet security requirements.
	Validating requirements	This topic describes methodologies to show that requirements meet objectives.
	Validating composition of components	This topic covers how to test a system as a whole.
	Unit versus system testing	This topic covers how system testing differs from component and connection testing.
	Formal verification of systems	This topic covers languages, theorem provers, and hierarchical decomposition.
Common System Architectures		This knowledge unit applies the topics of this knowledge area to specific architectures that are, or are becoming, more common.
[*See also Connection Security KA for related content, p. 32.*]	Virtual machines	This topic covers hypervisors, virtualization of disks and memory, and the use of virtual machines in security.
	Industrial control systems	This topic includes SCADA.
	Internet of Things (IoT)	This topic includes examples such as refrigerators and sensors.
	Embedded systems	This topic includes examples such as systems in

		spacecraft, and systems used in other hostile environments.
	Mobile systems	This topic includes examples such as laptops and smartphones.
	Autonomous systems	This topic includes examples such as robots and UAVs that do not require human control.
	General-purpose systems	This topic includes examples such as desktops, laptops, and mainframes.

4.5.2 Essentials and Learning Outcomes

Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes. Typically, the learning outcomes lie within the *understanding* and *applying* levels in the Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms).

Essentials	Learning outcomes
Holistic approach	
	Explain the concepts of trust and trustworthiness.
	Explain what is meant by confidentiality, integrity, and availability.
	Explain what a security policy is, and its role in protecting data and resources.
Security policy [*See also Organizational Security KA for related content, p. 51.*]	
	Discuss the importance of a security policy.
	Explain why different sites have different security policies.
	Explain the relationship among a security group, system configuration, and procedures to maintain the security of the system.
Authentication	Explain three properties commonly used for authentication.
	Explain the importance of multifactor authentication.
	Explain the advantages of pass phrases over passwords.
Access control	
	Describe an access control list.
	Describe physical and logical access control, and compare and contrast them.
	Distinguish between authorization and authentication.
Monitoring	Discuss how intrusion detection systems contribute to security.
	Describe the limits of anti-malware software such as antivirus programs.

	Discuss uses of system monitoring.
Recovery	
	Explain what resilience is and identify an environment in which it is important.
	Discuss the basics of a disaster recovery plan.
	Explain why backups pose a potential security risk.
Testing	
	Describe what a penetration test is and why it is valuable.
	Discuss how to document a test that reveals a vulnerability.
	Discuss the importance of validating requirements.
Documentation	
	Discuss the importance of documenting proper installation and configuration of a system.
	Be able to write host and network intrusions documentation.
	Be able to explain the security implications of unclear or incomplete documentation of system operation.

4.6 Knowledge Area: Human Security

The Human Security knowledge area 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.

4.6.1 Knowledge Units and Topics

Humans have responsibility to ensure the confidentiality, integrity, and availability (CIA) of their organizational and personal computer systems, while that responsibility is dependent upon each of the Human Security knowledge units outlined below. The following table lists the essentials, knowledge units, and topics of the Human Security knowledge area.

HUMAN SECURITY		
Essentials - Identity management, - Social engineering, - Awareness and understanding, - Social behavioral privacy and security, and - Personal data privacy and security.		
Knowledge	**Topic**	**Description/Curricular Guidance**

Units		
Identity Management		
	Identification and authentication of people and devices	This topic provides an overview of various access control methods to demonstrate the benefits and challenges of each. Topics include an overview of Network Access Control (NAC), Identity Access Management (IAM), roles, multi-method identification and authentication systems, biometric authentication systems (including issues such as accuracy/FAR/FRR, resistance, privacy, etc.), as well as usability and tolerability of the methods.
	Physical and logical assets control	This topic covers various access controls to physical assets including system hardware, network assets, backup/storage devices, etc. Examples are Network Access Control (NAC), Identity Access Management (IAM), Rules-based Access Control (RAC), Roles-based Access Control (RBAC), inventory tracking methods, and identity creation methods (what type of user ID helps increase security with access control, for example, abc1234, first name and last name, first initial and last name).
	Identity as a Service (IaaS)	This topic cover identity management as a service (e.g., Cloud identity) brings forward issues such as the system being out of the user's control with no way to know what has happened to the information in the system, auditing access, ensuring compliance and flexibility to quickly revoke permissions.
	Third-party identity services	This topic provides an overview of the authentication infrastructure used to build, host, and manage third-party identity services. Topics include on-premises, cloud, centralized identity services/password management tools, end-point privilege management, etc.
	Access control attacks and mitigation measures	This topic provides an overview of various types of access control attacks to steal data or user credentials, and mitigation measures for combating them. Topics include password, dictionary, brute force, and spoofing attacks; multifactor authentication; strong password policy; secure password files; restrict access to systems; etc.
Social Engineering		
	Types of social engineering attacks	This topic provides an overview of the different ways that cybercriminals or malicious groups exploit weaknesses in organizations, systems, networks, and personal information used to enable a later cyberattack. Proposed topics included: phishing and spear phishing attacks, physical/impersonation, vishing (phone phishing), email compromise, and

		baiting.
	Psychology of social engineering attacks	This topic provides an overview of the psychological and behavioral factors related to individuals falling for social engineering attacks. Proposed topics include adversarial thinking, how emotional responses impact decision-making, cognitive biases of risks and rewards, and trust building.
	Misleading users	This topic provides an overview of message systems' and browsers' interfaces and/or user interaction that can be exploited to mislead users. Proposed topics include spoofing message senders, misleading URLs, how users judge and trust webpages and emails, as well as user behaviors with phishing and other browser warnings.
	Detection and mitigation of social engineering attacks	This topic provides scenario-based, hands-on activities via simulation or virtual tools to create an environment of various social engineering attacks. Hands-on experience on the use of tools and technical approaches to detect and/or mitigate different social engineering threats. Proposed tools such as email filtering, blacklist, security information and event management (SIEM) tools, and IDS/IPS.
Personal Compliance with Cybersecurity Rules/Policy/ Ethical Norms [*See also Societal Security KA for related content, p. 62.*]		
	System misuse and user misbehavior	This topic provides overview of intentional and unintentional system misuse, cyberbullying, cyber hacking, naive behavior, and ethical dilemmas related to system security decisions.
	Enforcement and rules of behavior	This topic provides an overview of methods and techniques to get people to follow the rules/policies/ethical norms (e.g., driving!). Topics include consequences for not following cybersecurity rules/policy/ethical norms, documentation and audit trail (evidence of compliance to prove that the cybersecurity rules/policy/ethical norms were followed), and knowledge of accountability for not following security rule/policy/ethical norms. Incentives to keep the job (especially after being educated and trained for the proper rules/policy/ethical norms, individuals are legally liable for not following the rules as an employee), and individuals may lose their identity/access in personal life due to a lack of adherence.

	Proper behavior under uncertainty	This topic provides an overview of the methods and techniques to adhere to when uncertain about how to respond to a cybersecurity situation. Topics include CyberIQ, intellectual adaptability, critical thinking, understanding the right versus wrong choices, how to make those choices under uncertainty, rational versus irrational thinking, ethical thinking/decisions, and behavior when there is no clear process to follow (reporting/point of contact/etc.), and human error mitigation.
Awareness and Understanding [*See also, Organizational Security KA for related content, p. 51*.]		
	Risk perception and communication	This topic covers how users perceive and respond to cybersecurity risks, cognitive biases in judging risks, metaphors for communicating particular security risks, and how to frame messages regarding risks. Definition of a mental model, how mental models impact user behavior, as well as common mental models (folk models) of cybersecurity and privacy.
	Cyber hygiene	This topic provides a discussion and activities focused on the individual responsibilities (not the organization) to protect and mitigate against cyberthreats and cyberattacks. Topics include password creation, password storage, mitigation tools, (i.e., anti-virus software), how to identify safe websites, identifying levels of privacy settings, etc.).
	Cybersecurity user education	Methods for educating end-users on various cybersecurity/privacy threats and behaviors. Topics include methods for raising user awareness (PreK-12, employees, public, etc.), delivery methods of cybersecurity education and training (e.g., posters, leaflets, computer-based training, gamification, communication styles, message framing, how to reach different audiences and user communities, individuals with disabilities and/or cognitive impairments), timing and reinforcement of education, as well as impact of training on users' knowledge and behaviors.
	Cyber vulnerabilities and threats awareness	This topic provides an overview of end-user-facing threats as well as Fear, Uncertainty, and Doubt (FUD). Proposed topics include warning signs of internal employee vulnerabilities and threats, awareness of identity theft, business email compromise, threat of free/open Wi-Fi networks, and malware, spyware, and ransomware.

Social and Behavioral Privacy [*See also* *Societal Security KA* *for related content, p. 62*.]		
	Social theories of privacy	This topic provides an overview of various theories of privacy from social psychology and social science, emphasizing privacy that involves interacting with other people as opposed to organizations. Proposed topics include privacy tradeoffs and risks in the social context, control and awareness of data consent, personal information monitoring, regulatory protections and concerns on maintaining social privacy.
	Social media privacy and security	This topic provides overview of privacy behaviors and concerns of users in protecting personal information when using social media. Proposed topics include users' online disclosure decisions and behaviors, personas and identity management, determining audience and social access controls, interface and coping mechanisms for managing privacy on various social media sites, challenges of managing time boundaries, as well as personal/workplace boundaries of social media.
Personal Data Privacy and Security [*See also* *Data Security KA*, *p. 16, and* *Organizational Security KA*, *p. 51, for related content*.]		
	Sensitive personal data (SPD)	This topic provides overview of the types of Personal Data (PD), including Personally Identifiable Information (PII), which are especially sensitive due to the risk that such information could be misused to significantly harm an individual in a financial, employment or social way. Proposed topics include examples of data elements of Sensitive Personal Data (SPD) (social security number, social insurance number or other government issued identification number such as a driver's license or passport number; bank account number; credit card numbers; health and medical information; biometric or genetic data, etc.), regulations governing the collection, use and distribution of SPD, and possibilities for

		inference of SPD.
	Personal tracking and digital footprint	Location tracking, Web traffic tracking, network tracking, personal device tracking, digital assistants recordings (Siri, Alexa, etc.). Topics include users' behaviors and concerns with each of these kinds of tracking, as well as current methods for limiting tracking and protecting privacy.
Usable Security and Privacy [*See also* *Organizational Security KA*, *p. 51, and* *Societal Security KA*, *p. 62, for related content*.]		
	Usability and user experience	Definition of usability and user experience, and the impact that usability (or lack thereof) has on the security and privacy of a system. Topics include examples of usability problems in traditional security systems such as authentication or encryption, usability and security tradeoffs in systems, methods for evaluating the usability of security and privacy systems.
	Human security factors	Students will be able to operate at the intersection of human factors, computer science, and the quality assurance area. This should include a strong core of computing and in-depth human factors and quality assurance. Topics include applied psychology in the context of adversarial thinking and security policies, security economics, regulatory environments, responsibility, liability, self-determination, impersonation, and fraud (e.g., phishing and spear phishing, trust, deception, resistance to biometric authentication and identity management).
	Policy awareness and understanding	This topic provides an overview of regulating policies (e.g., HIPAA, FERPA, PIIs) and the method or technique to take when a security situation arises. Topics include refresher training for policy updates, revisiting of existing threats, and knowledge tests to understand the policy when it comes to data protection. Due to the overlap in topics, also reference the knowledge units in the Societal Security and Organizational Security knowledge areas.
	Privacy policy	This topic provides an overview of privacy policies in social and localized variances. Jurisdictional variance in privacy policy definitions should be explored. The relationships between individuals, organizations, or governmental privacy policies

		should also be addressed from the users' perspective. Additional topics should include the impact of privacy policy on new tools/software, identifying a need for tools and techniques to be covered in most areas. Moreover, notifications of users of policy on how their data is used so they can make an informed choice as to whether to provide their information.
	Design guidance and implications	Guidelines include reducing user burden and decisions, providing secure defaults, reducing unintentional security and privacy errors, making threats along with risks contextual and concrete, as well as reducing technical language and jargon.

4.6.2 Essentials and Learning Outcomes

Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes. Typically, the learning outcomes lie within the *understanding* and *applying* levels in the Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms).

Essentials	Learning outcomes
Identity Management	
	Explain the difference between identification, authentication, and access authorization of people and devices.
	Discuss the importance of audit trails and logging in identification and authentication.
	Demonstrate the ability to implement the concept of least privilege and segregation of duties.
	Demonstrate the overall understanding of access control attacks and mitigation measures.
Social Engineering	
	Demonstrate overall understanding of the types of social engineering attacks, psychology of social engineering attacks, and misleading users.
	Demonstrate the ability to identify types of social engineering attacks.
	Demonstrate the ability to implement approaches for detection and mitigation of social engineering attacks.
Awareness and understanding	
	Discuss the importance of cyber hygiene, cybersecurity user education, as well as cyber vulnerabilities and threats awareness.
	Describe the major topics within Security Education, Training, and Awareness (SETA) programs.
	Discuss the importance of SETA as countermeasures.
	Discuss the importance of risk perception and communication in the context of mental models of cybersecurity and privacy.
Social behavioral privacy and security	
	Compare and contrast various theories of privacy from social

	psychology and social science.
	Describe the concepts of privacy tradeoffs and risks in the social context, control and awareness of data consent, personal information monitoring, regulatory protections and concerns on maintaining social privacy.
	Discuss the importance of social media privacy and security.
Personal data privacy and security	
	Discuss the importance of protection of Sensitive Personal Data (SPD) and Personally Identifiable Information (PII).
	Discuss the importance of regulations governing the collection, use and distribution of SPD, and possibilities for inference of SPD.
	Describe the concepts of personal tracking and digital footprint, while understanding the invasiveness of such tools in the context of privacy.

4.7 Knowledge Area: Organizational Security

The Organizational Security knowledge area focuses on protecting organizations from cybersecurity threats and managing risk to support the successful accomplishment of the organization's mission. Organizations have responsibility to meet the needs of many constituencies and those needs must inform each of these knowledge units.

