Public Review and Comment period: open until July 3, 2017
Provide feedback at: http://csec2017.org

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 Security (AIS SIGSEC)
International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)

Version 0.75 Report
12 June 2017

ISBN: <to be determined>
DOI: <to be determined>
Web link: <http:// to be determined>
ACM Order Number: <to be determined>

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
+1-800-342-6626
+1-212-626-0500 (outside U.S.)
orders@acm.org
Tel: +1 800 272 6657
Fax: +1 714 821 4641
http://computer.org/cspress
csbook@computer.org

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 Security (AIS SIGSEC)

U.S. National Science Foundation (Award# 1623104)
Intel Corporation
U.S. National Security Agency

The CSEC2017 Final Report has been endorsed by <to be determined>.

Cybersecurity Curricula 2017

Version 0.75 Report
12 June 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 Security (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/CEP)
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/CEP)
University Program Director
Intel Corporation, USA

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

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

Col. David Gibson, Ph.D. (ACM/CEP)
Professor, Computer Science
Chair, Department of Computer Science
United States Air Force Academy, USA

Elizabeth Hawthorne, Ph.D. (ACM/CEP)
Senior Professor, Computer Science
Union County College, USA

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

Yair Levy, Ph.D. (AIS SIGSEC)
Professor, Information Systems and Cybersecurity
Director, Center for e-Learning Security Research (CeLSR)
Nova Southeastern University, USA

Herbert Mattord, Ph.D. (AIS SIGSEC)
Associate Professor, Information Systems
Associate Director, Center for Information Security Education
Kennesaw State University, USA

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

Table of Contents

Chapter 1: Introduction

For nearly five decades, starting with Computer Science 1968[1], 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 (CC2005) report provides an overview of the curriculum guidelines for each of these five computing disciplines[2]. This volume, CSEC2017, represents an expansion of the ACM education initiative to include the first set of global curricular recommendations in 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 1.5 million cybersecurity-related positions going unfilled by 2020[3]. The workforce demand is acute, immediate, and growing[4]. 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 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.

1.1 Background

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 Security (AIS

[1] ACM Curriculum Committee on Computer Science. 1968. Curriculum 68: Recommendations for Academic Programs in Computer Science. *Comm. ACM* 11, 3 (Mar. 1968), 151-197.
[2] ACM Computing Disciplines Overview: http://acm.org/education/curricula-recommendations
[3] 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
[4] (ISC)2 Report available here: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf
[5] IEEE CS website: https://www.computer.org/

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 term "Cyber Sciences" reflects a collection of computing-based disciplines involving technology, people, and processes aligned in a way to enable "assured operations" in the presence of risks and adversaries. It involves the creation, operation, analysis, and testing of secure computer systems (including network and communication systems) as well as the study of how to employ operations, reasonable risk taking, and risk mitigations. The concept of "Cyber Sciences" refers to a broad collection of such programs, and disciplines under this umbrella often also include aspects of law, policy, human factors, ethics, risk management, and other topics directly related to the success of the activities and operations dependent on such systems, many times in the context of an adversary.

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 "cyber sciences" to label this effort, conceptually the terms are consistent. The precise definition of cybersecurity used to drive the CSEC2017 effort is provided below.

1.2 Vision, Mission, and Goals

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:

[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/

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.

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.
- 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.

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 and 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.

In order to further focus the content and structure included in the cybersecurity curricular guidance, the CSEC2017 JTF defined primary and secondary audiences as outlined 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;
- 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 Overall Scope of Cybersecurity

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.*

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) and, as a result, shape the nature of the curricular content. Although the knowledge areas included in the curricular guidance are recommended for all programs, the depth of coverage and the desired student learning outcomes may differ based on the disciplinary foundation (e.g. computer science vs. information systems). The manner in which the disciplinary lens shapes the curricular content will be fully described in chapters 3 and 4 of this document.

1.4 Guiding Principles and Community Engagement

The CSEC2017 JTF has continuously engaged the broad stakeholder community throughout the development process. Community members have provided input to shape the approach, content and organizational structure of the CSEC2017 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.

Among these activities, two key milestones in the early development process were the International Security Education Workshop and the Global Stakeholder Survey. They are summarized below. A full list of community engagement activities, along with updates on the development process, and information about opportunities for continued engagement are available through the CSEC2017 website[9].

1.4.1 International Security Education Workshop

The 2016 International Security Education Workshop (ISEW) was held June 13-15th, 2016 in Philadelphia, PA[10]. 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.

[9] CSEC2017 website: http://csec2017.org
[10] 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).

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 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 are particularly appreciative of the many comments provided as feedback on v. 0.50. The CSEC2017 v. 0.50 draft received more than 2300 downloads and we carefully considered all comments and critiques. We also gratefully recognize the global subject matter experts who provide advice as members of our advisory boards (Global Advisory Board and Industry Advisory Board),as well as the members of our Knowledge Area Working Groups who assisted in the development of knowledge area curricular content. A comprehensive list of contributors appears in an appendix at the end of this document.[11] Opportunities to support the work of the CSEC2017 JTF are ongoing.

1.5 Structure of the Cybersecurity 2017 Report

This report, CSEC2017, 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 roadmaps for implementing

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

the cybersecurity curricular framework, and includes exemplars to assist with institutional implementation.

CSEC2017 v. 0.75 is presented to the stakeholder community for review and comment. This second draft builds upon the content and critical feedback received on CSEC2017 v. 0.50. While significantly more developed, v. 0.75 remains in draft form. As such, not all sections of the report are fully developed. However, the JTF appreciates feedback on all portions of the report. Please submit all feedback using the comment form located at csec2017.org.

Chapter 2: The Cybersecurity Discipline

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.

During the Cold War beginning in the late 1940s, many more mainframe computers were brought online to accomplish more complex and sophisticated tasks. Department of Defense's Advanced Research Projects Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the exchange of computer data. ARPANET saw wider 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 early 1980s, the development of TCP (the Transmission Control Protocol) and IP (the Internet Protocol) led to the emergence of the Internet brought the networking aspects of Cybersecurity to the fore. 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 pervasive connectivity to virtually all computers where integrity and confidentiality were a lower priority than the drive for availability where many problems that plague the Internet today result from this early lack of security.

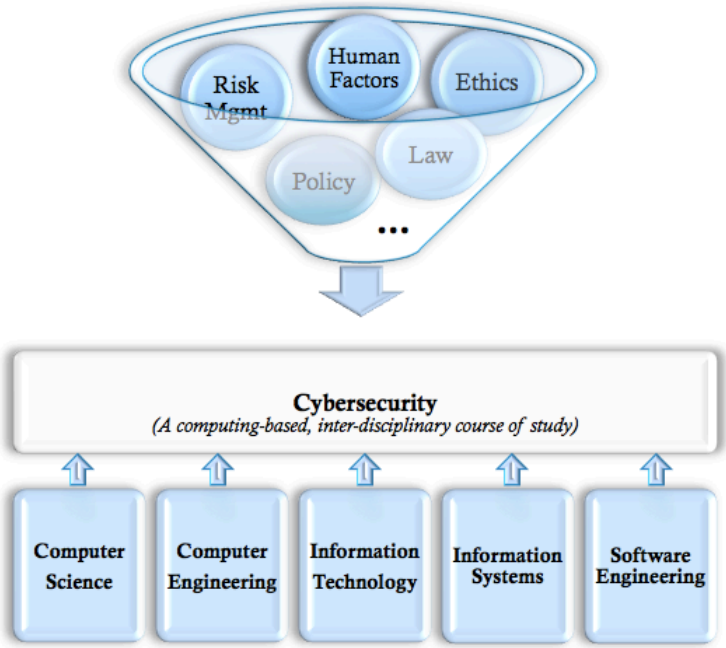
Early computing approaches relied on security that was built into the physical environment of the data center that housed the computers. As networked computers became the dominant style of computing, the ability to physically secure a networked computer was lost, and the stored information became more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

The Internet brings millions of unsecured computer networks and billions of computer systems 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 and then choosing security controls to apply and protect the information as it is transmitted, processed and stored. Recent years have seen a growing awareness of the need to improve cybersecurity, as well as a realization that cybersecurity is important to national defense. The growing threat of cyber attacks 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 information warfare, and the possibility that business and personal information systems could become casualties if they are undefended.

2.1 The Emergence of Cybersecurity as a Discipline

Given societies increasing dependence on the global cyber infrastructure, it is no surprise that cybersecurity is emerging as an identifiable discipline whose breadth and depth of content encompasses many of the sub-fields (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, 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 below, academic programs in cybersecurity are both informed by the inter-disciplinary content, and driven by the needs and perspectives of the computing discipline that forms the programmatic foundation.



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.

2.2 Characteristics of a Cybersecurity Program

Each graduate of a cybersecurity program of study should have a cybersecurity curriculum that includes: (1) a computing-based (e.g. computer science, information technology) foundation; (2) cross-cutting concepts that are broadly applicable across the range of cybersecurity specializations (e.g. cybersecurity's inherent adversarial mindset); (3) a body of knowledge containing core cybersecurity knowledge and skills; (4) a direct relationship to the range of specializations meeting the in-demand domains (for reference, we use the domains identified in the US National Cybersecurity Workforce Framework[12]); and (5) a strong emphasis on the ethical 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.

[12]US National Cybersecurity Workforce Framework website: http://csrc.nist.gov/nice/framework/

Chapter 3: Cybersecurity Curricular Framework

Cybersecurity programs require curricular content that includes: (1) the theoretical and conceptual knowledge essential to understanding the discipline and; (2) opportunities to develop the practical skills that will support the application of that knowledge. The content included in any cybersecurity program is requires a delicate balance of breadth, 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 flexibility necessitated by both local needs and advancements in the body of knowledge. The curricular framework presented in the chapter supports the achievement of these goals.

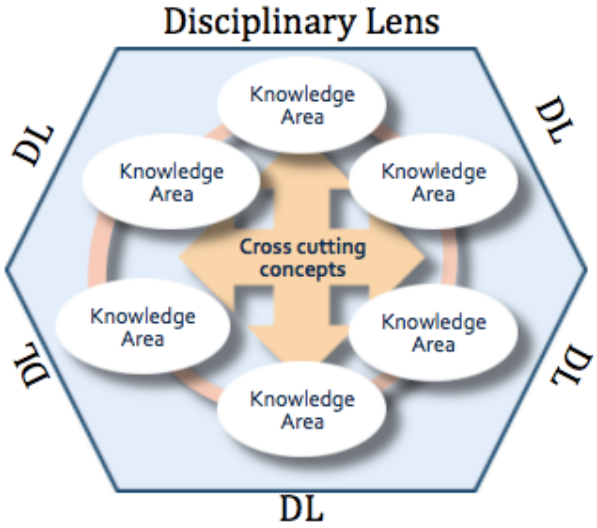
3.1 Philosophy and Approach

The CSEC2017 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[13], views cybersecurity as a body of knowledge grounded in enduring principles and continuously extended, refined, and revised through evidence-based practice.

3.2 CSEC2017 Thought Model

The CSEC2017 thought model has four dimensions: knowledge areas, crosscutting concepts, disciplinary lens, and application areas. The depiction below shows the first three dimensions. The internal coloring of the model represents the presence of foundational knowledge. While not explicitly identified as a model dimension, foundational knowledge underlies and supports all of the curricular content described below. The fourth dimension, application areas, is used to link the curricular content to workforce frameworks and is described in a subsequent chapter.

[13] US National Research Council Next Generation Science Standards website: http://nextgenscience.org



3.2.1 Foundational Knowledge

Foundational knowledge requirements are twofold: general education requirements and foundational cybersecurity knowledge.

General education. Students embarking on a cybersecurity course of study are expected to have a basic level of proficiency in foundational concepts. General education requirements provide an opportunity for students to learn basic communication, computational, critical thinking and analytical skills. These basic skills are fundamental to a student's ability to meet the learning objectives associated with each knowledge area.

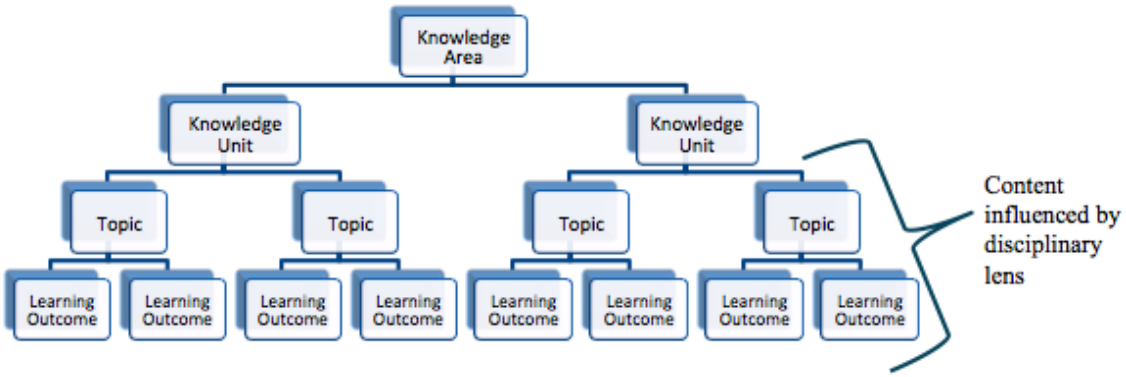
Foundational cybersecurity knowledge. Foundational cybersecurity knowledge should be introduced early and reinforced throughout any cybersecurity program. Foundational concepts, introduce students to basic cybersecurity concepts and terms, the threat environment, common vulnerabilities, and fundamentals of information assurance.

In the thought model, foundational knowledge sits outside of any single knowledge area and is depicted in the graphic by the colored space underlying the knowledge areas and crosscutting concepts.

3.2.2 Knowledge Areas

Knowledge areas serve as the basic organizing structure for cybersecurity content. Knowledge areas contain knowledge units - critical knowledge with broad importance within and across multiple computing-based disciplines. Collectively, knowledge areas represent the full body of knowledge within the field of cybersecurity.

The knowledge areas are structured as flexible buckets in the thought model to allow for the expansion and contraction of content as needed. Knowledge area content is structured with knowledge units - thematic groupings that encompass multiple, related topics; topics - curricular content; and learning outcomes - a description of what students should know or be able to do at the end of each topic. As shown below, each knowledge unit contains multiple topics and learning outcomes.



In the CSEC2017 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.

The disciplinary lens is used to focus the curricular content within each knowledge unit. It drives the depth and breadth of content covered in each topic, along with the associated learning outcomes.

The CSEC2017 thought model has six knowledge areas: data security, software security, system security, human security, organizational security, and societal security. The knowledge areas are organized by entities to be protected: data, software, systems, individuals, organizations, and society. The first three areas are primarily technical in nature while the last three areas include many topics not commonly taught in computing and engineering programs but with significant relevance to cybersecurity.

While the primary emphasis of each knowledge area is on protection and maintenance of security properties, some programs may choose to include the study of tools and techniques for circumventing protection mechanisms such as 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 six of the knowledge areas include knowledge units that can be taught from both cyber defense and cyber offense perspectives. With that in mind, all cybersecurity programs should include coverage of such knowledge units as ethics and cyber law. While the associated curricular guidance differs, these knowledge units (and others as shown in the knowledge area tables) are intentionally repeated in multiple knowledge areas.

Some cybersecurity programs may focus more heavily on the technical topics while others may include more emphasis on the individual, organizational and societal topics. However, the JTF believes that graduates of undergraduate cybersecurity programs should study topics in all six areas. The knowledge areas are listed and described briefly below from the most narrowly focused to the most broadly focused.

- The **Data Security** area focuses on the protection of data at rest and in transit. This is the most narrowly focused and theoretical of the six areas, requiring the application of mathematical and analytical algorithms to fully implement. The primary goals of data security are to achieve confidentiality of information and preserve data and origin integrity. Knowledge units in this area include: cryptography, confidentiality, and data integrity.

- The **Software Security** area focuses on the development and use of software that reliably preserve the security properties of the information and systems they protect. This is the most specialized of the six knowledge areas and the least likely to be developed in depth by all cybersecurity programs. Knowledge units in this area include: high assurance software, secure software development, deployment, and maintenance, software reverse engineering, and malware analysis. An understanding of data security is important for many aspects of software security.

- The **System Security** area focuses on establishing and maintaining the security properties of systems, including those of interconnected components. The components include data, software, and hardware devices of all kinds, networks, and humans. Knowledge units in this broad area include: availability, authentication, access control, secure system design, reverse engineering, cyber physical systems, digital forensics, supply chain management, and computer network defense. ***NOTE: Based on community feedback we are reevaluating the system security knowledge area. Some of the knowledge units originally considered to be components of this KA have been incorporated into other KAs and we are determining the best structure for the narrowed scope of this area.***

- The **Human Security** area focuses on protecting individuals' data in the context of organizations (i.e. as employees) or personal life, their privacy and threat mitigation. It also includes the study of human behavior and social engineering as it relates to cybersecurity. Knowledge units in this area include: identity management, social engineering, privacy, and security on social networks.

- The **Organizational Security** area focuses on protecting organizations from cybersecurity threats and on managing risk to support the successful accomplishment of the organization's mission. The organizations may be public or private, large or small, local, regional or international. Knowledge units in this area include: risk management, mission assurance, disaster recovery, business continuity, security evaluations and compliance, organizational behavior as it relates to cybersecurity, employee training, and intelligence.

- The **Societal Security** area focuses on aspects of cybersecurity that can broadly impact society as a whole for better or for worse. Knowledge units in this area include: cybercrime, cyber law, ethics, policy, intellectual property, professional responsibility, social responsibility, and cultural and international considerations

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. Again, while the associated curricular guidance will differ, knowledge units are intentionally repeated in multiple knowledge areas. 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.

3.2.3 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*[14]*"* into a coherent view of cybersecurity.