4.7.1 Knowledge Units and Topics

Students should be able to identify the types of security laws, regulations, and standards within which an organization operates. A government organization has a set of security profiles while a corporate entity has other focuses. A security policy needs to fit the current organization and be able to grow with the organization. A security professional should understand current governances and how they convey compliances to their respective business verticals such as healthcare and Ecommerce.

The following table lists the essentials, knowledge units, and topics of the Organizational Security knowledge area. Due to the overlap in topics, reference the knowledge units in the Societal Security knowledge area.

<table>
<tr><th colspan="3">ORGANIZATIONAL SECURITY</th></tr>
<tr><td colspan="3">Essentials
- Risk management,
- Governance and policy,
- Laws, ethics, and compliance, and
- Strategy and planning.</td></tr>
<tr><th>Knowledge Units</th><th>Topic</th><th>Description/Curricular Guidance</th></tr>
<tr><td>Risk Management</td><td></td><td>Risk management is finding and controlling risks to organizational information assets.</td></tr>
</table>

	Risk identification	Asset identification is the cataloging of information assets in an organization, such as databases or hardware, to aid in the determination of risk should the assets be compromised or lost. Threats include any event leveraging a vulnerability that has the potential to cause loss or damage for the organization. Threat intelligence (threat modeling) is increasingly used by organizations to maintain awareness and reactive capacity for existing and emerging threats.
	Risk assessment and analysis	Risk analysis is the organizational process to determine and deal with possible accidental or intentional losses, and designing and implementing procedures to minimize the impact of these losses. This can also encompass Threat Analysis and Threat Intelligence.
	Insider threats	This topic covers malicious human behavioral factors that might cause harm as a result of a conscious violation of trust, or best-use, or inadvertent error. An *insider* is defined as any person with authorized access to an organization's resources including personnel, facilities, information, equipment, networks, and systems. An *insider threat* is defined as the risk that an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization. This can include theft of proprietary information and technology; damage to company facilities, systems, or equipment; actual or threatened harm to employees; or, other actions that would prevent the company from carrying out its normal business practices This topic covers motive-means-opportunity behaviors: motivation and discipline factors, accountability, awareness and quality control. The FBI has developed materials including indicators useful in identifying potential insider threat risks.
	Risk measurement and evaluation models and methodologies	Risk models are used to explain how assets encounter risk. In addition, there a number of industry-accepted methodologies to measure, evaluate, and communicate risk to stakeholders. This topic includes both quantitative and qualitative approaches to risk assessment, application of models and methods for various business contexts (e.g., HIPAA for healthcare facilities). Tools of interest might include the Cyber Resilience Review self-assessment, Cybersecurity Evaluation Tool (CSET) as well as Security Risk Assessment tool from HSS.
	Risk control	*Risk control* is defined as the act of lessening the consequences of a cyber event, and as a result lessening

		the amount of risk. Each approach should include the means to communicate risk to decision makers including the *residual risk*. Topics covered should include assessment and ranking of risk and the Avoid, Reduce, Transfer, Accept categories. Curricular content should include widely-used risk control methodologies that are available for exposure and practice.
Security Governance & Policy [*See also Societal Security KA for related content, p. 62.*]		Each organization addresses its operating environment, internal and external, through policy and governance. Governance is the responsibility of the senior management of an organization to assure the effective implementation of strategic planning, risk management, and regulatory compliance usually by means of comprehensive managerial policy, plans, programs, and budgetary controls so as to secure the information of the organization. The implementation of security governance and policy should be framed within global, national, and local laws, regulations and standards. This knowledge unit focuses on an understanding of the security policy development cycle, from initial research to implementation and maintenance as well as giving exposure to real-world examples of security policies and practices.
	Organizational context	Many factors influence how security is operationalized in organizations. These contexts are critical when designing a curriculum and should inform the entire process. This topic covers how internal versus external contextual differences have a major impact on the coverage of policy, regulation, and statute (or jurisdiction). Also, location- or country-specific issues and concerns should be evaluated. Applicable standards and guidelines for compliance to industry/sector should also be evaluated. The variance between governments versus private organizations is a factor as is the need to include international aspects including but not limited to import/export restrictions. Further, there is significant difference between organizations in various business vertical industry segments such as energy versus agriculture.
[*See also Data Security KA, p. 16, Human Security KA, p. 44, and Societal Security KA, p. 62, for*	Privacy	Privacy is a concept with cultural and national variations in its definition. At its core, privacy is based on the right to be forgotten, and various levels of choice and consent for the collection, use, and distribution of an individual's information. This topic addresses social and localized variances in

related content.]		privacy. Jurisdictional variance in privacy definitions should be explored. The relationships between individuals, organizations, or governmental privacy requirements should also be addressed. The impact of privacy settings in new tools/software, identifying a need for tools and techniques to be covered in most areas. Additional consideration should be given to privacy in the context of consumer protection and health care regulations. Organizations with international engagement must consider variances in privacy laws, regulations, and standards across the jurisdictions in which they operate.
[*See also Societal Security KA for related content, p. 62*.]	Laws, ethics, and compliance	Laws, regulations, standards as well as ethical values are derived from the social context and how organizations meet requirements to comply with them. This topic includes how laws and technology intersect in the context of the judicial structures that are present – international, national and local – as organizations safeguard information systems from cyberattacks. Ethical instruction should also be an element. Professional codes of conduct and ethical standards should be addressed. Compliance efforts should include those efforts to conform to laws, regulations, and standards, and to include breach notification requirements by state, national, and international governing authorities. Examples of international laws and standards include GDPR and ISO/IEC 27000 et al. National laws of importance for U.S. organizations include HIPAA, Sarbanes-Oxley, GLBA, etc.
	Security governance	The principles of corporate governance are applicable to the information security function. Governance is the responsibility of the senior management of an organization to assure the effective implementation of strategic planning, risk management, and regulatory compliance usually by means of comprehensive managerial policy, plans, programs, and budgetary controls to secure the information of the organization. This topic should frame the implementation of security governance and policy within global, national, and local laws, regulations and standards, and programs of instruction should seek to convey the concepts with clarity and sound examples.
	Executive and board level communication	Delivering information to executives and external decision makers is a critical skill for information security leaders. This topic includes communication skills that are taught and practiced with rehearsals that include critical analysis and meaningful feedback.

	Managerial policy	Organizational guidelines that dictate certain behavior within an organization. This topic content should seeks to convey the concepts with clarity and sound examples including security program policy, issue-specific policy and system-specific policy as per NIST SP 800-12 Rev 1. This should also cover an understanding of the security policy development cycle, from initial research to implementation and maintenance, as well as giving exposure to real-world examples of security policies and practices.
Analytical Tools		This knowledge unit is a set of techniques using data analytics to recognize, block, divert, and respond to cyberattacks. Monitoring real-time network activities enables agile decision making, detection of suspected malicious activities, utilization of real-time visualization dashboard and employment of a set of hardware and software to manage such detected suspicious activities.
	Performance measurements (metrics)	A process of designing, implementing, and managing the use of specific measurements to determine the effectiveness of the overall security program. Built on metrics, a term used to describe any detailed statistical analysis technique on performance, but now commonly synonymous with performance measurement. Curricular content should include approaches and techniques to define and evaluate the utility of performance measurements should be explained to students.
	Data analytics	Data analytics is a set of techniques used to manipulate (often) large volumes of data to recognize, block, divert, and respond to cyberattacks. Monitoring real-time network activities enables agile decision making, detection of suspected malicious activities, utilization of a real-time visualization dashboard, and employment of a set of hardware and software to manage such detected suspicious activities. This topic includes definitions; the differences between security control and security analytic software and tools; the type and classifications of analytic tools and techniques (with examples such as OpenSOC); collect, filter, integrate and link diverse types of security event information; how security analytics tools work; the relationship between analytic software and tools and forensics; differences between forensic tools and analytic tool; network forensics (to include packet analysis, tools, Windows, Linux, UNIX, Mobile); differences between cyber forensics (social media for example) and network forensics.
	Security intelligence	Collection, analysis, and dissemination of security

		information including but not limited to threats and adversary capabilities. In this topic, tools and techniques should be explored to include data collection and aggregation, data mining, data analytics, statistical analysis. Examples of sources for security intelligence include SIEM for internal data, and public and private intelligence services for external data. Dissemination includes an understanding of the Information Sharing and Analysis Center approach as well organizations like InfraGard.
Systems Administration		System administration works behind the scenes to configure, operate, maintain, and troubleshoot the technical system infrastructure that supports much of modern life. Prerequisite knowledge: Basic understanding of computer systems (Windows/Linux), networks (OSI Model), software, and database (Oracle/SQL).
	Operating system administration	This topic covers the upkeep, reliable operation, configuration, and troubleshooting of technical systems, especially multi-user systems and servers. This topic includes but not be limited to account management, disk administrations, system process administration, system task automation, performance monitoring, optimization, administration of tools for security and backup of disks and process.
	Database system administration	This topic covers managing and maintaining databases by utilizing available and applicable management system software. This topic includes but not be limited to installation and configuration of database servers, creation and manipulation of schemas, tables, indexes, views, constraints, stored procedures, functions, user account creation and administration, and tools for database backup and recovery. Coverage should include the data storage technologies in wide use as well as emerging data management technologies.
	Network administration	Network administration relates to installation, and supporting various network system architectures (LANs, WANs, MANs, intranets, extranets, perimeter networks [DMZs], etc.), and other data communication systems. This topic includes but is not limited to the OSI Model, securing of network traffic, and tools for configuration of services.
[*See also Data Security KA*, *p. 16*, *Human Security KA*,	Cloud administration	Cloud administration refers to the upkeep and reliable access to a dynamic pool of configurable remote resources (e.g., networks, servers, storage, applications and services) that can be rapidly configured, provisioned

p. 44, and Societal Security KA, p. 62, for related content.]		and released with minimal oversight. This topic includes but is not limited to configuring and deploying applications and users in cloud infrastructures, analyzing performance, resource scaling, availability of cloud platforms, identifying security and privacy issues and mitigating risks.
	Cyber-physical system administration	Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components. CPS administration refers to installation and upkeep by ensuring safety, capability, adaptability, scalability, resiliency, security, and usability. This topic includes but is not limited to the architecture of cyber-physical systems, underlying communication standards (Zigbee), middleware, service-oriented architecture, tools supporting real-time control and application of real-world examples (power grid, nuclear facility, IoT, SCADA).
	System hardening	This topic covers securing a system by finding and remediating risks. This may include hardening or securing configuration, system software, firmware, and application. This topic includes but is not limited to identifying risks, threats, and vulnerabilities in commonly used systems (operating systems, database systems, networks); defining and administering procedures and practices to safeguard against threats; hardening through suitable tools (firewall, anti-virus, IDS, honeypot).
	Availability	Sound system operation requires all systems sustain targeted levels of availability by having their current state recoverable from failure through redundancy and backup and recovery. This topic includes but is not limited to identifying key assets and administering tools to have validated system backup and recovery.
Cybersecurity Planning		
	Strategic planning	The process of defining an organization's cybersecurity strategy – or direction – and determining the actions needed and resources to be allocated in order to implement such a strategy. This topic covers concepts such as determining the current organization's position; performing Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis; developing a strategy that fulfills the mission, values, and vision of the organization; determining long-term objectives; selecting key performance indicators

		(KPIs) to track progress; allocating the necessary budget; rolling out the strategy to the organization; and updating and adapting yearly.
[*See also* Data Security KA, *p. 16,* Human Security KA, *p. 44, and* Societal Security KA, *p. 62, for related content.*]	Operational and tactical management	The organization ability to securely operate organizational technical infrastructure. This topic includes a discussion of data protection and privacy by default and design, and cover basic concepts, issues, and techniques for efficient and effective operations. Special emphasis is placed on process improvement and supply chain management. Topics include operations strategy; tactical strategy; product and service design; process design and analysis; capacity planning; lean production systems; materials and inventory management; quality management and six sigma; project management; and supply chain management.
Business Continuity, Disaster Recovery, and Incident Management		Description of the role disaster recovery (DR) plays within business continuity (BC). BC planning includes contingency planning, incident response, emergency response, and backup and recovery efforts of an organization to ensure the availability of critical resources during an emergency situation while the disaster recovery refers to the recovery of the systems in the event of a disaster. Continuity of organizations in the wake of major events is also a component. This topic includes creation and use of the IR/DR/BP BC plans, organization of the plans, occasions to review/rewrite plans, examination of sanitized plans, opportunities should be given for students to write case-based or actual plans to gain some experience.
	Incident response	Incident response (IR) refers to the actions taken by senior management to specify the organization's processes and procedures to anticipate, detect, and mitigate the effects of an incident. This topic includes the creation and use of the IR plans, organization of the plans, occasions to review/rewrite plans, and examination of sanitized plans. Opportunities should be given for students to write case-based or actual plans to gain some experience.
	Disaster recovery	Disaster recovery (DR) refers to the actions taken by senior management to specify the organization's efforts in preparation for and recovery from a disaster. Specifically, DR refers to the recovery of the systems in the event of a disaster. This topic includes the creation and use of the DR plans, organization of the plans, occasions to review/rewrite plans, and examination of sanitized plans. Opportunities should be given for students to write case-based or

		actual plans to gain some experience.
	Business continuity	Business continuity refers to the actions taken by senior management to specify the organization's efforts if a disaster renders the organization's primary operating location unusable. Business continuity (BC) planning includes contingency planning, incident response, emergency response, and backup and recovery efforts of an organization to ensure the availability of critical resources during an emergency situation. Continuity of organizations in the wake of major events is also a component. Curricular content should include the creation and use of the BC plans, organization of the plans, occasions to review/rewrite plans, and examination of sanitized plans. Opportunities should be given for students to write case-based or actual plans to gain some experience.
Security Program Management		
	Project management	Project management is the application of knowledge, skills, tools, and techniques to project activities to meet the project requirements. This topic includes project integration; project scope management; project time and cost management; quality management; human resource considerations; communications; risk management; and procurement management.
	Resource management	Resource management is the efficient and effective deployment and allocation of an organization's resources when and where they are needed. Such resources may include financial resources, inventory, human skills, production resources, or information technology. This topic explains and develops current practices in resource management, specifically in the context of projects typical of cybersecurity.
	Security metrics	Metrics, often described as measures, are effective tools to discern the effectiveness of the components of their security programs and drive actions taken to improve a security program. This topic includes the elements of security metrics, and how to design, develop, validate and organize them. The use of metrics in various contexts should be included such as: ● Use of security metrics in decision making, ● Use of security metrics in strategic, tactical and operational planning, and ● Use of security metrics in security program evaluation, audition, and performance.