The CSEC2017 thought model includes five crosscutting concepts: Confidentiality, Integrity, Availability, Risk, and Adversarial Thinking. The cross cutting concepts are described as follows:

- **Confidentiality**: rules that limit access to system information to unauthorized persons
- **Integrity**: assurance that information is accurate and trustworthy
- **Availability**: information is accessible
- **Risk**: exposure to environmental threats
- **Adversarial Thinking**: a thinking process that considers the potential actions of the opposing force working against the desired result

[14] US National Research Council Next Generation Science Standards

3.2.4 Disciplinary Lens

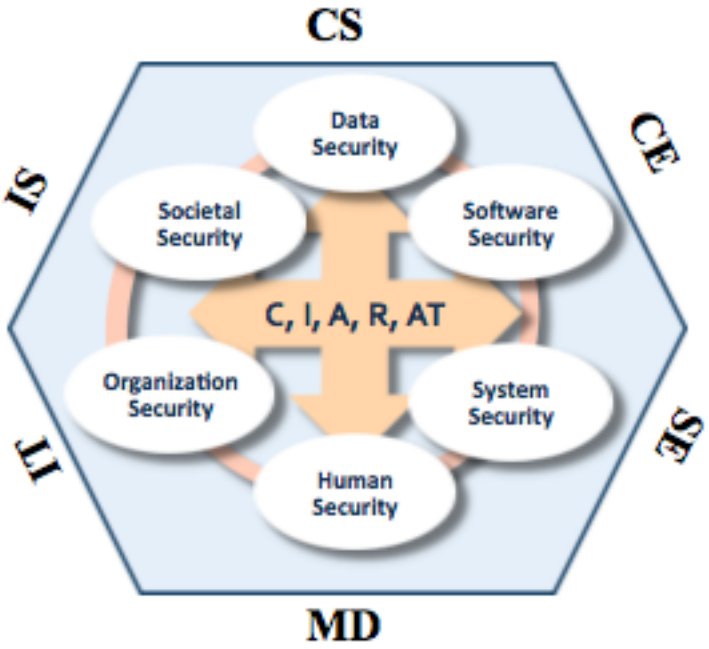
The disciplinary lens is the third dimension of the thought model. It represents the underlying computing discipline that forms the foundation of the cybersecurity program. As such, the disciplinary lens drives the approach, depth of content, and learning outcomes for each knowledge unit. It also influences the learning outcomes resulting from the interplay between the knowledge units and the crosscutting concepts.

The CSEC2017 thought model encompasses the five computing disciplines identified by the ACM: computer science, computer engineering, information systems, information technology, software engineering, and a category for mixed or cross disciplinary majors established as "informatics" or "computational" programs.

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 versus those in an information systems cybersecurity program.

3.2.5 Summary of CSEC2017 Thought Model

The dimensions of the thought model are depicted below:



- Foundational knowledge: general education and specialized cybersecurity foundations
- Knowledge areas: Data security, Software Security, System Security, Human Security, Organizational Security, and Societal Security
- Cross cutting concepts: Confidentiality, Integrity, Availability, Risk, and Adversarial Thinking
- Disciplinary lenses: Computer Science (CS); Computer Engineering (CE); Software Engineering (SE); Information Technology (IT); Information Systems (IS); and Mixed Disciplinary majors (MD)

Taken together, the combination of the dimensions provides a pathway to identify core content for learners in a range of computing-based cybersecurity programs. The application areas, described in chapter 6 of this volume, link the thought model to workforce frameworks and provide insight for connecting curricular content and career development.

Chapter 4: Curricular Content

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

4.1 Foundational Knowledge

Recommendations for the foundational knowledge are categorized into general education and specialized cybersecurity foundations.

General education. General education requirements provide an opportunity for students to learn basic communication, computational, critical thinking and analytical skills.

Foundational cybersecurity knowledge. Foundational concepts, introduce students to basic cybersecurity concepts and terms, the threat environment, common vulnerabilities, and fundamentals of information assurance.

The next draft will provide a comprehensive listing of the recommended foundational knowledge topics in each category.

4.2 Knowledge Areas

The sections below provide an overview of the curricular content for each knowledge area. For each knowledge area, the table lists 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 at the beginning of each KA subsection. In the next iteration of this work, the KAWGs will further refine the content; including the identification of specific learning outcomes and a recommended number of hours for each knowledge unit based on the disciplinary lens that is driving the curricular emphasis of a particular cybersecurity program.

Cybersecurity experts wishing to participate in the disciplinary working groups are encouraged to provide feedback on knowledge units and topics included in this report, and to express their interest through the feedback form located at http://csec2017.org.

4.2.1 Knowledge Area: Data Security

The Data Security area focuses on the protection of data at rest and in transit. This is the most narrowly focused and theoretical of the six areas, requiring the application of mathematical and analytical algorithms to fully implement. The Data Security Working Group (DSWG) includes: Keyu Jiang, Regis University; Travis Mayberry, United States Naval Academy; Travis Atkison, University of Alabama; Matthew Hudnall, University of Alabama; Faisal Kaleem, Metropolitan State; Richard Weiss, Evergreen State College; Marius Zimand, Towson University; James Walden, Northern Kentucky University; and Golden Richard, Louisiana State University. JTF members Sidd Kaza, Towson University and Allen Parrish, United States Naval Academy led this working group. The following table lists the knowledge units and component topics of the Data Security Knowledge Area.

Knowledge Unit *(KU)*	**Topics** *(Discrete content areas with each KU)*	**Description/Notes/Comments** *(Points to note: 1. The bulleted list under each topic describes the content and will be the foundation for specific curricular guidance (forthcoming)).*
Cryptography		
	Basic concepts	**Description:** • 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) • Computational security

	Advanced Concepts	**Description:**
		• Advanced protocols
		  ○ zero-knowledge proofs, and protocols
		  ○ secret sharing
		  ○ commitment
		  ○ oblivious transfer
		  ○ secure multi-party computation
		• Advanced recent developments: fully homomorphic encryption, obfuscation, quantum cryptography

	Mathematical background	**Description:** • 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 • Information theory

	Historical Ciphers	**Description:** • Shift cipher, affine cipher, substitution cipher, Vigenere cipher • Hill cipher, Enigma machine, …
	Symmetric (private key) Ciphers	**Description:** • Block ciphers and stream ciphers (pseudo-random permutations, pseudo-random generators) • Feistel networks, DES • AES • Modes of operation for block ciphers • Differential attack, linear attack • Stream ciphers, linear feedback shift registers, RC4
	Asymmetric (public-key) Ciphers	**Description:** 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 (Goldwasser-Micali, Rabin, Paillier, McEliece, …) • elliptic curves ciphers
Digital Forensics		
	Introduction	**Description:** • Definition • Limits • Types of tools (open source vs. closed source)
	Legal Issues	**Description:** • Right to privacy • 4th and 5th amendments • Protection of encryption keys under 5th amendment • Affidavits, testimony and testifying • Wiretapping
	Investigatory process	**Description:** • Alerts • Identification of evidence • Collection and preservation of evidence • Timelines, reporting, chain of custody • Authentication of evidence
	Acquisition and preservation of evidence	**Description:** • Pull-the-plug vs. triage • Imaging procedures • Acquisition of volatile evidence • Live forensics analysis
	Analysis of evidence	**Description:**

		• 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 • File carving
	Reporting, Incident Response and Handling	**Description:** • Report structures • Incident detection and analysis • Containment, Eradication and Recovery • Post Incident Activities • Information sharing
	Mobile forensics	**Description:** • Wireless technologies • Mobile device technology • Mobile OS and Apps • Mobile artifacts
Data Integrity and Authentication		
	Authentication strength	**Description:** • Multi-factor authentication • Cryptographic tokens • Cryptographic devices • Biometric authentication • One-time passwords • Knowledge-based authentication
	Password attack techniques	**Description:** • Dictionary attack • Brute force attack • Rainbow table attack • Phishing and social engineering • Malware-based attack • Spidering • Off-line analysis • Password cracking tools
	Password storage techniques	**Description:** • Cryptographic hash functions (SHA-256, SHA-3, collision resistance) • Salting • Iteration count • Password-based key derivation

	Data integrity	**Description:** • Message authentication codes (HMAC, CBC-MAC) • Digital signatures • Authenticated encryption • Hash trees
Access Control		
	Physical data security	**Description:** • Data center security, including keyed access, man trips, key cards and video surveillance. • Rack level security • Data destruction
	Logical data access control	**Description:** • 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) • Federated identities and access control
	Secure architecture design	**Description:** • Principles of a security architecture • Protection of information in computer systems
Secure Communication Protocols		
	Application-layer protocols	**Description:** • HTTP • HTTPS • SSH
	Transport-layer protocols	**Description:** • SSL/TLS
	Attacks on TLS	**Description:** • Downgrade attacks • Certificate forgery • Implications of stolen root certificates • Certificate transparency
	Internet/Network Layer	**Description:** • IpSEC and VPN
	Privacy Preserving Protocols	**Description:** • Mixnet, Tor, Off-the-record message, Signal
	Data Link Layer	• L2TP, PPP and RADIUS

Cryptanalysis		
	Classical attacks	**Description:** • Brute-force attack • Frequency-based attacks • Attacks on the Enigma machine • Birthday-paradox attack
	Side-channel attacks	**Description:** • Timing attacks • Power-consumption attacks • Differential fault analysis
	Attacks against private-key ciphers	**Description:** • Differential attack • Linear attack • Meet-in-the-middle attack
	Attacks against public-key ciphers	**Description:** • Factoring algorithms (Pollard's p-1 and rho methods, quadratic sieve, number field sieve)
	Algorithms for solving the Discrete Log Problem	**Description:** • Pohlig-Hellman • Baby Step/Giant Step • Pollard's rho method
	Attacks on RSA	**Description:** • Shared modulus • Small public exponent • Partially exposed prime factors
Privacy		
	Overview	**Description:** • Definitions (Brandeis, Solove) • Legal (HIPAA, FERPA, GLBA) • Data Collection • Data Aggregation • Data dissemination • Privacy invasions • Social Engineering • Social Media
Information Storage Security		
	Data storage technologies	**Description:** • Hard drives, Flash memory, Tapes • Redundancy (e.g., RAID) • Network-level storage

		• Cloud-based storage
	Backups	**Description:** • Local, network and cloud backups
	Disk and File Encryption	**Description:** • Hardware-level versus software encryption
	Data Erasure	**Description:** • Overwriting, Degaussing • Physical destruction methods
	Data Storage Formats	**Description:** • Database technologies, XML/JSON
	Data Masking	**Description:** TBD
	Database Security	**Description:** • Access/authentication, Auditing • App integration paradigms.
	Data Security Law	

4.2.2 Knowledge Area: Software Security

The Software Security area focuses on the development and use of software that reliably preserve the security properties of the information and systems they protect. This is the most specialized of the six knowledge areas and the least likely to be developed in depth by all cybersecurity programs. The Software Security Working Group (SSWG) includes: Bill Chu, University of North Carolina Charlotte; Melissa Dark, Purdue University; Michael Howard, Microsoft; Andrew Kornecki, Embry Riddle Aeronautical University; Gary McGraw, Synopsis; Kara Nance, Virginia Tech; Phillip Nico, Cal Poly SLO; Blair Taylor, Towson University; Michael Wertheimer, private consultant; and Alec Yasinsac, University of South Alabama. JTF members Matt Bishop, University of California at Davis and J Ekstrom, Brigham Young University led this working group. The knowledge units within this knowledge area are comprised of principles and practices. The following table lists the "principles" knowledge units and component topics of the Software Security Knowledge Area. These knowledge units have been validated by the SSWG using the OWASP Top 10 and the IEEE "Avoiding the Top 10 Software Security Design Flaws." The "practices" knowledge units are currently under development.

Knowledge Unit *(KU)*	**Topics** *(Discrete content areas with each KU)*	**Description/Notes/Comments** *(Points to note: 1. To validate the proposed content, the Software Security Working Group compared each of the principles to the OWASP Top 10 and the IEEE "Avoiding the Top 10 Software Security Design Flaws". 2. The SSWG is using a similar method to validate the topics included in the practice area curricular guidance. These topics are forthcoming.)*

Fundamental Design Principles		
	Simplicity principles	**Description:** • Economy of mechanism: security features of software should be as simple as possible. • Minimize common mechanism: Reduce sharing of resources as much as possible. • Least astonishment: The security features of software, and the security mechanisms it implements, should be designed so that their operation is as logical and simple as possible.
	Restrictive Principles	**Description:** • Least privilege: software should be given only those privileges that it needs in order to complete its task. • Fail-safe defaults: 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; also and the initial state should be to deny access unless access is explicitly required. • Complete mediation: software should validate every access to objects to ensure that they are allowed. (For example, with respect to confidentiality, integrity, and other properties.) • 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.
	Methodology Principles	**Description:** • Open design: the 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. It also 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). (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 security of changing the design if the specifications do not match an environment that the

		software is used in.)

4.2.3 Knowledge Area: System Security

The intent of the System Security knowledge area is to focus on the acts of establishing and maintaining the security properties of systems, including those of interconnected components. The components include data, software, hardware devices, networks, and humans.

NOTE: Based on community feedback we are reevaluating the system security knowledge area. Some of the knowledge units originally considered to be components of this KA have been incorporated into other KAs and we are determining the best structure for the narrowed scope of this area.

4.2.4 Knowledge Area: Human Security

The Human Security area focuses on protecting individuals' data in the context of organizations (i.e. as employees) or personal life, their privacy and threat mitigation. It also includes the study of human behavior and social engineering as it relates to cybersecurity. Human Security Working Group (HSWG) members include: Heather Lipford, University of North Carolina at Charlotte; Laurie Dringus, Nova Southeastern University; Linda Brock, IBM; Johnathan Yerby, Middle Georgia State University; Melissa Carlton, Florida State University; Steven Furnell, Plymouth University; Robert Hambly, Department of Defense; Daniel Shoemaker, University of Detroit Mercy; Karla Clarke, KPMG LLP; Alvaro Arenas, IE University (Spain); Sameer Patil, Indiana University. JTF member Yair Levy, Nova Southeastern University led this working group. The following table lists the knowledge units and component topics of the Human Security Knowledge Area.

Knowledge Unit *(KU)*	**Topics** *(Discrete content areas with each KU)*	**Description/Notes/Comments** *(Points to note: 1. Humans have responsibility to ensure the CIA of their organization and personal computer systems, while that responsibility is dependent upon each of these knowledge units. 2. Foundational/prerequisite knowledge must be covered prior to the topics presented here.)*
Identity Management		**Description:** The administration and management of electronic identities or roles, including the management of access privileges for each individual identity. **No guidance in KU level, see topics.**
	Identification and authentication of people and devices	**Description:** Determining and validating if a user or device is allowed access to a requested asset or object. **Curricular Guidance:** Overview of various access control

	(Proposed as a lecture)	methods to demonstrate the benefits and challenges of each. Topics could include overview of Network Access Control (NAC), Identity Access Management (IAM), Rules-based Access Control (RAC), Roles-based Access Control (RBAC), 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 ***(Proposed as a lab)***	**Description:** The enforcement and tracking of access control to physical assets including system hardware, network assets, backup/storage devices, etc. as well as the enforcement of identification, authorization, verification, authentication, and accountability of logical assets. For example: access may be authorized using password, a pin, card reader, or biometrics, while asset control may require centralized software. **Curricular Guidance:** Practice and hands-on exercises of various access control to physical assets including system hardware, network assets, backup/storage devices, etc. Lab example of Network Access Control (NAC), Identity Access Management (IAM), Rules-based Access Control (RAC), Roles-based Access Control (RBAC), inventory tracking methods, identity creation methods (what type of userid helps increase security with access control (i.e., abc1234, first name.last name, first initial last name)
	Identity as a service	**Description:** Cloud identity is a hosted service used to store and authenticate a person. There are multiple providers offering this service. **Curricular Guidance:** Identity management as a service (e.g. Cloud identity) brings forward issues such as: the system being out of 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	**Description:** Third-party identity service is an infrastructure built, hosted and managed by a third-party provider in order to authenticate access to services. **Curricular Guidance:** Overview of the authentication infrastructure used to build, host, and manage third-party identity services. Topics include on-premise, centralized identity services/password management tools, etc.
	Access control attacks and mitigation measures	**Description:** Attacks that circumvent or bypass the access control methods to steal data or user credentials and mitigation measures **Curricular Guidance:** 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, or spoofing attacks, multi-factor authentication, strong password policy, secure password files, restrict access to systems, etc.
Social Engineering		**Description:** The manipulation of the human mind to build trust through human interaction so it can later be used as a penetration vector to computer systems for the purpose of financial/personal gains or information theft. **No guidance in KU level, see topics**
	Types of attacks	**Description:** Different ways that cyber-criminals or malicious groups exploit weaknesses in organizations, systems, networks, and personal information **Curricular Guidance:** Overview of the different ways that cyber-criminals or malicious groups exploit weaknesses in organizations, systems, networks, and personal information used to enable a later cyber attack. Proposed topics included: phishing and spear phishing attacks, physical/impersonation, vishing (phone phishing), e-mail compromise, and baiting.
	Psychology of attacks	**Description:** The psychological and behavioral factors related to individuals falling for social engineering attacks. **Curricular Guidance:** Overview of the psychological and behavioral factors related to individuals falling for social engineering attacks. Proposed topics include: adversarial thinking, emotional responses impact decision-making, cognitive biases of risks and rewards, and trust building.
	Usability issues with message systems/browsers	**Description:** The use of message systems' and browsers' interfaces and/or user interaction that can be exploited to mislead users. **Curricular Guidance:** 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.
	Technical detection and mitigation ***(Proposed as a lab)***	**Description:** Guidance provided to individuals for preventing attacks, as well as techniques for delivering that guidance. Tools and technical approaches to detect and mitigate different social engineering threats. **Curricular Guidance:** 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 e-mail filtering, blacklist, security information and event management (SIEM) tools, and IDS/IPS.
Personal Compliance with Cybersecurity Rules/Policy/ Ethical Norms		**Description:** The personal motivation to follow the rules/policy, including intentional and unintentional behavior leading to compliance **No guidance in KU level, see topics.**
	System misuse and user	**Description:** User behavior that falls outside the rules/policy