	Quality assurance and quality control	Quality assurance (QA) and quality control (QC) are methods used to prevent mistakes which might impact the character of a deliverable such as a software system; control specifically refers to methods used to increase the quality of these systems. This topic explains and develop current practices in QA/QC, specifically in the context of projects typical of cybersecurity.
Personnel Security		
[*See also Human Security KA*, *p. 44, for related content.*]	Security awareness, training and education	This topic covers the avoidance and/or proper use of Fear Uncertainty, and Doubt (FUD) as a tool for awareness. This topic includes physical security; desktop security; password security; wireless networks; security phishing; file sharing and copyright; browsing; encryption; insider threat; international travel; social networking and social engineering.
	Security hiring practices	The practices, governed by policies, used by organizations to recruit, hire and train employees across the organization. This topic includes the principles of this topic, and students should gain experience with a review of fictional resumes, fictional background checks, fictional acted-out interview techniques, fingerprint analysis results, and financial review.
	Security termination practices	The practices, governed by policies, used by organizations to terminate employees across the organization including assigned asset recovery, removal of credentials and proactive prevention of data exfiltration. This topic includes the principles of this topic, and students should gain experience with practice sets and simulations.
	Third-party security	Those practices of firms to manage the risks from contractors, consultants and the staff of key business partners. This topic includes the principles of this topic, and students should gain experience with practice sets and simulations.
	Security in review processes	Those practices of firms to manage the periodic review of staff members. This topic includes the principles of this topic, and students should gain experience with practice sets and simulations.

[*See also* *Data Security KA*, *p. 16*, *Human Security KA*, *p. 44, and* *Societal Security KA*, *p. 62, for related content.*]	Special issue in privacy of employee personal information	Those practices of firms to secure the personal information of employees and other stakeholders. This topic includes the principles of this topic, and students should gain experience with practice sets and simulations.
Security Operations		This knowledge unit covers efforts to enhance the security of the origin and traceability of sourced system components, such as externally produced hardware or software.
	Security convergence	The merging of management accountability in the areas of corporate (physical) security, corporate risk management, computer security, network security, and InfoSec has been an observed phenomenon in practice in many moderate and large organizations. This topic includes emerging examples of convergence in practice, which can be a useful outlet for classroom discussion of emerging topics.
	Global security operations centers (GSOCs)	Optimized processes can add value to broad organizational operations centers that intersect physical security and cybersecurity. This topic covers how correlating global attacks with local compliance measures is a necessity at times. How does an attack in Malaysia affect business functions in Colorado? GSOC functions need to have clear communications of the identified attack as well as the identified region of attack and the region of origin. A GSOC will need to be able to completely determine the type of attack, the profile and where it originated to be able to disseminate that information to the other security operation centers.

4.7.2 Essentials and Learning Outcomes

Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes. Typically, the learning outcomes lie within the *understanding* and *applying* levels in the Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms).

Essentials	Learning outcomes
Risk Management	
	Describe risk management and its role in the organization.
	Describe risk management techniques to identify and prioritize risk factors for information assets and how risk is assessed.
	Discuss the strategy options used to treat risk and be prepared to select from them when given background information.

	Describe popular methodologies used in the industry to manage risk.
Governance and policy	
	Discuss the importance, benefits, and desired outcomes of cybersecurity governance and how such a program would be implemented.
	Describe information security policy and its role in a successful information security program.
	Describe the major types of information security policy and the major components of each.
	Explain what is necessary to develop, implement, and maintain effective policy and what consequences the organization may face if it does not do so.
Laws, ethics, and compliance	
	Differentiate between law and ethics.
	Describe why ethical codes of conduct are important to cybersecurity professionals and their organizations.
	Identify significant national and international laws that relate to cybersecurity.
	Explain how organizations achieve compliance with national and international laws and regulations, and specific industry standards.
Strategy and planning	
	Explain strategic organizational planning for cybersecurity and its relationship to organization-wide and IT strategic planning.
	Identify the key organizational stakeholders and their roles.
	Describe the principal components of cybersecurity system implementation planning.

4.8 Knowledge Area: Societal Security

The Societal Security knowledge area focuses on aspects of cybersecurity that broadly impact society as a whole for better or for worse. Cybercrime, law, ethics, policy, privacy and their relation to each other are the key concepts of this knowledge area. The threat of cybercrime across the global society is incredibly serious and growing. Laws, ethics and policies are vital to the security of corporate and government secrets and assets, as well as to the protection of individual privacy and identity.

4.8.1 Knowledge Units and Topics

The following table lists the essentials, knowledge units, and topics of the Societal Security knowledge area.

SOCIETAL SECURITY
Essentials - Cybercrime,

- Cyber law,
- Cyber ethics,
- Cyber policy, and
- Privacy.

Knowledge Units	Topics	Description/Curricular
Cybercrime		This knowledge unit aims to provide students with an understanding of the scope, cost and legal environment relating to cyber-based intellectual property theft. This includes both national and international environments. Students should have a strong understanding of the basic property-rights legislation and be able to help others navigate the complex legal and ethical world of intellectual property rights.
	Cybercriminal behavior	Behavior that attacks individual / companies compute device or computer infrastructure to perform malicious activities, such as spreading viruses, data theft, and identity theft..
	Cyber terrorism	Activities in cyberspace geared to generate societal fear and uncertainty.
	Cybercriminal investigations	Methods for investigating cyberattacks by criminals, cybercriminal organizations, overseas adversaries, and terrorists.
	Economics of cybercrime	• Risks of cybercrime are too low, while the rewards are too high, and • The use of (untraceable) cryptocurrencies in committing cybercrimes online and in the Dark Web (bitcoin).
Cyber Law [*See also* *Organizational Security KA* *for related content, p. 51.*]		This knowledge unit aims to provide students with a broad understanding of the current legal environment in relation to cyberspace. This includes both domestic and international laws as well as the application of jurisdictional boundaries in cyber-based legal cases. Students should have a strong understanding of current applicable legislation and a strong background in the formation of these legal tools.
	Constitutional foundations of cyber law	This topic included: • Executive power, • Legislative power, • First amendment, • Fourth amendment, and • Tenth amendment.
	Intellectual property related to cybersecurity	This topic covers: • The scope, cost and legal environment relating to cyber-based intellectual property theft, • The specific content will be driven by the country of focus. In the U.S., cover Section 1201 of the Digital Millennium

		Copyright Act, and ● Anti–circumvention - Digital Millennium Copyright Act (DMCA 1201).
[*See also Data Security KA, p. 16, Human Security KA, p. 44, and Organizational Security KA, p. 51, for related content.*]	Privacy laws	This topic includes: ● Laws governing Internet privacy, ● Laws governing social media privacy, and ● Electronic surveillance laws, such as Wiretap Act, Stored Communications Act, and Pen Register Act.
	Data security law	This topic includes: ● Section 5 of the U.S. Federal Trade Commission, ● State data security laws, ● State data-breach notification laws, ● Health Insurance Portability Accountability Act (HIPAA), ● Gramm Leach Bliley Act (GLBA), and ● Information sharing through US-CERT, Cybersecurity Act of 2015.
	Computer hacking laws	This topic covers: ● U.S. Federal computer crime laws, such as Computer Fraud and Abuse Act. Most computer hacking offenses are prosecuted under the Computer Fraud and Abuse Act in the U.S. ● International framework and cooperation needed to prosecute overseas hackers.
	Digital evidence	This topic includes: ● Forensically-sound collection of digital evidence, and ● Preserving the chain of custody.
	Digital contracts	This topic includes: ● Distinction among browse-wrap, click-wrap, and shrink-wrap agreements. ● The Electronic Signatures in Global and International Commerce Act (ESGICA) of 2000; digital contracts and electronic signatures are just as legal and enforceable as traditional paper contracts signed in ink.
	Multinational conventions (accords)	This topic covers jurisdictional limitations of multinational accords. Examples: Budapest Convention on cybercrime and the G-7 Cybersecurity Accord on financial institutions.
[*See also Data Security KA, p 16, Human Security KA, p. 44, and Organizational Security KA, p. 51, for related content.*]	Cross-border privacy and data security laws	Requirements of the General Data Protection Regulation (GDPR). Privacy Shield agreement between countries, such as the United States and the United Kingdom, allowing the transfer of personal data.
Cyber Ethics [*See also*		This knowledge unit aims to give students a foundation for both understanding and applying moral reasoning models to addressing current and emerging ethical dilemmas on an

Organizational Security KA, p. 51, and Software Security KA, p. 23, for related content.]		individual and group (professional) level. It also sensitizes students to debates about whether ethics in computing is a unique problem or part of a larger phenomenon, and helps students to think through how their nation's culture and legal framework impact their understanding and implementation of ethics in their society.
	Defining ethics	For this topic: ● Compare and contrast major ethical stances, including virtue ethics, utilitarian ethics and deontological ethics. ● Apply the three different ethical stances in thinking through the ethical consequences of a particular problem or action.
	Professional ethics and codes of conduct	This topic covers: ● Major professional societies, such as ACM, IEEE-CS, AIS, and $(ISC)^{2,}$ ● Professional responsibility, and ● Ethical responsibility in relation to surveillance.
	Ethics and equity/diversity	For this topic: ● Describe the ways in which decision-making algorithms may over-represent or underrepresent majority and minority groups in society, and ● Analyze the ways in which algorithms may implicitly include social, gender and class biases.
	Ethics and law	For this topic: ● Understand that ethical practices and legal codes may not always align exactly, ● Ethical practices can be seen as universal while laws may be nation- or region-specific (e.g., European Union), and ● Laws may evolve but ethical values can be described as unchanging.
	Autonomy/robot ethics	For this topic: ● Define autonomous decision-making, ● Define artificial intelligence and describe ethical dilemmas presented by the use or employment of artificial intelligence (AI), ● Describe legislative advances which have defined personhood and digital personhood, and ● Describe the conflict created by legal notions of responsibility and the use of unmanned or autonomous decision-making programs.
	Ethics and conflict	This topic includes: ● Just War Principles to cyberspace in relation to conflict initiation, behaviors in conflict, conflict cessation/post conflict situation; ● Ethical problems created in conduct of cyber espionage; ● Norm and rule violation as it relates to cyber terrorism.
	Ethical hacking	This topic includes: ● Ethical penetration testing versus unethical hacking, ● Ethical hacking principles and conditions, and

		● Distinguish among nuisance hacking, activist hacking, criminal hacking, and acts of war.
	Ethical frameworks and normative theories	Common ethical frameworks and normative theories related to cybersecurity from individual and societal perspectives.
Cyber Policy [*See also* *Organizational Security KA* *for related content, p. 51*.]		The Cyber Policy knowledge unit is intended to help students understand and analyze cyber issues as they relate to the national interest generally, and to national (and national security) policy more specifically. Students are expected to gain an understanding of questions relating to the use of cyber as an instrument of war, and to distinguish between the uses of cyber as such an instrument and the possibility of cyberwar itself occurring. Students will be given an opportunity to grapple with questions regarding how the use of cyber can be signaled to other countries, as well as the challenges associated with its deterrence. Students are also expected to grasp the historical trends that have made cyber important to national policy and the development of a national cyber policy architecture. Students will be expected to demonstrate original thinking about how cyber affects the national interest, including economic, and the policy implications for national policy arising from cyber.
	International cyber policy	This topic includes: ● International cyber policy challenges, ● International Cyber Policy Oversight Act of 2015, and ● Department of State international cyberspace policy strategy.
	U.S. federal cyber policy	This topic includes: ● Federal Information Security Modernization Act, an update to the Federal Government's cybersecurity policies and guidance; ● Relationship to the nation's critical infrastructure; and ● Managing risk at a national level.
	Global impact	This topic covers: ● Effects of cybersecurity on the international system generally and on international security specifically. ● How cyber has become and will continue to become an instrument of power, and how this power might change the balance of power between stronger and weaker countries. ● Global governance of cyber. Also examine the possibilities of the development of normative behavior related to the use of cyber. ● Effects of cyber on the global economy.
	Cybersecurity policy and national security	This topic covers: ● How a country defines its cybersecurity policy, doctrine and execution responsibility, including national cybersecurity policy, architecture, signals and narratives, and coercion and brandishing; and ● A nation's cybersecurity messaging; how it signals its intentions to gain other nation's attention and cooperation.