	misbehavior	and/or ethical norms that leads to intentional and unintentional system misuse. **Curricular Guidance:** Overview of intentional and unintentional system misuse, cyber-bullying, cyber-slacking, naive behavior, and ethical dilemmas related to system security decisions.
	Incentives (internal & external)	**Description:** Methods of motivation and encouragement (internal & external) to follow the rules/policy and ethical norms. **Curricular Guidance:** Overview of internal and external motivational and encouragement methods to follow the rules/policy and ethical norms. Topics include: incentives to keep the job (especially after being educated & trained for the proper rules/policy/ethical norms, individuals are legally liable for not following the rules as employee), individuals may lose their identity/access in personal life
	Enforcement and Rules of Behavior	**Description:** The methods and techniques to compel an individual to comply with the rules/policy/ethical norms. **Curricular Guidance:** Overview of methods and techniques to get people to follow the rules/policies/ethical norms (like in 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), knowledge of accountability for not following security rule/policy/ethical norms
	Proper behavior under uncertainty	**Description:** The methods and techniques to follow/adhere when uncertain on how to respond to a security situation **Curricular Guidance:** Overview of the methods and techniques to follow/adhere to when uncertain on how to respond to a cybersecurity situation. Topics include: CyberIQ, intellectual adaptability, critical thinking, understanding the right vs. wrong choices, how to make those choices under uncertainty, rational vs. irrational thinking, ethical thinking/decisions, behavior when there is no clear process to follow (reporting/Point of Contact/Etc.)
Awareness and Understanding		**Description:** The ability to demonstrate knowledge of what action to take when a security situation arises. **No guidance in KU level, see topics**
	Cyber-hygiene	**Description:** The responsible behaviors and actions that individuals do (or not do) to protect their systems from being infected with malicious applications when connected to the Internet **Curricular Guidance:** Discussion and activities focused on the individual responsibilities (not the organization) to protect and to mitigate against cyber threats/attacks. Topics

		include: password creation, password storage, mitigation tools, (i.e., anti-virus software), how to identify safe websites, identifying levels of privacy settings, etc.).
	Cyber vulnerabilities and threats awareness	**Description:** Develop awareness for threats, as well as Fear Uncertainty, and Doubt (FUD) **Curricular Guidance:** Overview of threats as well as Fear Uncertainty, and Doubt (FUD). Proposed topics include: warnings signs of internal employee vulnerabilities and threats, awareness of identity theft, business e-mail compromise, threat of free/open WiFi networks, malware, spyware, and ransomware.
	Policy awareness and understanding	**Description:** Knowledge of regulating policies (e.g., in the U.S. HIPPA, FERPA, PIIs; in the UK GDPR) and the method or technique to take when a security situation arises. **Curricular Guidance:** Overview of regulating policies (e.g., in the U.S. HIPPA, FERPA, PIIs; in the UK GDPR) 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.
Social Behavioral Privacy		**Description:** TBD **No guidance at KU level, see topics**
	Social Media Privacy	**Description:** Privacy behaviors and concerns of users in protecting personal information when using social media **Curricular Guidance:** Overview of privacy behaviors and concerns of users in protecting personal information when using social media. Proposed topics include: limit the permissions given to applications or social networking sites to access their information or post on their behalf, users' forgetting the broader audience on social media, mistakes/forget data privacy in social media, no cleanup, interfaces and mechanisms for managing online social privacy (settings), digital legacies, disclosure frequency, online personas and multiple identity management, as well as personal/workplace boundaries of social media.
	Social theories of privacy	**Description:** Social Networking Tools/Sites **Curricular Guidance:** TBD
Personal Data Privacy and Security		**Description:** "Personal Data" (PD) is any information about an individual. PD includes information that relates to individuals in their personal capacity (e.g. an individual's home address) as well as information that relates to individuals in their professional or business capacity (e.g. an individual's business address). PD includes information provided by the individual through data collection forms and information inferred about individuals (e.g. an individual's propensity to buy a certain product or their expertise). Privacy laws generally require organizations to obtain individuals' consent before they collect, use or disclose Personal Data.

		No guidance in KU level, see topics
	Sensitive Personal Data (SPD)	**Description:** Some types of Personal Data 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. Examples of data elements always considered Sensitive Personal Data (SPD) include an individual's 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 and many more. Consent to use PD or SPD is understood to be implied when an individual voluntarily provides it or explicitly given after a notice (clearly presented with an option to agree or disagree) which explains to the individual how their personal data will be used or disclosed. If the new section titled "Personal Data Privacy and Security" then this likely belongs under that section. **Curricular Guidance:** Overview of the types of Personal Data (PD), including Personally Identifiable Information (PII), 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.).
	Personal Tracking and Digital Footprint	**Description:** Approaches and techniques to track individuals and their behaviors using their devices or tracking of digital footprint or other technologies. **Curricular Guidance:** Location tracking, Web traffic tracking, network tracking, personal device tracking, digital assistants recordings (Siri, Alexa, etc.)
	Privacy Policy	**Description:** Privacy policy is a set of rules, regulations, and/or accepted behaviors that individuals are required to follow to protect the privacy of others or themselves. **Curricular Guidance:** 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.
Human Computer		**Description:** The application of cognitive principles, ergonomics, and human factors guidelines and principles to

Interaction[15] and Usable Security		the design and evaluation of human-computer systems. Topics include display technologies, human visual capacities, design of display parameters, and image quality metrics. **No guidance in KU level, see topics**
	Human Security Factors	**Description:** Incorporates aspects of psychology, systems engineering, and computer science toward the improvement of the interface between operator and equipment. **Curricular Guidance:** 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.
	Usable Security	The balance in use and integration of security vs. the ease of using it, while minimizing the increase in stress and anxiety during usage. The trade-off between security and usability, minimization of unintentional errors, while a secure system will aim at ensuring that undesirable actions in a system are prevented or mitigated. Moreover, including the aspect of user experience, which incorporate how users interact with systems, how people perceive and learn about using secure systems, as well as how people react and adapt to technologies. **Curricular Guidance:** Overview of the philosophy that secure systems are socio-technical systems, thus concern must be for the improvement of the effectiveness of security systems, but also on reducing human and financial costs associated with operating it. Proposed topics should include: trade-off between security and usability, usability with existing cybersecurity tools, user perceptions of cybersecurity and privacy in cyberspace, usability evaluation, applied psychology and security policies, security economics, responsibility, liability, and self-determination, complex security and privacy solutions vs. complexity on the user side, poorly designed security interfaces, trust (systems & other individuals), safety (non-abstract concept), incentives for users to value security and privacy solutions, reduce or remove the user's burden when using security systems, understand how users evaluate and make decisions regarding security, usability vs. utility of security systems including user attributes (user errors, memorability, accessibility, ease of use, predictability, repeatability, visibility, & trust), end user requirements and definition (description of what is needed of the user who wants to perform tasks), usability testing of security

[15] See CS UG Curriculum Guidelines (2013) on an elective course in "HCI/Human Factors and Security"

		mechanisms/secure systems, to understand what users perceive and to evaluate what users do.

4.2.5 Knowledge Area: Organizational Security

The Organizational Security area focuses on protecting organizations from cybersecurity threats and on managing risk to support the successful accomplishment of the organization's mission. Organizational Security Working Group (OSWG) members include: Phillip Mahan, Private sector; Hossain Shahriar, Kennesaw State University; Wasim Alhamdani, Imam Abdulrahman bin Faisal University; William Mahoney, University of Nebraska, Omaha; Gordon Shenkle, Private sector; Gerhard Steinke, Seattle Pacific University Timothy Cullen, Private sector; Samir Tout, Eastern Michigan University. JTF member Herbert Mattord, Kennesaw State University led this working group. The following table lists the knowledge units and component topics of the Organizational Security Knowledge Area.