	National economic implications of cybersecurity	This topic covers: ● The cost of cybersecurity to a nation, ● The losses and gains of cybersecurity to a nation, and ● The investment to keep a nation protected from cyberthreats and cyberattacks.
	New adjacencies to diplomacy	This topic includes: ● The "delicate dance" of cyber diplomacy, and ● Aspects of cybersecurity that have become part of the relationships between countries, including the covert collection of information alongside the practice of diplomacy, and the covert application of cyberforce in cyberspace and physical space.
Privacy [*See also Human Security KA, p. 44, Organizational Security KA, p. 51, and Data Security KA, p. 16, for related content.*]		This knowledge unit is intended to provide students with an understanding of privacy and its related challenges. Students are expected to understand the tradeoffs of sharing and protecting sensitive information; and how domestic and international privacy rights impact a company's responsibility for collecting, storing and handling personal data. Students will gain an understanding of privacy-enhancing technologies and security application, which can include the concepts of appropriate use, as well as protection of information.
	Defining privacy	For this topic: ● Apply operational definitions of privacy, ● Identify different privacy goals, e.g., confidentiality of communications and privacy of metadata, and ● Identifying privacy tradeoffs – increasing privacy can have risks (e.g., the use of Tor could make someone a target for increased government scrutiny in some parts of the world).
	Privacy rights	For this topic: ● Describe informed consent conditions in relation to personal data collection and sharing, ● Recognize national privacy rights in the existence of privacy rights, and ● Demonstrate familiarity with the debate about the universal human right to privacy.
	Safeguarding privacy	For this topic: ● List cyber-hygiene steps to safeguard personal privacy, ● List privacy-enhancing technologies and their use and the properties that they do and do not provide (i.e., Tor, encryption), ● Describe conditions for ethical and lawful use of privacy enhancing technologies, ● Describe steps in carrying out a privacy impact assessment, ● Describe the role of the data trustee, ● Describe legislation related to data localization practices, ● Demonstrate an understanding difference between privacy rights and privacy-enhancing capability – operationalizing privacy, and

		• Discuss the dynamic impact of metadata and big data on privacy.
	Privacy norms and attitudes	This topic includes: • Privacy calculus theory and models, and • Cultural differences in the existence of privacy norms and boundaries.
	Privacy breaches	This topic covers the role of corporations in protecting data and addressing circumstances when data privacy is compromised.
	Privacy in societies	This topic includes: • Privacy rights and threats to privacy related to public figures, • Differential surveillance and its risks; challenges for smart cities, and • Harm matrix for cybersecurity surveillance.

4.8.2 Essentials and Learning Outcomes

Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes. Typically, the learning outcomes lie within the *understanding* and *applying* levels in the Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms).

Essentials	Learning outcomes
Cybercrime	
	Discuss various motives for cybercrime behavior.
	Summarize terror activities in cyberspace geared toward generating societal fear and certainty.
	Describe methods for investigating both domestic and international crimes.
	Explain why preserving the chain of digital evidence is necessary in prosecuting cybercrimes.
Cyber law	
	Describe the constitutional foundations of cyber law.
	Describe international data security and computer hacking laws.
	Interpret intellectual property laws related to security.
	Summarize laws governing online privacy.
Cyber ethics	
	Distinguish among virtue ethics, utilitarian ethics and deontological ethics.
	Paraphrase professional ethics and codes of conduct from prominent professional societies, such as ACM, IEEE-CS, AIS and $(ISC)^2$.

	Describe ways in which decision-making algorithms could over-represent or under-represent majority and minority groups in society.
Cyber policy	
	Describe major international public policy positions and the impact they have on organizations and individuals.
	Summarize nation-specific cybersecurity public policy with respect to the protection of sensitive information and protection of critical infrastructure.
	Explain global impact of cybersecurity to culture including areas such as the economy, social issues, policy and laws.
Privacy	
	Describe the concept of privacy including the societal definition of what constitutes personally private information and the tradeoffs between individual privacy and security.
	Summarize the tradeoff between the rights to privacy by the individual versus the needs of society.
	Describe the common practices and technologies used to safeguard personal privacy.

Chapter 5: Industry Perspectives on Cybersecurity

The field of cybersecurity is in its formative stages of development and is experiencing growing pains as the need for a structured discipline is recognized throughout industry. While the field has grown in past decades, defining cybersecurity as a stand-alone discipline has been frequently discounted or overlooked as a critical success factor for developing the cadre of professionals needed across government and industry to secure their systems. Today, there is a general consensus that addressing cybersecurity challenges must be a priority for nations and businesses alike, and the need for a structured discipline is clear.

While programs to expand the cybersecurity workforce have seen some success, global workforce gaps – estimated to reach 1.8 million in 2022 ((ISC)2, 2017), are growing[13]. Unfortunately, although jobs are and will be available, finding qualified people to fill them is often difficult. Students graduating from technical programs such as information technology or computer science often lack the specific cybersecurity knowledge and skills needed to fit within an industry or government environment. Students graduating from non-technical programs often receive only surface level coverage of important cybersecurity concepts and thus lack the depth of understanding of cybersecurity concepts necessary to apply their knowledge and skill in the operational environment.

5.1 The Technical – Business Skills Continuum

Many of the solutions to the cybersecurity problem are technical, but they also require that individuals and organizations implement policy and program activities to make intended control systems function properly. There does exist a continuum of skillsets within the discipline of cybersecurity ranging from the highly technical (areas like cryptography and network defense) to the highly managerial (areas like planning, policy development and regulatory compliance). Regardless of where one is positioned within the cybersecurity workforce, each graduate of a cybersecurity program will need a combination of skills from areas across this broad continuum and should possess both the technical skills and the business acumen to effectively participate in the problem solving, analysis, and project management activities necessary to implement cybersecurity solutions.

Non-technical (sometimes called *soft*) skills are vital to the success of cybersecurity professionals. The ability to work in a team, communicate technical topics to non-technical audiences, successfully argue for resource allocations, hone situational awareness, and operate within disparate organizational cultures are just a few of these skills. The U.S. Chief Human Capital Officers Council (CHCO), among other bodies, has developed a list of non-technical competencies pertinent to the cybersecurity workforce. The list includes: accountability, attention to detail, resilience, conflict management, reasoning, verbal and written communication, and teamwork. The full list of competencies is available in the Competency Model for Cybersecurity[14]. Professional

[13] Global Information Security Workforce Study is available here: https://iamcybersafe.org/gisws/
[14] U.S. Chief Human Capital Officers Council Competency Model for Cybersecurity is available here: https://www.chcoc.gov/content/competency-model-cybersecurity

associations such as $(ISC)^2$, ISACA and CompTIA also provide recommendations for non-technical skills required for cybersecurity professionals.

5.2 Career Focus

As students prepare for their future career, an important consideration is their ability to be able to transition from an academic environment to a career within a corporation, organization, academic institution, or even an entrepreneurial environment. One can appreciate what a difficult transition this can be if an individual has not received the proper mix of cybersecurity-related technical and soft skills exposure during their academic career. Many contributors to this report have identified the critical need in meeting cybersecurity workforce needs for coming years both at their specific companies and in the broader business community.

Adaptability, the ability to adjust easily to different environmental conditions and situational contexts, is an especially important personality trait for individuals working within the field of cybersecurity. Cybersecurity professionals will find the ability to learn new technologies and embrace change to be of considerable importance in years to come. Georgia Nugent states, "It's a horrible irony that at the very moment the world has become more complex, we're encouraging our young people to be highly specialized in one task. We are doing a disservice to young people by telling them that life is a straight path. The liberal arts are still relevant because they prepare students to be flexible and adaptable to changing circumstances."[15] The cybersecurity industry has historically appealed to individuals who thrive in this environment of constant change.

In addition to focusing on the industry and gaining valuable work experience while attending a college, it is important that students nearing graduation are ready for important interviews by structuring their resumes into a format that highlights their technology background. What distinguishes a technical resume from a standard one is the emphasis on attributes such as specific technical skill sets and industry certifications. Monster.com, a leading job board and career site, is a good source for examples of how to create a technical resume.[16]

Being able to handle a successful interview is a career skill that is essential for students to practice and master in the course of their academic studies. It is as important as learning basic technical subjects. If students are unable to handle the rigors of a career interview, their academic GPA and various scholastic achievements will fail them in achieving the desired goal of a useful cybersecurity education—to graduate and secure a position that can lead to career fulfillment and growth.

A cybersecurity advisory board can help academic programs provide students with important networking within the broader cybersecurity industry and the specific employment options in cybersecurity that will also help them to perform successfully in the interviewing process. Often, advisory boards act as mentors to students, giving them valuable feedback on their resumes and academic background. They often aid and encourage students to work in internships, the value of which is also a topic for

[15] Reference: https://www.fastcompany.com/3034947/the-future-of-work/why-top-tech-ceos-want-employees-with-liberal-arts-degrees
[16] Monster.com website: http://monster.com

discussion. Additionally, the importance of non-technical skills and getting along in a team environment are all components of good networking. To continue and advance in one's career in the future, the ability to network and find career opportunities will become a very important skill.

5.3 Linking Cybersecurity Curriculum to Professional Practice

Cybersecurity practices refers to the combination of knowledge and skills required to perform in the field. Practices are a critical consideration in cybersecurity education. The CSEC thought model links the academic curriculum to professional practice through the use of application areas. The application areas provide an organizing structure to combine curricular content, professional development and training opportunities, and professional certifications.

5.3.1 Application Areas

Application areas serve as an organizing framework to identify competency levels for each practice. The application areas help to define the depth of coverage needed for each core idea. In addition, application areas provide a bridge between the thought model and a specific workforce framework.

The seven application areas included are:

- **Public Policy.** Executive managers at the level of CEO or board of directors; legislators who will pass laws affecting the development, deployment, and use of information technology; regulators who will regulate those things; and other public and private officials will develop a *de facto* public policy. These people must understand how those laws, regulations, and requirements affect the use of the systems, how people interact with them and with the regulating authorities, how compliance checking is done, and what risks the public policy both controls and introduces. They must understand the basics of design because the design of a system, and the process in which the organization uses it, affects the way compliance is implemented and tested. This leads to the need to understand what a computing system can, and (perhaps more importantly) cannot, do. This also means they must understand the cost of security, in budgetary and human terms.
- **Procurement.** Those who procure information technology, and who hire the people who will work with it, must understand how the systems and the hires fit into the goals of the organization in general, and the particular goals of the projects for which the procurement and hiring is undertaken. This requires an understanding both of business continuity and risk management, the latter so the technology and people are chosen to minimize risk, to make risk as easy as possible to manage, or (ideally) both. The implication of these is to know what is required of people, systems, infrastructure, procedures, and processes to provide the desired level and assurance of security.
- **Management.** Management refers to both systems and people within an organization of some type. Both internal policies and external policies (regulations, laws, etc.) affect management. Managers must understand compliance and business continuity issues to ensure that the systems and people they manage meet the needs of the organization and governmental and other

regulators. As they must ensure that people using their systems are authorized to, and know whom those people are, they must be well versed in identity and authorization management. Changes to the systems require that they understand the goals of testing and whether the manner in which the tests are conducted speak to those goals. Finally, they must be prepared to deal with the results of attacks, by understanding both how to manage the incidents and how the incident will affect the organization. Thus, they must have a basic understanding of both incident management and accident recovery.

- **Research.** Researchers in academia, industry, and government who study security should know the basics of access control, confidentiality (including the basic principles and use of cryptography), integrity, and availability. Beyond that, the specifics of what they should know depends upon their area of research, and any specific goals of that research. For example, a researcher studying network security should understand how the networks are used in practice in order to understand how their operation affects the parameters of her research; it is probably unnecessary to understand the proof of the HRU theorem and the associated results. But someone studying foundational aspects (such as undecidability) needs to know the HRU theorem and related results, and not the details of network operations.
- **Software Development.** Software must meet requirements, which are often controlled by laws, regulations, business plans, and organizational factors. Developers muse ensure their software is designed to meet these requirements, or the requirements are changes to what the software can satisfy. Then their implementations must satisfy the design and be robust (secure programming), which includes the proper handling of exceptions and errors. This includes taking into account the environment in which the software will operate. They must know how to validate their claims by testing the software. Finally, they must be able to set the environment in which the software will run to that which their design and implementation assumes; and if this cannot be done, they must document this in their installation guides, and (ideally) display appropriate messages during the installation of the software.
- **IT Security Operations.** Similarly, operations must preserve the security of the system. As *security* is defined by a set of requirements, the system administrators, system security officers, and other information security personnel must understand how to translate requirements into procedures and configurations. They must be able to design and implement security enclaves and infrastructures to this end, for example to ensure that identity and authorization management systems are installed, initialized, configured, and connected properly. They will need to know how to test the systems, infrastructure, and procedures, and analyze the results. Finally, the operations personnel must understand system maintenance under both normal conditions (patching and upgrading, for example) and abnormal conditions (incident handling and response, for example).
- **Enterprise Architecture.** Enterprise architecture refers to the systems, infrastructure, operations, and management of all information technology throughout an enterprise. This requires elements from all other applications areas.

> Policy drives the architecture; the design of the architecture drives procurement, management, and operations. The architecture also affects much of the software, for example that needed to run the infrastructure. Therefore, the enterprise architects must understand the policy, procurement, management and operations application areas, as well as elements from the area of software development.

5.3.2 Training and Certifications

In the field of cybersecurity, knowledge acquisition and skill development at all post-secondary levels occurs in both formal higher education settings and in the professional development, training, and certification space. Academic program developers should identify and connect with training providers in order to identify opportunities for collaboration.

5.4 Workforce Frameworks

Within the context of the larger economic environment, workforce development initiatives are often driven by workforce frameworks that provide an organizing structure for the various job roles; education, training and professional development requirements; and career pathways. In the field of cybersecurity, nations have begun to develop workforce frameworks to outline skill requirements and support workforce development initiatives. For instance, the U.S. National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NCWF)[17] is being developed as a comprehensive resource to describe cybersecurity work. In Singapore, the National Cybersecurity Strategy calls for the development of a professional cybersecurity workforce through industry-oriented curricula at institutions of higher education, clear career pathways, and specific frameworks such as the Data Protection Competency Framework (DPCF) for data protection officers to ensure that they have the requisite skills, competencies and certifications required to effectively perform their duties[18]. In the United Kingdom, the National Cyber Security Strategy outlines how the UK government will support the development of a robust cybersecurity workforce[19]. These national strategies are illustrative of how governments around the world are developing workforce frameworks to support the growing need for cybersecurity professionals.

5.4.1 NCWF Implementation Roadmaps

In in order to effectively meet workforce demands, it is important for academic institutions to link the curricular recommendations offered in this volume with the relevant workforce framework. As an example of how to make this connection, the community engagement website (http://cybered.acm.org) provides instructions on a mapping procedure and sample roadmaps that link specific NCWF work role knowledge and skill requirements to the CSEC Curricular Guidance. Figure 5 shows how the roadmaps will link the curricular guidance and the workforce framework.