Knowledge Unit *(KU)*	**Topics** *(Discrete content areas with each KU)*	**Description/Notes/Comments** *(Points to note: 1. Organizations have responsibility to meet the needs of many constituencies and those needs must inform the delivery of each of these knowledge units. 2. Foundational/prerequisite knowledge must be covered prior to the topics presented here.)*
Security Policy and Governance		**Description:** Each organization addresses its operating environment, internal and external, through policy and governance. SPG seeks to place constraints on the behavior of its members. **Curriculum Guidance:** The implementation of security governance and policy should be framed within global, national, and local laws, regulations and standards. Curriculum 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. Notes: Graduates should be able to: • Identify the relevant security policies for a particular organizational sector, business vertical (e.g. education, finance, health care), and national operating environment. For instance, a U.S. federal government agency must adhere to a set of security profiles such as FIPS and HIPAA; while a U.S. corporate entity would focus on compliance with GLB, SOX, as well as HIPAA and PCI. • Apply policies to the current environment potential

		future states (e.g. organizational growth, market changes). • Integrate general guidelines with vertical specific requirements.
	Organizational Context	**Description:** Many factors influence how security is operationalized in organizations. These contexts are critical when designing a curriculum and should inform the entire process. **Curricular Guidance:** Internal vs. external contextual differences have a major impact on the coverage of policy, regulation, and statute (or jurisdiction). Also, location/country specific issues and concerns should be evaluated. Applicable standards and guidelines for compliance to industry/ sector should also be evaluated. The variance between government vs. 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.
	Privacy	**Description:** 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. **Curricular Guidance:** Social and localized variances in privacy should be addressed. 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.
	Laws, Ethics, and Compliance	**Description:** Laws, regulations, standards as well as ethical values are derived from the social context and how organizations meet requirements to comply with them. Curricular Guidance: Content should include 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 cyber attacks. Ethical instruction should aso 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 would include GDPR and ISO/IEC 27000 et al.. National laws of importance for US organizations include HIPAA, Sarbanes-Oxley, GLBA etc.
	Security Governance	**Description:** The principles of corporate governance are applicable to the information security function. Executive management has a responsibility to provide strategic direction, ensure the accomplishment of objectives, oversee that risks are appropriately managed, and validate responsible resource use. **Curricular Guidance:** Programs of instruction should seek to convey the concepts with clarity and sound examples.
Analytical Tools		**Description:** A set of techniques using data analytics to recognize, block, divert, and respond to cyber attacks. 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 **Curricular Guidance:** Coverage in this topic should include definitions, differences between security control and security analytic software and tools. Type and classifications of analytic tools and techniques, examples (OpenSOC, ...), collect, filter, integrate and link diverse types of security event information; How security analytics tools work, relationship between analytic software and tools and forensics; differences between forensic tools and analytic tool ; network forensic (to include packet analysis, tools, Windows, Linux, UNIX, Mobile); differences between cyber forensic (social media for example); and network forensics.
	Security Metrics	**Description:** Metrics are effective tools to discern the effectiveness of the components of their security programs and drive actions taken to improve a security program. **Curricular Guidance:** Coverage in this topic should include the elements of security metrics, 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 • Use of security metrics in security program evaluation, audition, and performance.
	Security Intelligence	**Description:** Collection, analysis, and dissemination of security information including but not limited to threats and adversary capabilities. **Curricular Guidance:** Tools and techniques should be explored to include data collection & aggregation, data

		mining, data analytics, statistical analysis. Examples of sources for security intelligence include SIEM for internal data, public and private intelligence services for external data. Dissemination includes an understanding of information sharing models such as the Information Sharing and Analysis Center (ISAC model in the U.S.) approach as well organizations like U.S. FBI Infragard.
Systems Administration		**Description:** 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	**Description:** OS administration is upkeep, reliable operation, configuration, and troubleshooting of technical systems, especially multi-user systems and servers. **Curricular Guidance:** Content should include but not 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	**Description:** Database administration is managing and maintaining of databases by utilizing available and applicable management system software. **Curricular Guidance:** Content should include but not 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	**Description:** Network administration relates to installation, and supporting various network system architectures (LANs, WANs, MANs, intranets, extranets, DMZs, etc…), and other data communication systems. **Curricular Guidance:** Content should include but not limited to OSI Model, securing of network traffic, tools for configuration of services.
	Cloud Administration	**Description:** 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 and released with minimal oversight. **Curricular Guidance:** Content should include but 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	**Description:** 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. **Curricular Guidance:** Content should include but 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	**Description:** Securing a system by finding and remediating risks. This may include hardening or securing configuration, system software, firmware, and application. **Curricular Guidance:** Content should include but not limited to identifying risks, threats, and vulnerabilities in commonly used systems (operating systems, database systems, networks), define and administering procedures and practices to safeguard against threats, hardening through suitable tools (firewall, antivirus, IDS, honeypot).
	Availability	**Description:** Sound system operation requires all systems sustain targeted levels of availability by having their current state recoverable from failure through redundancy and backup & recovery. **Curricular Guidance:** Content should include but not limited to identifying key assets and administering tools to have validated system backup and recovery.
Cybersecurity Planning		
	Strategic Planning	**Description:** 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. **Curricular Guidance:** This should cover concepts such as determining the current organization's position, performing SWOT Analysis, developing a strategy that fulfills the mission, values, and vision of the organization, determine long-term objectives, selecting Key Performance Indicators (KPIs) to track progress, allocate the necessary budget, rollout the strategy to the organization, and update and adapt yearly.
	Operational and Tactical Management	**Description:** The organization ability to securely operate organizational technical infrastructure. **Curricular Guidance:** Data protection and privacy by default and design should be discussed and would include 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.
	Executive and Board-level Communication	**Description:** Delivering information to executives and external decision makers is a critical skill for information security leaders. **Curricular Guidance:** Communication skills should be taught and practiced with rehearsals that include critical analysis and meaningful feedback.
	Business Continuity / Disaster Recovery *[Note: this may need to be raised a level and stand as separate KU]*	**Description:** Description of the role DR plays within BC. Business Continuity Planning includes emergency response, 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. **Curricular Guidance:** Should include: subjects to include in a DR/BP plan, organization of the plan, occasions to review/rewrite the plan, and the examination of sanitized plans. All students should gain experience in writing DR/BP plans by preparing drafts for their home, family business, or similar.
Security Program Management		
	Project Management	**Description:** Project management is the application of knowledge, skills, tools, and techniques to project activities to meet the project requirements. **Curricular Guidance:** Project integration, project scope management, project time and cost management, quality management, human resource considerations, communications, risk management, and procurement management.
	Resource Management	**Description:** 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. **Curricular Guidance:** Current practices in resource management, specifically in the context of projects typical of cybersecurity should be explained and developed.
	Quality Assurance / Quality Control	**Description:** Quality assurance and control is a method used to prevent mistakes that 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. **Curricular Guidance:** Current practices in QA/QC,

		specifically in the context of projects typical of cybersecurity should be explained and developed.
Personnel Security		
	Security Awareness, Training and Education	**Description:** Avoidance and/or proper use of fear, uncertainty, and doubt (FUD) as a tool for awareness. **Curricular Guidance:** Physical Security, Desktop Security, Password Security, Wireless Networks Security Phishing, File Sharing and Copyright, Browsing, Encryption, Insider Threat, International Travel, Social Networking, Social Engineering.
	Security Hiring Practices	**Description:** TBD **Curricular Guidance:** Review of fictional resumes, fictional background checks, fictional acted out interview techniques, fingerprint analysis results, financial review (fictional Credit Check results) etc.
	Security for Contractors and Consultants	**Description:** TBD **Curricular Guidance:** Include topics such as evaluating vendors, resumes, statements of prior performance.
	Security in Review Processes	**Description:** TBD **Curricular Guidance:** TBD
	Security and Termination Practices	**Description:** Recommended techniques for securely ending employment for personnel. **Curricular Guidance:** Hostile termination techniques, timeframes for terminating access to accounts, to include workspace, VPN, terminal, PC, Server, email, Active Directory, Security (Police?) escort from building, etc.
	Special issue in Privacy of Employee Data	**Description:** TBD **Curricular Guidance:** Include discussions of relevant laws (e.g. U.S. - HIPPA, EU – General Data Protection Regulation (GDPR))
	Staffing the Security Function	**Description:** TBD **Curricular Guidance:** TBD
Risk Management		**Description:** Risk Management is finding and controlling risks to organizational information assets.
	Identifying assets, threats, vulnerabilities, and consequences	**Description:** 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 organization to maintain awareness and reactive capacity for existing and emerging threats.

		Curricular Guidance: In the U.S. NIST SP 800-30 serves as an outline for the elements to be included; as does ISO/IEC 27001. (Additional guidance on threat intelligence will be included)
	Risk Assessment and Analysis	**Description:** 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. **Curricular Guidance:** For example, "The Accidents Organizations Make" as a case reference. See also, https://www.ntsb.gov/news/speeches/RSumwalt/Documents/Sumwalt_012511.pdf Differentiation of safety engineering versus security engineering.
	Insider Threats	**Description:** Malicious human behavioral factors that might cause harm as a result of a conscious violation of trust, or best-use, or inadvertent error. **Curricular Guidance**: Motive-means-opportunity behaviors - motivation and discipline factors accountability, awareness and quality control In the U.S., the FBI has developed materials including indicators useful in identifying potential insider threat risks. Definitions: • Insider - Any person with authorized access to an organization's resources to include personnel, facilities, information, equipment, networks, or systems. • Insider Threat - The risk an insider will us 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.
	Risk Measurement and Evaluation Models and Methodologies	**Description:** 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. **Curricular Guidance:** Curriculum content should include 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 Cyber Resilience Review self-assessment, Cybersecurity Evaluation Tool (CSET) as well as Security Risk Assessment tool from HSS.
	Risk Control	**Description:** The act of lessening the consequences of a cyber event, and as a result lessening the amount risk. Each approach should include means to communicate risk to

		decision makers including the *residual risk*. (Avoid, Reduce, Transfer, Accept) **Curricular Guidance:** Widely used risk control methodologies are available for exposure and practice..
Security Operations	***Supply Chain Security***	**Description:** Efforts to enhance the security of the origin and traceability of sourced system components, such as externally produced hardware or software **Curricular Guidance:** TBD
	Global Security Operations Centers (GSOC)	**Description:** Optimized processes can add value to broad organizational operations centers that intersect physical security and cybersecurity. **Curricular Guidance:** 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 SOC's. The operations center should also be knowledgeable in "chain of evidence" procedures in the event that the attack is determined to be need of Local or Federal investigation. Also, if the attack digest needs to be disseminated to other SOC's, the "Chin of Evidence" would need to be adhered to.]