---

[17] NICE Cybersecurity Workforce Framework: https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice/nice-cybersecurity

[18] Singapore Cybersecurity Strategy: https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

[19] HM Government National Cyber Security strategy 2016-2021: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

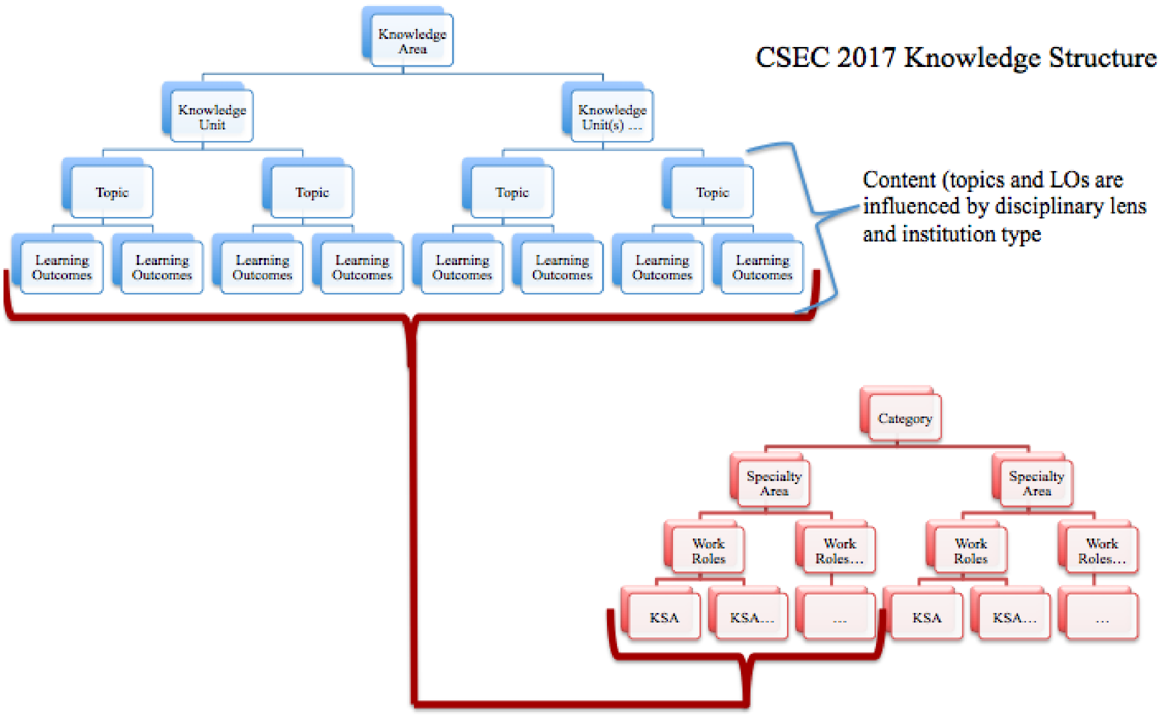


Figure 5. Linking the CSEC thought model and workforce frameworks.

An overview of the roadmap components is shown below in Figure 6. The first set of sample roadmaps will link the CSEC curricular guidance to the NCWF foundational Knowledge, Skills, and Abilities (KSA) requirements of the six specialty areas within the Oversee and Govern (OV) category[20].

In the CSEC thought model, foundational knowledge is identified as essential cybersecurity concepts. Essential cybersecurity concepts should be introduced early and reinforced throughout any cybersecurity program. Essential concepts introduce students to basic cybersecurity concepts and terms, the threat environment, common vulnerabilities, and fundamentals of information assurance.

As described above, the essential concepts are explicitly identified in each of the eight knowledge areas. These concepts may appear within the knowledge area body of knowledge as separate knowledge units, as topics within specific knowledge units, or as aggregates of topics across knowledge units. The essential concepts across all knowledge areas are provided in Appendix B.

Taken together, the essential concepts across all of the knowledge areas comprise the minimum required content for any cybersecurity program.

Each course roadmap will:

[20] NCWF categories and associated requirements are available here:: https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice/nice-cybersecurity

1. Provide a rationale for knowledge and its importance for the specific work role.
2. Identify and describe relevant courses and course modules.
3. Outline strategies for obtaining the knowledge when specific courses are not available or accessible within the institution.
4. Highlight challenges (and associated strategies to overcome them) to following the suggested course of study.

Figure 6. Roadmap components for coursework.

5.4.2 Overview

The KSA rationale provides a frame of reference for students embarking on the course of study. It explains the relationship between the knowledge and the specific work role.

5.4.3 Relevant Courses

The central portion of the roadmap will be the identification of relevant courses and a description of needed course content. Because relevant courses are spread through the university in a variety of schools and in a variety of formats, it is critical to include specific content in this section, not simply a listing of course titles. This section of the roadmaps also includes strategies for independent study courses and other customizable options.

5.4.4 KSA Acquisition Strategies

Colleges and universities often have programs and courses housed across multiple university academic units. In addition, some relevant content may be accessible through activities that are external to the formal course structure. As a result, it can be challenging for students (and their faculty advisors) to identify the most effective knowledge acquisition strategies. The roadmaps will assist in this navigational effort.

Taken together, the roadmap elements provide a comprehensive planning document for both students and faculty members by:

- Identifying the content and depth of knowledge of cybersecurity principles needed for the optimal development of the specific OV work roles.

- Delineating knowledge and skills-based learning, both brick-and-mortar (traditional classroom) and online from various resources within and outside of George Washington University, with the goal of providing a range of choices that meet the individual needs of the student and the expectation that knowledge acquisition strategies may continue on a largely part-time basis within and outside of a formal degree program.
- Identifying opportunities for students to engage in cohort experiences within and across programs that aid in the development of a multidisciplinary understanding and application of cybersecurity principles.
- Utilizing the multidisciplinary resources and educators across the university, which is home to several undergraduate and graduate programs focusing on cybersecurity, legal and policy practice relating to cybersecurity, and leadership/executive training relating to cybersecurity.
- Identifying special experiential learning opportunities – beyond a typical classroom experience – that will be included in the roadmaps; including simulations and/or tabletop exercises and special guest speakers (available both online and in the physical classroom). These will include opportunities to learn together with technical specialty areas with the objective of improving communication between OV and various technical skills language – i.e., becoming conversant in a different cybersecurity language and lexicon so participants will be better prepared to lead.

5.4.5 Challenges

Roadmaps represent the ideal plan of study. However, implementing the roadmaps within the context of the university structure, even when that context has been explicitly considered in the development process, can be challenging. This section of the roadmaps outlines specific challenges and suggests strategies to overcome them.

- Courses with relevant knowledge are spread throughout the university and students are not easily able to design customized courses of study
- Meeting course prerequisites can be an additional challenge when moving between schools
- Identifying and tracking extracurricular learning opportunities

Members of the international community are encouraged to develop and share course, curricular, and workforce exemplars; and workforce framework road maps through the community engagement website. This site, http://cybered.acm.org will be regularly updated and will serve as the foundation of the global community of practice that links cybersecurity educators and stakeholders in a continuous development process.

[End of CSEC v. 1.0]

References

- ACM Committee on Professional Ethics. ACM Code of Ethics and Professional Conduct (The Code): https://ethics.acm.org/
- ACM Europe Policy Committee. Advancing Cybersecurity Research and Education in Europe: Major Drivers of Growth in the Digital Landscape: https://www.acm.org/binaries/content/assets/public-policy/2016_euacm_cybersecurity_white_paper.pdf
- ACM CSEC Community Engagement: http://cybered.acm.org *(coming soon).*
- ACM Curriculum Committee on Computer Science. 1968. Curriculum 68: Recommendations for Academic Programs in Computer Science. *Comm. ACM* 11, 3 (Mar. 1968), 151-197
- ACM Curricula Recommendations: https://www.acm.org/education/curricula-recommendations
- Anderson, L. W., & Krathwohl, D. R. (2001). *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives*. New York: Longman
- Arce, I., K. Clark-Fisher, N. Daswani, J. DelGrosso, D. Dhillon, C. Kern,….West, J. (2015). Avoiding the Top 10 Software Security Design Flaws. Retrieved from https://www.computer.org/cms/CYBSI/docs/Top-10-Flaws.pdf
- Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC): http://aisnet.org/group/SIGSEC
- *Bloom's Revised Taxonomy*. Committee for Computing Education in Community Colleges (CCECC). Retrieved from: http://ccecc.acm.org/assessment/blooms
- *Competency Model for Cybersecurity*. (2011). U.S. Chief Human Capital Officers Council. Retrieved from: https://www.chcoc.gov/content/competency-model-cybersecurity
- *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science (CS2013)*. (2013). Retrieved from https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf or http://dx.doi.org/10.1145/2534860
- *Curricula Recommendations.* Association for Computing Machinery (ACM). Retrieved from http://acm.org/education/curricula-recommendations
- Cyber Education Project (CEP): http://cybereducationproject.org/about/
- Cybersecurity Education Curricula 2017 (CSEC 2017): http://csec2017.org
- Dictionary.com: http://www.dictionary.com/browse/adaptable
- *Global Information Security Workforce Study.* (2017). Center for Cyber Safety and Education. Retrieved from: https://iamcybersafe.org/gisws/
- Grand, Joe. "Practical Secure Hardware Design for Emedded Systems." *Proceedings of the 2004 embedded systems conference.* Vol. 23. 2004. (USED). Retrieved from http://www.grandideastudio.com/wp-content/uploads/secure_embed_paper.pdf
- *Guide to the Systems Engineering Body of Knowledge (SEBok*) v.1.9 (November 17, 2017). Retrieved from: http://sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK)

- HM Government National Cyber Security strategy 2016-2021: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
- Hu, Vincent C., Rick Kuhn, and Dylan Yaga. (2017). "Verification and Test Methods for Access Control Policies/Models." *NIST Special Publication 800-192*. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-192.pdf
- IEEE Computer Society: https://www.computer.org/
- *Information Technology Curricula 2017: Curriculum Guidelines for Baccaluaureate Degree Programs in Information Technology*. (2017) ACM/IEEE-CS. Retrieved from: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/it2017.pdf
- Intel University Programs Office: https://www.intel.com/content/www/us/en/education/highered/higher-ed-overview.html
- International Security Education Workshop (ISEW) was co-located with the Colloquium for Information Systems Security Education (CISSE), and sponsored by the Intel Corporation, the National Science Foundation (NSF), and the Institute for Information and Infrastructure Protection (I3P) at the George Washington University (GW): Report available at http://csec2018.org
- *ISO/IEC 27002:2013 Information Technology – Security techniques – Code of practice for information security controls.* (2013). International Organization for Standardization (ISO). Retrieved from https://www.iso.org/standard/54533.html
- Monster.com: http://monster.com
- Morgan, Steve. (July 28, 2015). Cybersecurity job market to suffer severe workforce shortage. *CSO Online*. Retrieved from http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html
- National Centers of Academic Excellence in Cyber Defense: https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/
- National Centers of Academic Excellence in Cyber Operations: https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/
- National Institute of Standards and Technology / National Initiative for Cybersecurity Education (NIST/NICE) Cybersecurity Workforce Demand: https://www.nist.gov/sites/default/files/documents/2017/01/30/nice_workforce_demand.pdf
- NGSS Lead States. 2013. *Next Generation Science Standards: For States, By States*. Washington, DC: The National Academies Press.
- Rostami, Masoud, Farinaz Koushanfar, and Ramesh Karri. "A Primer on Hardware Security: Models, Methods and Metrics." *Proceedings of the IEEE 102.8* (2014): 1283-1295. (USED)
- Segran, Elizabeth. Why Top Tech CEOs Want Employees With Liberal Arts Degrees. *Fast Company* (August 28, 2014). Retrieved from https://www.fastcompany.com/3034947/the-future-of-work/why-top-tech-ceos-want-employees-with-liberal-arts-degrees.

- Global IT Skills Framework for the Information Age (SFIA): https://www.sfia-online.org
- Singapore Cybersecurity Strategy: https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy
- Stoneburner, Gary, Clark Hayden, and Alexis Feringa. Engineering Principles for Information Technology Security (A Baseline for Achieving Security, Revision A" *NIST Special Publication* (2004): 800-27 Rev A. Retrieved from: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=151294
- *The 2015 (ISC)^2 Global Information Security Workforce Study*. (2015). International Information Systems Security Certification Consortium – (ISC)^2. Retrieved from https://www.boozallen.com/content/dam/boozallen/documents/Viewpoints/2015/04/frostsullivan-ISC2-global-information-security-workforce-2015.pdf
- U.K. Government Communications Headquarters (GCHQ)
- U.S. National Initiative for Cybersecurity Education (NICE), Cybersecurity Workforce Framework (NCWF): https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice/nice-cybersecurity
- U.S. National Research Council. 2013. Next Generation Science Standards: For *States*, *By States*. Washington, DC: The National Academies Press
- U.S. National Research Council Next Generation Science Standards: http://nextgenscience.org
- U.S. National Security Agency and Department of Homeland Security Centers of Academic Excellence in Cyber Defense and Cyber Operations: https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/ and https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/
- U.S. National Science Foundation
- Weingart S.H. (2000) Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses. In: Koç Ç.K., Paar C. (eds) Cryptographic Hardware and Embedded Systems — CHES 2000. CHES 2000. Lecture Notes in Computer Science, vol 1965. Springer, Berlin, Heidelberg (USED)
- *WG 11.8: Information Security Education*. International Federation for Information Processing Working Group (IFIP WG 11.8). Retrieved from https://www.ifiptc11.org/wg118

Appendix A: Contributors

This appendix lists the members of the Global Advisory Board, The Industrial Advisory Board, the working group members for each knowledge area, and a complete list of contributors.[21]

The Global Advisory Board
To the Joint Task Force on Cybersecurity Education

<u>Lynn Futcher, (GAB Chair)</u>
IFIP WG11.8 Chair (Information Security Education)
Member of the Centre for Research in Information and Cyber Security
Port Elizabeth, South Africa

<u>Jill Slay, (GAB Co-Chair)</u>
Director, Australian Centre for Cyber Security
University of New South Wales Canberra, Australia

<u>Ryma Abassi</u>
Assistant Professor, Higher Institute of Technological Studies in Communication in Tunis (ISET'Com)
University of Carthage, Tunisia

<u>Maria Bada</u>
Oxford Martin Fellow, The Global Cybersecurity Capacity Centre
Academic Centre of Excellence in Cyber Security
Oxford University College, United Kingdom

<u>KP Chow</u>
Associate Professor, Programme Director, MSc (Comp SC)
Associate Director, Center for Information Security and Cryptography (CISC)
University of Hong Kong, Hong Kong

<u>Audun Jøsang</u>
Professor, Department of Informatics
University of Oslo, Norway

<u>Stewart Kowalski</u>
Professor, Information Security
Norwegian University of Science and Technology, Norway

<u>Natalia Miloslavskaya</u>
Associate Professor Candidate of Tech. Sciences
National Research Nuclear University
MEPhl (Moscow Engineering Physics Institute)
Moscow, Russia

<u>Stig Frode Misolsnes</u>
Professor, Department of Information Security and Communication Technology
Norwegian University of Science and Technology, Norway

[21] While we tried to accurately capture all contributors, if we missed or misrepresented your participation, please contact us for corrections.

Johan van Niekerk
Professor, Information Security
Nelson Mandela University, South Africa

Jerzy Nawrocki
Dean of Faculty of Computing
Poznań University of Technology, Poland

Angela Sasse
Professor, Human-Centered Security
Director, U.K. Research Institute in Science of Cyber Security (RISCS)
University College London, United Kingdom

Matt Warren
Professor, Cyber Security
Deakin University, Australia

Steven Wong
Associate Professor, Informatics
Singapore Institute of Technology, Singapore

The Industrial Advisory Board
To the Joint Task Force on Cybersecurity Education

Christa Anderson
Senior Security Program Manager, Microsoft Security Response Center
Microsoft

David Biros
Associate Professor Management Science and Information Systems
Oklahoma State University

Eric Braun
Engineering Program Manager
Emerson Automation Solutions

Emily Darraj
Health IT Manager, Health Division
Northrop Grumman Information Systems

Angel Diaz
CEO
Technical Services Corp.

Stephen Dill
Lockheed Martin Fellow, Chief Architect Cyber Security (ret.)
Lockheed Martin Information Systems

Ashutosh Dutta
Director of Technology Security
AT&T

Gerhard Eschelbeck
Vice President Security & Privacy Engineering
Google

Dianne Fodell
Program Director Global University Programs, Cybersecurity Innovation
IBM

Mark Graff
Founder & CEO
Tellagraff, LLC

Dwayne Hodges
Senior Cyber Security Program Manager
U.S. Department of Energy

Josh Kebbel-Wyen
Senior Program Manager, Security
Adobe Systems, Inc.

Mark Kuhr
CTO
Synack

<u>Mark-David McLaughlin</u>
PSIRT Core Team Lead
Cisco Systems

<u>David Manz</u>
Senior Cyber Security Scientist
Pacific Northwest National Laboratory

<u>Mark Mykytishyn</u>
Chairman and CEO
Tangible Security

<u>Srini Ramaswamy</u>
Software Technology Manager
ABB, Inc.

<u>Tiina Rodrigue</u>
Senior Advisor for Cybersecurity
U.S. Department of Education

<u>Matt Rosenquist</u>
Cybersecurity Strategist
Intel Corporation

<u>Carter Schoenberg</u>
President and CEO
HEMISPHERE Cyber Risk Management

<u>Rick Tracy</u>
CSO/CTO
Telos Corporation

<u>Zachary Tudor</u>
Associate Laboratory Directory, National and Homeland Security
Idaho National Laboratory

<u>Mike Westra</u>
In-Vehicle Cyber Security Technical Manager
Ford Motor Company

<u>Brett Williams</u>
President, Operations, Training and Security Division
IronNet Cybersecurity, Inc.

Knowledge Area Working Groups

Knowledge Area: Data Security

Travis Atkison
University of Alabama

Matthew Hudnall
University of Alabama

Keyu Jiang
Regis University

Faisal Kaleem
Metropolitan State

J. Richard Kiper
U.S. Federal Bureau of Investigation

Travis Mayberry
United States Naval Academy

James Walden
Northern Kentucky University

Golden Richard
Louisiana State University

Richard Weiss
Evergreen State College

Marius Zimand
Towson University

The following JTF members led this working group:

Sidd Kaza
Towson University

Allen Parrish
United States Naval Academy led this working group.

Knowledge Area: Software Security

Bill Chu
University of North Carolina Charlotte

Melissa Dark
Purdue University

Michael Howard
Microsoft

Andrew Kornecki
Embry Riddle Aeronautical University

Gary McGraw
Synopsys

Kara Nance
Virginia Tech

Phillip Nico
California Polytechnic State University

Blair Taylor
Towson University

Michael Wertheimer
Private consultant

Alec Yasinsac
University of South Alabama

The following JTF members led this working group:

Matt Bishop
University of California at Davis

J Ekstrom
Brigham Young University

Knowledge Area: Component Security

Matt Bishop
University of California at Davis

J Ekstrom
Brigham Young University

Scott Graham
U.S. Air Force Institute of Technology

Michael R. Grimaila
U.S. Air Force Institute of Technology

Steven Lingafelt
IBM

Patrick Sweeney
U.S. Air Force Research Laboratory

Avinash Varna
Intel

The following JTF member led this working group:

David S. Gibson
U.S. Air Force Academy

Knowledge Area: Connection Security

Matt Bishop
University of California at Davis

David S. Gibson
U.S. Air Force Academy

Scott Graham
U.S. Air Force Institute of Technology

Michael R. Grimaila
U.S. Air Force Institute of Technology

Steven Lingafelt
IBM

Patrick Sweeney
U.S. Air Force Research Laboratory

The following JTF member led this working group:

J Ekstrom
Brigham Young University

Knowledge Area: System Security

J Ekstrom
Brigham Young University

David S. Gibson
U.S. Air Force Academy

Scott Graham
U.S. Air Force Institute of Technology

Michael R. Grimaila
U.S. Air Force Institute of Technology

Steven Lingafelt
IBM

Patrick Sweeney
U.S. Air Force Research Laboratory

The following JTF member led this working group:

Matt Bishop
University of California at Davis

Knowledge Area: Human Security

Alvaro Arenas
IE University (Spain)

Linda Brock
IBM

Melissa Carlton
Florida State University

Karla Clarke
KPMG LLP

Laurie Dringus
Nova Southeastern University

Steven Furnell
Plymouth University

Robert Hambly
U.S. Department of Defense

Heather Lipford
University of North Carolina at Charlotte

Sameer Patil
Indiana University

Daniel Shoemaker
University of Detroit Mercy

Johnathan Yerby
Middle Georgia State University

The following JTF member led this working group:

Yair Levy
Nova Southeastern University

Knowledge Area: Organizational Security

Wasim Alhamdani
Imam Abdulrahman bin Faisal University

Timothy Cullen
Private sector

Phillip Mahan
Private sector

William Mahoney
University of Nebraska, Omaha

Michelle Ramim
Middle Georgia State University

Hossain Shahriar
Kennesaw State University

Gordon Shenkle
Private sector

Gerhard Steinke
Seattle Pacific University

Samir Tout
Eastern Michigan University

The following JTF member led this working group:

Herbert Mattord
Kennesaw State University

Knowledge Area: Societal Security

David Aucsmith
University of Washington

Scott Bell
Northwest Missouri State University

Ryan Calo
Stanford University

Yoshi Kohno
University of Washington

Jeff Kosseff
United States Naval Academy

Martin Libicki
United States Naval Academy

Mary Manjikian
Regent University

James Smith
Nova Southeastern University

Samuel Sanders Visner
MITRE Corporation

The following JTF members led this working group:

Scott Buck
Intel Labs, Intel

Elizabeth K. Hawthorne
Union County College

Contributing Reviewers

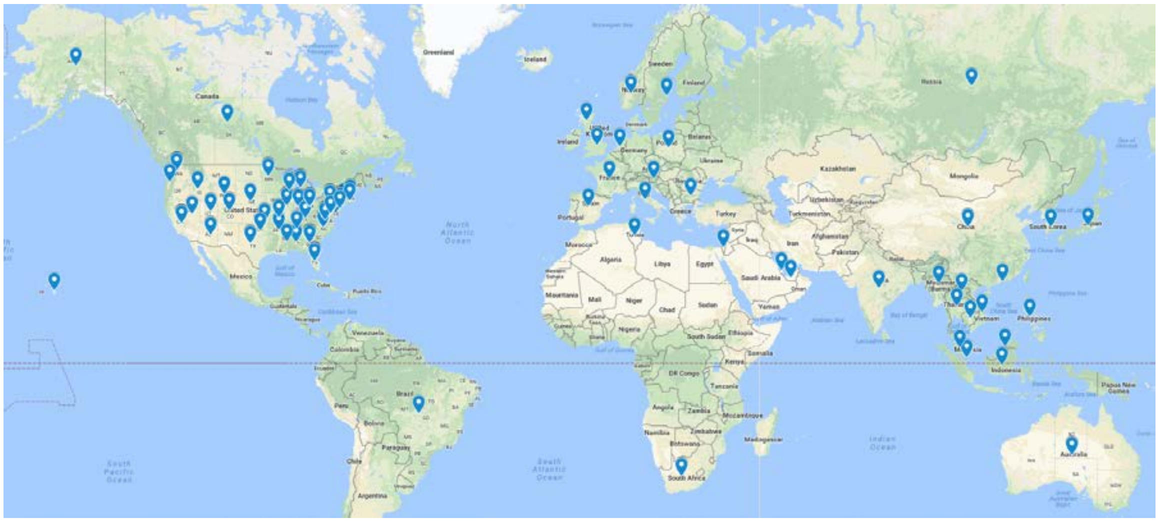


Figure 7. Contributors by country.

Name	Institution	Country
Ryma Abassi	University of Carthage	Tunisia
Sherly Abraham	Georgia Gwinnett College	United States (Georgia)
Joshua Adams	Saint Leo University	United States (Florida)
Mustaque Ahamad	Georgia Institute of Technology	United States (Georgia)
Sara Akers	Terra State Community College	United States (Ohio)
Massimiliano Albanese	George Mason University	United States (Virginia)
Brian Albertson	State Farm	United States (Georgia)
Wasim Alhamdani	University of the Cumberlands	United States (Kentucky)
James Alves-Foss	University of Idaho	United States (Idaho)
Christa Anderson	Microsoft	United States (Washington)
Patricia Anderson	Volunteer State Community College	United States (Tennessee)
Thibaud Antignac	CEA	France
Flo Appel	Saint Xavier University	United States (Illinois)
Alvaro E. Arenas	IE Business School	Spain
Rob Arnold	Threat Sketch	United States (North Carolina)
Travis Atkison	University of Alabama	United States (Alabama)
David Aucsmith	University of Washington	United States (Washington)
Bruce Bakis	MITRE	United States (Massachusetts)
Maria Bada	Oxford University College	United Kingdom (England)
Albert Ball	Hodges University	United States (Florida)
Masooda Bashir	University of Illinois at Urbana–Champaign	United States (Illinois)
Shannon Beasley	Middle Georgia State University	United States (Georgia)
Scott Bell	Northwest Missouri State University	United States (Missouri)

Kimberly Bertschy	Northwest Arkansas Community College	United States (Arkansas)
Debasis Bhattacharya	University of Hawaii Maui College	United States (Hawaii)
Vijay Bhuse	Grand Valley State University	United States (Michigan)
Diana Bidulescu	School City, Inc.	United States (Texas)
David Biros	Oklahoma State	United States (Oklahoma)
Matt Bishop	University of California at Davis	United States (California)
Chutima Boonthum-Denecke	Hampton University	United States (Virginia)
Brandi Boucher Fabel	Ivy Tech Community College	United States (Indiana)
Eric Braun	Emerson	United States (Minnesota)
Linda Brock	IBM	United States (Florida)
Scott Buck	Intel Labs, Intel	United States (Arizona)
Ingrid Buckley	Florida Gulf Coast University	United States (Florida)
Diana L. Burley	George Washington University	United States (District of Columbia)
William Butler	Capitol Technological University	United States (Maryland)
Bonnie Butlin	Security Partners' Forum	Canada
William (Bill) Caelli	Queensland University of Technology	Australia
Ryan Calo	Stanford University	United States (California)
Roy Campbell	University of Illinois at Urbana-Champaign	United States (Illinois)
Martin Carlisle	Carnegie Mellon University	United States (Pennsylvania)
Melissa Carlton	Florida State University	United States (Florida)
Lillian N. Cassel	Villanova University	United States (Pennsylvania)
John Chandy	University of Connecticut	United States (Connecticut)
Ankur Chattopadhyay	University of Wisconsin - Green Bay	United States (Wisconsin)
Zhen Chen	Tsinghua University	China
Li-Chiou Chen	Pace University	United States (New York)
Hongmei Chi	Florida A&M University	United States (Florida)
Jessica Chisholm	Valencia College	United States (Florida)
KP Chow	Hong Kong University	Hong Kong
Bill Chu	University of North Carolina	United States (North Carolina)
Lynn Clark	U.S. Federal Government	United States (Maryland)
Karla Clarke	KPMG	United States (California)
Marrci Conner	Henry Ford College	United States (Michigan)
Wanda Cowan	ABLE Christian School	United States (Georgia)
Timothy Cullen	Adapture	United States (Georgia)
Kevin Daimi	University of Detroit Mercy	United States (Michigan)
Melissa Dark	Purdue University	United States (Indiana)
Emily Darraj	Northrop Grumman	United States (Georgia)
Don Davidson	US Department of Defense	United States (Virginia)
Lisa Davidson	University of New South Wales	Australia
Ruth Davis	Santa Clara University	United States (California)