4.2.6 Knowledge Area: Societal Security

The Societal Security area focuses on aspects of cybersecurity that can broadly impact society as a whole for better or for worse. Societal Security Working Group (SSWG) members include: Flo Appel, Saint Xavier University; David Aucsmith[1]; Scott Bell[1], North West Missouri State University; Ryan Calo, University of Washington; Yoshi Kohno, University of Washington; Jeff Kosseff, United States Naval Academy; Mary Manjikian, Regent University; Martin Libicki, United States Naval Academy; James Smith, NOVA Southeastern University; and Samuel Visner. JTF members Scott Buck, Intel and Elizabeth Hawthorne, Union County College led this working group. The following table lists the knowledge units and component topics of the Societal Security Knowledge Area.

Knowledge Unit *(KU)*	**Topics** *(Discrete content areas with each KU)*	**Description/Notes/Comments** *(Points to note: 1. The descriptions and curricular guidance for many of the knowledge units are currently under development.)*
Cybercrime		**Description:** 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.
	Cyber Criminal Behavior	**Description:** TBD
	Cyber Terrorism	**Description:** Activities in cyberspace geared to generate societal fear and uncertainty
	Cyber Criminal Investigations	**Description:** TBD
	Digital Evidence: Chain of Custody	**Description:** TBD
	Cyber-focused crimes	**Description:** TBD
	Cyber-assisted crimes	**Description:** TBD
	Economics of Cybercrime	**Description:** TBD
	Dark Web	**Description:** TBD
Cyber law		**Description:** This knowledge unit aims to provide students with a broad understanding of the current legal environment in relation to cyberspace. **Curriculum Guidance:** The topics include international laws, as well as the application of jurisdictional boundaries in cyber-based legal cases. Students should develop a strong understanding of current applicable legislation and a strong background in the formation of these legal tools. Additional content should include: Government Surveillance Statutes (i.e. in the US, Stored Communications Act, Wiretap Act, and Pen Register Act);

		Cybersecurity Litigation (i.e., what do data breach victims need to demonstrate in order to establish standing to sue?); Cyber Threat Information Sharing Laws (i.e., the US Cybersecurity Act of 2015's information sharing provisions and U.S.-CERT); and International Legal Issues (primarily looking at how the U.S. government and companies can pursue criminal and civil claims against hackers located in other countries, the Budapest Convention, etc.).
		Description: TBD **Curricular guidance:** The specific content will be driven by the country of focus. In the US, the focus would be on Constitutional Foundations of Cyber Law: Executive Power (Article II); Legislative Power (Commerce Clause and other sources of authority in cyber); First Amendment; Fourth Amendment; Tenth Amendment
	Military and civilian cyber law	**Curricular guidance:** The specific content will be driven by the country of focus. In the US, Posse Comitatus; Title 10 and 50 authorities
	Intellectual property	**Curricular guidance:** The specific content will be driven by the country of focus. In the US, Section 1201 of the Digital Millennium Copyright Act
	Digital Evidence: Digital Forensics	**Description:** TBD
	Privacy Laws	**Curricular guidance:** The specific content will be driven by the country of focus. In the US, Section 5 of the FTC Act; GLBA Privacy Rule; HIPAA Privacy Rule; California Online Privacy Protection Act; Children's Online Privacy Protection Act; Identity Theft Laws
	Data security law	**Curricular guidance:** The specific content will be driven by the country of focus. In the US, Section 5 of the FTC Act GLBA Safeguards Rule; HIPAA Security Rule; State data breach notification laws; State data security laws; Private data security litigation; PCI/DSS
	Computer hacking laws	**Curricular guidance:** The specific content will be driven by the country of focus. In the US, Computer Fraud and Abuse Act; Counterfeit Device Law; Economic Espionage Act
	Digital contracts	**Curricular guidance:** Clickwrap/Browsewrap distinction
	Multi-national conventions about cyber law (accords)	**Curricular guidance:** Include topics such as: Jurisdictional limitations; Budapest Convention
	Cyber Threat Information Sharing	**Curricular guidance:** The specific content will be driven by the country of focus. In the US, Cybersecurity Act of 2015
	Cross-Border Privacy and Data Security Laws	**Curricular guidance:** GDPR; Privacy Shield
Cyber Ethics		**Description:** 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 individual and group (professional) level. It also sensitizes students to debates about whether ethics in IT 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.
	Cyber ethical frameworks	**Curricular guidance:** TBD
	Cyber normative theories	**Curricular guidance:** TBD
	Professional ethics and codes of conduct	**Curricular guidance:** TBD
	Ethics and Law	**Curricular guidance:** Include learning outcomes for students to: o Evaluate the relationship between ethics and law; o Describe civil disobedience and its relation to ethical hacking; o Describe criminal penalties related to unethical hacking; and o Apply notion of Grey Areas to describing situations where law has not yet caught up technological innovation
	Ethics and Conflict	**Curricular guidance:** Include learning outcomes for students to: o Articulate Just War Principles o Apply Just War Principles to cyberspace in relation to conflict initiation o Apply Just War Principles to cyberspace in relation to behaviors in conflict o Apply Just War Principles to cyberspace in relation to conflict cessation/post conflict situation o Describe ethical problems created in conduct of cyber espionage o Describe norm and rule violation as it relates to cyber terrorism
	Defining Ethics	**Curricular guidance:** Include learning outcomes for students to: o Compare and contrast major ethical stances – including virtue ethics, utilitarian ethics and deontological ethics o Apply the three different ethical stances in thinking through the ethical consequences of a particular problem or action o Articulate a position regarding the uniqueness debate: are ethical problems in cyberspace unique to cyberspace or an extension of existing ethical issues in real space o Identify Key thinkers whose work can provide a model for ethical behavior in cyberspace == including Kant, Rawls, Bentham.
	Autonomy/Robot Ethics	**Curricular guidance:** Include learning outcomes for students to: o Define autonomous decision-making o Define artificial intelligence and describe ethical dilemmas presented by the use or employment of AI o Describe legislative advances which have defined personhood and digital personhood o Describe the conflict created by legal notions of responsibility and the use of unmanned or

		autonomous decision-making programs
	Ethics and Equity/Diversity	**Curricular guidance:** Include learning outcomes for students to: o Describe the ways in which decision-making algorithms may over-represent or underrepresent majority and minority groups in society o Analyze the ways in which algorithms may implicitly include social, gender and class biases o Describe ways in which spaces can be regulated in cyberspace in order to create a space where all voices are heard
	Anticipatory Ethics	**Curricular guidance:** Include learning outcomes for students to: o Name at least three ethical issues which may present themselves in the future, looking at the evolution of computer technology o Describe how the computer professional can anticipate and prepare for ethical challenges, including making engineering decisions which address or preempt these challenges
	Ethics and Credibility of Information	**Curricular guidance:** TBD
Policy		**Description:** 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. **Curricular guidance:** Students will be expected to gain an understanding of questions relating to the use of cyber as an instrument of war, and to distinguish between the use 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 will also be 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.
	Cyber War and Strategy	**Curricular guidance:** TBD
	International Cyber Laws and Policy	**Curricular guidance:** TBD
	U.S. Cyber Policy	**Curricular guidance:** TBD
	Intellectual Property	**Curricular guidance:** TBD
	National Cyberspace Interests	**Description:** How a country defines its interest in cyberspace
	Cybersecurity and National Security	**Description:** How a country defines its cybersecurity policy and doctrine. This includes National Cybersecurity Policy Architecture, Signals and Narratives, and Coercion and Brandishing. **Curricular guidance:** To include o Understanding how a country assigns policy, doctrine, and execution responsibility