Shawn Davis	Illinois Institute of Technology	United States (Illinois)
Bostjan Delak	ITAD	United Kingdom (England)
Ravi Dhungel	Dexcom	United States (California)
Angel Diaz	Technical Services Corp	United States (District of Columbia)
Stephen Dill	Lockheed Martin (ret.)	United States (Maryland)
Ron Dodge	Palo Alto Networks	United States (California)
Bill Doherty	Truckee Meadows Community College	United States (Nevada)
Lynette Drevin	North-West University	South Africa
Laurie Dringus	Nova Southeastern University	United States (Florida)
Ashutosh Dutta	AT&T	United States (New York)
J Ekstrom	Brigham Young University	United States (Utah)
Barbara Endicott-Popovsky	University of Washington	United States (Washington)
Burkhard Englert	California State University Long Beach	United States (California)
Gerhard Eschelbeck	Google	United States (California)
Deidre Evans	Florida A&M University	United States (Florida)
Leslie D. Fife	The Church of Jesus Christ of Latter-day Saints	United States (Utah)
Dave Filer	New River Community College	United States (Virginia)
Saa E. Fillie	Wangoh Dynamics Technologies	United States (Virginia)
Dianne Fodell	IBM - Cyber Security Innovation	United States (North Carolina)
Renee Forney	The Forney Group / Capital One	United States (Virginia)
Guillermo Francia III	Jacksonville State University	United States (Florida)
Robert Francis	Federal Reserve Bank of New York	United States (New York)
Lothar Fritsch	Karlstad University	Sweden
Steven Furnell	Plymouth University	United Kingdom (England)
Janos Fustos	Metropolitan State University of Denver	United States (Colorado)
Lynn Futcher	Nelson Mandela University	South Africa
Thoshitha Gamage	Southern Illinois University Edwardsville	United States (Illinois)
Catherine Garcia van Hoogstraten	The Hague University of Applied Sciences	Netherlands
Ruti Gafni	Academic College of Tel-Aviv Yaffo	Israel
Daniel Garrie	ZEK LLC	United States (New York
Jim Gast	Gast and Associates	United States (Wisconsin)
Markus Geissler	Cosumnes River College	United States (California)
Dickie George	Johns Hopkins University Applied Physics Laboratory	United States (Maryland)
Duane Gerstenberger	Marion Technical College	United States (Ohio)

Tirthankar Ghosh	St. Cloud State University	United States (Minnesota)
David Gibson	U.S. Air Force Academy	United States (Colorado)
Andrew Ginter	Waterfall Security	Israel, United States (Virginia), France
Joseph Giordano	Utica College	United States (New York)
Bonnie Goins	Illinois Institute of Technology	United States (Illinois)
Kartik Gopalan	Binghamton University	United States (New York)
Mark Graff	Tellagraff, LLC	United States (New York)
Scott Graham	U.S. Air Force Institute of Technology	United States (Ohio)
Michael R. Grimaila	U.S. Air Force Institute of Technology	United States (Ohio)
Andy Green	Kennesaw State University	United States (Georgia)
Steve Hailey	CyberSecurity Academy	United States (Washington)
Hassan Hajjdiab	Abu Dhabi University	Unite Arab Emirates
H. Hall	Athens Technical College	United States (Ohio)
Robert Hambly	U.S. Department of Defense	United States (North Carolina)
K Harisaiprasad	Manhindra	India
Richard Harknett	University of Cincinnati	United States (Ohio)
Elizabeth K. Hawthorne	Union County College	United States (New York)
Matt Heff	SANDS	United States (Nevada)
Michael Hefley	University of Nebraska at Omaha	United States (Nebraska)
Danis J. Heighton	Clark State Community College	United States (Ohio)
Rochelle Heller	George Washington University	United States (District of Columbia)
Jim Helm	Arizona State University	United States (Arizona)
Morgan Henrie	MH Consulting Inc.	United States (Alaska)
Jayantha Herath	St. Cloud State University	United States (Minnesota)
Erik Hjelmås	Norwegian University of Science and Technology	Norway
Dwayne Hodges	U.S. Department of Energy	United States (Delaware)
Lance Hoffman	George Washington University	United States (District of Columbia)
Kenneth Hoganson	Kennesaw State University	United States (Georgia)
Marko Hölbl	University of Maribor	Slovenia
Adrianna Holden-Gouveia	Northern Essex Community College	United States (Massachusetts)
Susan Holland	University of Massachusetts Lowell	United States (Massachusetts)
Micaela Hoskins	Cisco Systems	United States (California)
Michael Howard	Microsoft	United States (Washington)
Matthew Hudnall	University of Alabama	United States (Alabama)
Grant Hudson	United States Postal Service	United States (North Carolina)
Angel L Hueca	Nova Southeastern University	United States (Florida)
Andrew Hurd	Excelsior College	United States (Minnesota)
John Impagliazzo	Hofstra University	United States (New York)

Stephen Itoga	University of Hawaii at Manoa	United States (Hawaii)
Murray Jennex	San Diego State University	United States (California)
Keyuan Jiang	Regis University	United States (Colorado)
Sonja Johnson		United States
Audun Jøsang	The University of Oslo	Norway
Connie Justice	Indiana University Purdue University Indianapolis	United States (Indiana)
Thomas Kaczmarek	Marquette University	United States (Wisconsin)
Chris Kadlec	Georgia Southern University	United States (Georgia)
Andrew Kalafut	Grand Valley State University	United States (Michigan)
Faisal Kaleem	Metropolitan State	United States (Minnesota)
Alan Katerinsky	Hilbert College	United States (New York)
Jonathan Katz	University of Maryland	United States (Maryland)
Sidd Kaza	Towson University	United States (Maryland)
Josh Kebbel-Wyen	Adobe	United States (California)
Walter Kerner	Fashion Institute of Technology	United States (New York)
Rami Khasawneh	Lewis University	United States (Illinois)
J. Richard Kiper	U.S. Federal Bureau of Investigation	United States (Florida)
Laszlo Kish	Texas A&M University	United States (Texas)
Valentin Kisimov	University National and World Economy Bulgaria	Bulgaria
Yoshi Kohno	University of Washington	United States (Washington)
Andrew Kornecki	Embry Riddle Aeronautical University	United States (Florida)
Peter Komisarczuk	Royal Holloway University of London	United Kingdom
Jeff Kosseff	United States Naval Academy	United States (Maryland)
Stewart Kowalski	Norwegian University of Science and Technology	Norway
Donald Kraft	Colorado Technical University and U.S. Air Force Academy	United States (Colorado)
Mark Kuhr	Synack	United States (California)
CRS Kumar	Defense Institute of Advanced Technology, Pune	India
Ojoung Kwon	California State University at Fresno	United States (California)
Mischel Kwon	Mischel Kwon and Associates LLC	United States (Virginia)
David Lanter	Temple University	United States (Pennsylvania)
Stephen Larson	Slippery Rock University of PA	United States (Pennsylvania)
Margaret Leary	Northern Virginia Community College	United States (Virginia)
Roy Levow	Florida Atlantic University	United States (Florida)
Yair Levy	Nova Southeastern University	United States (Florida)

Peng Li	East Carolina University	United States (North Carolina)
Martin Libicki	United States Naval Academy	United States (Maryland)
Alan Lin	U.S. Air Force Institute of Technology	United States (Ohio)
Steven Lingafelt	IBM	United States (North Carolina)
Heather Lipford	University of North Carolina at Charlotte	United States (North Carolina)
Xun Luo	China Computer Federation	China
Phillip Mahan	Private sector	United States (Georgia)
William Mahoney	University of Nebraska Omaha	United States (Nebraska)
Qutaibah Malluhi	Qatar University	Qatar
Mary Manjikian	Regent University	United States (Virginia)
David Manz	Pacific Northwest National Laboratory	United States (Washington)
Fabio Massacci	University of Trento	Italy
Herbert Mattord	Kennesaw State University	United States (Georgia)
Travis Mayberry	United States Naval Academy	United States (Maryland)
Cory A. Mazzola	Mandiant, a FireEye Company	United States (Virginia)
Todd McDonald	University of South Alabama	United States (Alabama)
Ernest McDuffie	Global McDuffie Group	United States (Virginia)
Andrew McGettrick	University of Strathclyde	Scotland
Gary McGraw	Synopsys	United States (California)
Mark-David McLaughlin	Cisco Systems	United States (Massachusetts)
Nancy Mead	Carnegie Mellon University	United States (Pennsylvania)
Mark Merkow	Charles Schwab and Co. Inc.	United States (Arizona)
NG Mien Ta	Wizlearn Technologies Pte Ltd	Singapore
Natalia Miloslavskaya	National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)	Russia
Dustin Mink	University of West Florida	United States (Florida)
Stig Frode Misolsnes	Norwegian University of Science and Technology	Norway
Dawn Montemayor	Independent CISO	United States (Florida)
Teresa Moor	Volunteer State Community College	United States (Tennessee)
Michael Moorman	Saint Leo University	United States (Florida)
Drew Morin	T-Mobile	United States (District of Columbia)
Diane Murphy	Marymount University	United States (Virginia)
Mike Murphy	Retired	
Igor Muttik	Cyber Curio	United Kingdom (England)
Mark Mykytishyn	Tangible Security	United States (Virginia)
Debra Nakama	University of Hawaii Maui College	United States (Hawaii)
Kara Nance	Virginia Tech	United States (Virginia)
Priyadarsi Nanda	University of Technology Sydney (Australia)	Australia

Jerzy Nawrocki	Poznań University of Technology	Poland
Nam P. Nguyen	Towson University	United States (Maryland)
Phillip Nico	California Polytechnic State University	United States (California)
Stephen Olechnowicz	Institute for Defense Analysis	United States
Robert Olson	Rochester Institute of Technology	United States (New York)
Jacques Ophoff	University of Cape Town	South Africa
Mohd Fairuz Iskandar Othman	Universiti Teknikal Malaysia Melaka	Malaysia
Doyel Pal	LaGuardia Community College, CUNY	United States (New York)
Bernardo Palazzi	Brown University	United States (Rhode Island)
Alan Paller	SANS	United States (Maryland)
Hyungbae Park	University of Central Missouri	United States (Missouri)
Allen Parrish	United States Naval Academy	United States (Maryland)
Rahul K. Patel	Illinois Institute of Technology	United States (Illinois)
Sameer Patil	Indiana University	United States (Indiana)
Malcolm Pattinson	University of Adelaide	Australia
Kimberly Perez	Tidewater Community College	United States (Virginia)
Mathew (Pete) Peterson	U.S. Government	United States (Virginia)
Rodney Petersen	U.S. National Initiative for Cybersecurity Education	United States (Maryland)
Amelia Phillips	Highline College	United States (Washington)
Joe Pilla	ADP	United States (Virginia)
Mathias R. Plass	Lewis University	United States (Illinois)
Christine Pommerening	George Mason University	United States (Virginia)
Damira Pon	University at Albany, State University of New York	United States (New York)
Michael Brian Pope	Independent Scholar	
Randy Purse	Government of Canada	Canada
Portia Pusey[22]	Portia Pusey, LLC	United States (Maryland)
Michelle Ramim	Middle Georgia State University	United States (Georgia)
Srini Ramaswamy	ABB, Inc.	United States (Ohio)
Alan Rea	Western Michigan University	United States (Michigan)
Thomas Reddington	New York University (NYU)	United States (New York)
Randy Reid	University of West Florida	United States (Florida)
Tiina Rodrigue	U.S. Department of Education/George Washington University	United States (District of Columbia)
Matt Rosenquist	Intel	United States (California)
Dale Rowe	Brigham Young University	United States (Utah)
Andrew Rozema	Grand Rapids Community	United States (Michigan)

[22] Evaluator

	College	
John Ruero	ISSA	Phillipines
Rebecca Rutherfoord	Kennesaw State University	United States (Georgia)
Daniel Ryan	Wyndrose Technical Group	United States (Maryland)
Julie Ryan	National Defense University	United States (District of Columbia)
Eric Salveggio	Casper College	United States (Wyoming)
Altair Santin	PUCPR	Brazil
Gerry Santoro	Penn State University	United States (Pennsylvania)
Angela Sasse	University College, London	United Kingdom (England)
Carter Schoenberg	HEMISPHERE Cyber Risk Management	United States (Virginia)
Christian Servin	El Paso Community College	United States (Texas)
Hossain Shahriar	Kennesaw State University	United States (Georgia)
Cynthia Shelton	CenturyLink	United States (Virginia)
Gordon Shenkle	Private sector	United States (Georgia)
Sujeet Shenoi	University of Tulsa	United States (Oklahoma)
Daniel Shoemaker	University of Detroit Mercy	United States (Michigan)
Shahid Shahidullah	Hampton University	United States (Virginia)
Wengchang Shi	Renmin University of China	China
Rhea Siers	George Washington University	United States (District of Columbia)
Neelu Sinha	Fairleigh Dickinson University	United States (Pennsylvania)
Ambareen Siraj	Tennessee Tech University	United States (Tennessee)
Jill Slay	University of New South Whales, Canberra	Australia
James N. Smith	Nova Southeastern University	United States (Florida)
Avinash Srinivasan	Temple University	United States (Pennsylvania)
S Srinivasan	Texas Southern University	United States (Texas)
Nelbert C. St.Clair	Middle Georgia State University	United States (Georgia)
Gerhard Steinke	Seattle Pacific University	United States (Washington)
Mark Stockman	University of Cincinnati	United States (Ohio)
Laura Sullivan	East Central Community College	United States (Mississippi)
S. M. Taiabul Haque	University of Central Missouri	United States (Missouri)
Cara Tang	Portland Community College	United States (Oregon)
April Tanner	Jackson State University	United States (Florida)
Blair Taylor	Towson University	United States (Maryland)
Jeff Teo	Montreat College	United States (North Carolina)
Haydar Teymourlouel	Bowie State University	United States (Maryland)
Cynthia Thomas	Northern Kentucky University	United States (Kentucky)
David Tobey	Indiana University South Bend	United States (Indiana)
Samir Tout	Eastern Michigan University	United States (Michigan)
Kim Tracy	Michigan Technological University	United States (Michigan)
Rick Tracy	Telos Corporation	United States (Virginia)

Joe Tront	Virginia Polytechnic Institute and State University	United States (Virginia)
Ray Trygstad	Illinois Institute of Technology	United States (Illinois)
Michael Tu	Purdue University Northwest	United States (Indiana)
Zachary Tudor	U.S. Department of Energy Idaho National Laboratory	United States (Idaho)
Douglas Twitchell	Boise State University	United States (Idaho)
Johan van Niekerk	Nelson Mandela University	South Africa
Avinash Varna	Intel	United States (Arizona)
Randal Vaughn	Baylor University	United States (Texas)
Samuel Sanders Visner	MITRE Corporation	United States (Virginia)
Harald Vranken	Open University of the Netherlands	Netherlands
Paul Wagner	University of Wisconsin – Eau Claire	United States (Wisconsin)
James Walden	Northern Kentucky University	United States (Kentucky)
Charles Walker	U.S. Federal Government	United States
David Wang	DePaul University	United States (Illinois)
Paul Wang	University of Maryland University College	United States (Maryland)
Xinli Wang	Michigan Technological University	United States (Michigan)
Matt Warren	Deakin University	Australia
Alan B. Watkins	National University	United States (California)
Steve Weber	Drexel University	United States (Pennsylvania)
Richard Weiss	Evergreen State College	United States (Washington)
Michael Wertheimer	Private Consultant	United States
Deanne Wesley	Forsyth Technical Community College	United States (North Carolina)
Mike Westra	Ford Motor Company	United States (Michigan)
Suzanne Wetzel	Stevens Institute of Technology	United States (New Jersey)
Doug White	Roger Williams University	United States (Rhode Island)
Scott White	George Washington University	United States (District of Columbia)
Michael Whitman	Kennesaw State University	United States (Georgia)
Brett Williams	IronNet Cybersecurity, Inc.	United States (District of Columbia)
Patrea Wilson	University of Maryland University College	United States (Maryland)
Steven Wong	Singapore Institute of Technology	Singapore
Scott Woodison	University System of Georgia (Ret)	United States (Georgia)
Carol Woody	Software Engineering Institute, Carnegie Mellon University	United States (Pennsylvania)
Tom Worthington	Australian National University	Australia

Bill Wright	Symantec	United States (District of Columbia)
Martin Wybourne	Dartmouth College	United States (New Hampshire)
Alec Yasinsac	University of South Alabama	United States (Alabama)
Johnathan Yerby	Middle Georgia State University	United States (Georgia)
Louise Yngstrom	Stockholm University	Sweden
Chuan Yue	Colorado School of Mines	United States (Colorado)
Xiaodong Yue	University of Central Missouri	United States (Missouri)
Neal Ziring	NSA	United States (Maryland)
Natalia	National Research Nuclear University MEPhI	Russia
ZhangXuan	Shandong Police College	China
Marius Zimand	Towson University	United States (Maryland)

Appendix B: Essentials Table Overview

Data Essentials	Software Essentials
Basic cryptography concepts	Fundamental design principles; least privilege, open design, and abstraction
End-to-end secure communications	Security requirements and the roles they play in design
Digital forensics	Implementation issues
Data integrity and authentication	Static, dynamic analysis
Data erasure	Configuring, patching
	Ethics, especially in development, testing, and vulnerability disclosure

Component Essentials	Connection Essentials	System Essentials
Vulnerabilities of system components	Systems, architecture, models, and standards	Holistic approach
Component lifecycle	Physical component interfaces	Security policy
Secure component design principles	Software component interfaces	Authentication
Supply chain management	Connection attacks	Access control
Security testing	Transmission attacks	Monitoring
Reverse engineering		Recovery
		Testing
		Documentation

Human Essentials	Organizational Essentials	Societal Essentials
Identity management	Risk management	Cybercrime
Social engineering	Governance and policy	Cyber law
Awareness and understanding	Laws, ethics, and compliance	Cyber ethics
Social behavioral privacy and security	Strategy and planning	Cyber policy
Personal data privacy and security		Privacy

Appendix C: Exemplars

This appendix contains the Curricular, Workforce, and Course exemplar templates.

Curricular Exemplar Template

The CSEC2017 Body of Knowledge affords the flexibility to support many different types of curricula. The curricular exemplars will demonstrate how the curricula from specific institutions cover the knowledge area essentials and some subset of the knowledge units. The exemplars will be provided to demonstrate the ways that the Body of Knowledge may be organized into a complete curriculum.
(Note: *Please remove the italicized instructions in your responses.)*

Disciplinary Lens and Institution Type

➔ To Do: Select the disciplinary lens and institution type that best describes your program. Provide the primary location of your institution.

		Institution Type	
Disciplinary Lens		Degree / Program Length	Country
	Computer Science	*(e.g.) BA / 4-year*	*(e.g.) United States*
	Computer Engineering		
	Software Engineering		
	Information Systems		
	Information Technology		
	Other Disciplines (e.g., Cyber Science)		

In addition to the disciplinary lens and institution type differences, we recognize that institutions use different instructional delivery methods (e.g., lecture, laboratory, blended, online), and have other constraints or opportunities that impact the number of hours spent on various topics. While we expect that any curriculum or program of study within the broad field of cybersecurity should include the essentials from each knowledge area, we also expect that the inclusion of knowledge units, the depth of coverage for the topics within those knowledge units, and the specific learning outcomes will differ. At a minimum, we expect these differences to be based on the disciplinary lens and institution type. However, given the constant evolution of the field, we expect that other factors including the development of new knowledge, will contribute to these differences.

➔ To Do: Provide additional information about your program which influences curricular content.

Institution Information

➔ *To Do: Provide the following information.*

Institution:
Institution Location:
Faculty Contact:
Email Address:

Permanent URL where additional materials and information are available *(if applicable; this may be a program or catalog listing)* :

Curricular Overview

➔ *To Do: Describe your institution, program and general program requirements – course requirements, electives, and other requirements*

Knowledge Unit Table

Each curricular exemplar contains a large table that maps courses to knowledge area coverage. Within that table, columns represent courses and rows represent the knowledge units. The following example shows a Knowledge Unit Table template.

Knowledge Areas	**Knowledge Units**	**Course 1**	**Course 2**	**Course 3**	**Course 4**	**…**	**Course X**
Data Security	Essentials	*List of LOs*					
	Cryptography						
	Digital Forensics						
	Data Integrity and Authentication						
	Access Control						
	Secure Communication Protocols						
	Cryptanalysis						
	Data Privacy						
	Information Storage Security						

Example Knowledge Unit Table Template

➔ *To Do: Download KnowledgeUnitTable_Template.xls from the CSEC2017.org website and follow the instructions included in the file for completion of the table.*

➔ *To Do: Include the name of your Knowledge Unit Table in this section to ensure that the documents are appropriately connected.*

Curricular Analysis: Essentials and Knowledge Units in a Typical Major

➔ *To Do: For a typical major, map coverage of the essentials and knowledge units. Provide the list of topics covered in each course. Then provide an overall assessment of the KU coverage. The template for this table is included as the second worksheet in the file: KnowledgeUnitTable_Template.xls.* The following example shows the KU Coverage table template.

Knowledge Areas	Knowledge Units	Course 1	Course 2	Course 3	Course 4	...	Course X	% of Coverage	Optional: Additional Topics
Data Security	Essentials	*List of topics covered*						*% of topics covered*	*List of addiional topics covered*
	Cryptography								
	Digital Forensics								
	Data Integrity and Authentication								
	Access Control								
	Secure Communication Protocols								
	Cryptanalysis								
	Data Privacy								
	Information Storage Security								

Example of a KU Coverage Table

➔ *To Do: Provide a high-level picture of your coverage of CSEC2017 knowledge area essentials. Provide the percentage of essentials concepts for each knowledge area that are covered in your curriculum.*
Note: this table is an excerpt of the KU Coverage Table.

Knowledge Area	Essentials Coverage
Data Security	*% of essentials*
Software Security	
Component Security	
Connection Security	
System Security	
Human Security	
Organizational Security	
Societal Security	

Possible Curricular Revisions (based on CSEC2017)

➔ *To Do: Describe any possible curricular changes resulting from your review of the CSEC2017 curricular guidance.*

➔ *To Do: Describe any curricular topics that you cover and are not present in the CSEC2017 curricular guidance.*

Course Summaries

➔ *To Do: Include the published course summaries for all courses included in your table.*

Workforce Exemplar Template

The CSEC 2017 Body of Knowledge affords the flexibility to support preparation for many different work roles (or positions) within the cybersecurity workforce. The workforce exemplars demonstrate how the work role requirements align with knowledge area essentials and some subset of the knowledge units. The exemplars are provided to show a variety of ways that employers can use the Body of Knowledge to characterize the needs of individual work roles within the cybersecurity workforce. (Note: *Please remove the italicized instructions in your responses.)*

➔ To Do: Provide the following information

Contact Name:
Email Address:
Company Name:
Location (country): *[Primary location(s) of the position.]*
Position Title:

Position Description

➔ To Do: Provide a description of the position and position requirements (e.g., degree, certifications, experience, Knowledge, Skills, and Abilities [KSA]).

Permanent URL where additional materials and information are available
(if applicable, this may be course website for a recent offering):

Knowledge Areas Summary

➔ To Do: List knowledge area(s) and the learning outcomes associated with the position. Note: It might be easier to complete this table last.

Knowledge Area	**Learning Outcomes**
(e.g.) System Security	

CSEC2017 Body of Knowledge Coverage

➔ *To Do: List the topics and learning outcomes (LOs) for the essentials and knowledge units required for this position.*

The workforce exemplar table is located on the fourth tab in the KnowledgeUnitTable_Template.xls file (see the table below).
Note: This section will likely be the most time-consuming to complete, but is the most valuable for educators planning to adopt the CSEC2017 guidelines.

Knowledge Areas	**Knowledge Units**	**Position Label**	
Data Security	Essentials	*List of Topics*	*List of LOs*
	Cryptography		
	Digital Forensics		
	Data Integrity and Authentication		
	Access Control		
	Secure Communication Protocols		
	Cryptanalysis		
	Data Privacy		
	Information Storage Security		

Example Knowledge Unit Table Template

Additional Topics

➔ *To Do: List topics, knowledge, skills, abilities, and/or competencies required for this position but not included in the CSEC2017 Body of Knowledge.*

Other Comments

➔ *To Do: Provide any additional information. [Optional]*

Course Exemplar Template

The CSEC 2017 Body of Knowledge affords the flexibility to support many different courses. The course exemplars demonstrate how the courses from specific institutions cover the knowledge area essentials and some subset of the knowledge units. The exemplars are provided to demonstrate the ways in which the Body of Knowledge can be operationalized into individual courses.

➔ *To Do: Provide the following information*

Course Number, Course Name, Institution

Institution Location:
Faculty Contact Name:
Email Address:

Permanent URL where additional materials and information are available *(if applicable, this may be course website for a recent offering):*

Disciplinary Lens and Institution Type

➔ *To Do: Select the disciplinary lens and institution type that best describes your program. Provide the primary location of your institution.*

		Institution Type	
Disciplinary Lens		Degree / Program Length	Country
	Computer Science	*(e.g.) BA / 4-year*	*(e.g.) United States*
	Computer Engineering		
	Software Engineering		
	Information Systems		
	Information Technology		
	Other Disciplines (e.g., Cyber Science)		

Knowledge Areas Summary

➔ *To Do: List knowledge area(s) and the learning outcomes associated with the course. (Note: It might be easier to complete this table last.)*

Knowledge Area	**Learning Outcomes**
(e.g.) System Security	

Course Description

➔ *To Do: Answer the following questions about the course. Remove italicized instructions when answering.*

Where does the course fit in your curriculum?
In what year do students commonly take the course? Is it mandatory? Does it have pre-requisites or is it in a sequence of courses? On an average, how many students take it in a semester/quarter/year?

What is covered in the course?
Provide a short description, and/or a concise list of topics - possibly from your course syllabus. (This is likely to be your longest answer.)

What is the course format?
Describe the course format. Is it face-to-face, online or blended? How many contact hours? Does it have lectures, lab sessions, or discussion sessions?

How are students assessed?
Describe student assessment. What type, and number, of assignments are students are expected to do? (Examples: papers, problem sets, programming projects, etc.). How long do you expect students to spend on completing assessed work?

Course textbooks and materials
Provide a brief description of materials used (e.g., textbooks, programming languages, environments, etc.)

Why do you teach the course this way?
Provide a description of the course rationale and goals. If you know, indicate the history and background of the course and when it was last reviewed/revised. Do students typically consider this course to be challenging?

CSEC2017 Body of Knowledge Coverage

➔ *To Do: List the topics and learning outcomes for the Essentials and Knowledge Units covered in the course.*

The course exemplar table is located on the third tab in the KnowledgeUnitTable_Template.xls file. (See the table below.)
Note: This section will likely be the most time-consuming to complete, but is the most valuable for educators planning to adopt the CSEC2017 guidelines.

Knowledge Areas	**Knowledge Units**	**Course Label**	
Data Security	Essentials	*List of Topics*	*List of LOs*
	Cryptography		
	Digital Forensics		
	Access Control		
	Secure Communication Protocols		
	Cryptanalysis		
	Data Privacy		
	Information Storage Security		

Example Knowledge Unit Table Template

KU Topics Not Covered

➔ *To Do: For KU topics not covered, indicate whether they are covered in another course or not covered in your curriculum at all.*

Additional Topics

➔ *To Do: List notable topics covered in the course that you do not find in the CSEC2017 Body of Knowledge.*

Other Comments

➔ *To Do: Provide any additional comments [Optional]*

Page intentionally left blank