		○ A country's cybersecurity message ○ How a country signals its intentions to gain other countries' attention and cooperation
	Cybersecurity and Statecraft	**Description:** Concepts include Coercion and Brandishing, Deterrence, Escalation, Signals and Narratives
	Cyber-in-War versus Cyberwar	**Description:** To include concepts such as Cyber-in-Warfare Cyberwar; Cyberwarfare as an element of information warfare; Strategic Implications Escalation and Deterrence **Curricular guidance:** ○ The integration of cyber as an aspect of military operations ○ The concept of conflict fought in and for the domination of cyberspace ○ Cyber-in-War as a component of information dominance in warfare ○ How cybersecurity changes a country's strategic posture ○ Escalation of crises in cybersecurity; challenges of detecting and deterring cyber exploits and attacks significant to national security
	The New Adjacencies to Diplomacy	**Description:** Delicate dance of cyber diplomacy **Curricular guidance:** How have aspects of cybersecurity become part of the relationships between countries ○ The covert collection of information, alongside the practice of diplomacy ○ The covert application of cyber force in cyberspace and physical space - between diplomacy and war ○ Computer Network Exploitation - the New Intelligence ○ Computer Network Attack - the New Covert Action
	Cyberspace Operations	**Description:** **Curricular guidance:** Include ○ Element of Military Operations and associated strategic implications ○ International security including Potentials and Limitations, and Cybersecurity and the Balance of Power ○ Norms of behavior including laws of armed conflict, domain sovereignty
	Strategic Cyberwar	**Description:** **Curricular guidance:** Include ○ Potentials and Limitations ○ Cybersecurity and the Balance of Power
	Cybersecurity and "the New Normal"	**Description:** **Curricular guidance:** Includes ○ Cybersecurity as an aspect of intelligence. ○ Cybersecurity as an aspect of covert action
	The National Economic	Description:

	Implications of Cybersecurity	Curricular guidance: What does cybersecurity cost a nation? What is lost? What must be invested? What can be gained?
Privacy		
	Privacy Norms and Attitudes	**Curricular guidance:** Include o Establish conditions for the use of a Privacy Calculus, in which individuals are asked to furnish personal information or access to personal information in return for a discount or convenience o Recognize cultural differences in the existence of privacy norms o Demonstrate an understanding of privacy boundaries in their culture.
	Privacy Rights	**Curricular guidance:** Include o Describe Informed Consent conditions in relation to personal data collection and sharing o Recognize national privacy rights in the existence of privacy rights o Demonstrate familiarity with the debate about the universal human right to privacy.
	Safeguarding Privacy	**Curricular guidance:** Include o List cyber-hygiene steps to safeguard personal privacy o List Privacy-Enhancing Technologies and their use and the properties that they do and do not provide (i.e. Tor, encryption) o Describe conditions for ethical and lawful use of Privacy Enhancing Technologies o Describe steps in carrying out a Privacy Impact Assessment o Describe the role of the data trustee o Describe legislation related to data localization practices o Demonstrate an understanding difference between privacy rights and privacy enhancing capability - operationalizing privacy o Discuss the dynamic impact of meta data and big data on privacy.
	Defining Privacy	**Curricular guidance:** Include o Apply operational definitions of privacy o Identify different privacy goals, e.g., confidentiality of communications, privacy of metadata o 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)
	Addressing Privacy Breaches	**Curricular guidance:** Describe the role of the corporation in protecting data and addressing circumstances when data privacy is compromised
	Privacy in Societies ~~***Democracy***~~	**Curricular guidance:** Describe privacy rights related to public figures as well as threats to privacy for public figures, and define differential surveillance and give examples

	Ethical Limits of Privacy	**Curricular guidance:** Include o Describe criminal penalties for privacy violations (i.e. cyberstalking) o Discuss ethical and legal limits on individual surveillance o Demonstrate awareness of contemporary issues and legal principles in privacy (e.g., 4th Amendment in U.S.)
	Privacy and Professionalism	**Curricular guidance:** Describe specific social sectors which incorporate a norm or regulation regarding privacy (i.e. FERPA, HIPAA, ABA standards for lawyers)
Global Impacts		**Description:** The Cyber Global Impacts Policy Unit is intended to help students understand and analyze the effects of cyber on the international system generally and on international security more specifically. Students will be challenged with understanding 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. Students will be given the opportunity to examine and discuss possibilities for the global governance of cyber, and to examine the possibilities also of the development of normative behavior relate to cyber's use. The Knowledge Unit will also examine the effects of cyber on the global economy. Students will be asked to demonstrate original thinking regarding the emergence of cyber as a factor in the international system, and the implications of this factor for that system's development and structure in future.
	Internet governance	**Description: TBD** **Curricular guidance: TBD**
	Cyber Espionage	**Description: TBD** **Curricular guidance: TBD**
	Cyberspace Operations	**Description:** **Curricular guidance:** o Laws of Armed Conflict - Explore the role of cyberspace operations vis-a-vie the laws of armed conflict o Norms of Behavior - Explore such questions as - Should constraints exist for national behavior? What might those constraints be?
	Global Governance in Cybersecurity	**Description:** Explore such questions a**s -** How is cybersecurity to be governed? Are all countries equal? Do we need collective security?
	Cybersecurity, Privacy, and Global Human Rights	**Description:** Explore such questions as - Do we need a global regime in respect to privacy, human rights, and freedom of expression and collaboration?
	Cyberspace as a Sovereign Domain Versus the Global Commons	**Description:** **Curricular guidance:** Explore such questions as - Is cyberspace a global commons? Do we apply universal jurisdiction? Is cyberspace a domain in which governments have sovereign prerogatives? If cybersecurity is not a global commons, how can it be bordered, segmented? Can it be governed separately by individual countries? Should it be?
	Cybersecurity and the	**Description:**

	Balance of Power	**Curricular guidance:** Explore such questions as - Is cybersecurity changing the balance of power among countries, between countries and non-state actors? How is it affecting international security? o Joe Nye proposes the analysis of cyber power at the national, multi-polar, and non-polar levels. What implications exist at each level? o How should we consider cybersecurity in the context of other models (traditional power models, Doran's Power Cycle Theory, etc.?)
	Global Economic Implications of Cybersecurity	**Description:** Explore such questions as - What does cybersecurity cost the international economic system? Does it undermine global institutions? Can we compensate? How?
Digital Forensics		**Description:** This knowledge unit provides an overview of digital forensics and cyber investigations from both the technical and legal perspectives. Topics and student learning outcomes focus on the recovery and investigation of potential evidence found in digital and IoT devices as well as in the "cloud", often in relation to computer crimes.
Professional Responsibility	***Professional responsibility for cyber professionals***	**Description:** Identify relationship between professionalism and ethics
Social Responsibility	***Ethical hacking***	**Description:** **Curricular guidance:** o Describe steps for carrying out ethical penetration testing o Describe 'ethical hacking' principles and conditions o Distinguish between ethical and unethical hacking o Distinguish between nuisance hacking, activist hacking, criminal hacking and acts of war
	Privacy	**Description:** Describe ethical responsibilities of computer professional in relation to safeguarding privacy
	Intellectual Property	**Description:** Describe ethical responsibilities of computer professional in relation to respecting and protecting intellectual property
	Surveillance	**Description:** Describe ethical responsibilities of computer professional in relation to implementing ethical surveillance
	Including Values in Design	**Description:** Designing for Privacy Designing for Security

4.3 Recommended Hours per Knowledge Area

Sections 4.3 – 4.5 will be developed by leveraging the work of the knowledge area working groups. Cybersecurity experts interested in joining the working group process are encouraged to contact the JTF through the csec2017.org website.

The final version of the CSEC2017 report will provide initial recommendations, along with the rationale, for the number of hours for each knowledge area by knowledge unit and disciplinary lens. The current plan is to provide recommended hours by discipline and in summary form using a table structured as follows:

KA: Data Security	DL CS	DL CE	DL SE	DL IT	DL IS
KU 1					
Topic 1					
Topic 2					
…					
KU 2					
Topic 1					
Topic 2					
…					
KU 3					
…					
…					
…					
Total					

4.4 Course Guidance

Because curricular content can be distributed throughout the curriculum in a number of ways, this document does not provide specific guidance on courses. Rather, the CSEC2017 report will provide recommendations on the number of hours per topic within the context of each discipline. This structure allows for maximum flexibility as academic institutions seeks to develop programs within their specific environments. However, academic institutions seeking specific course guidance are encouraged to review the program exemplars, which will be included in the appendix of the final report. Institutions or individuals wishing to discuss how their programs and courses might be included as exemplars are encouraged to provide feedback on this report and to express their interest through the feedback form located at http://csec2017.org.

4.5 Learning Outcome Guidance

Learning outcomes describe what a student should know or be able to do at the conclusion of each topic. The learning outcome guidance to be included in the CSEC2017 report will follow the definition and structure of the CS2013 report by defining three levels of mastery:

- Conceptualization: The learner understands the essence of the concept and has an awareness of its meaning. This learning outcome answers the question "What do you know about this?"
- Application: The learner is able to use or apply a concept. This learning outcome answers the question "What do you know how to do?"
- Interpretation: The learner is able to apply the concept in multiple contexts, select an appropriate approach from understood alternatives, and consider a concept from multiple viewpoints. The learning outcome answers the question "Why would you do that?"

The final version of the CSEC2017 report will provide initial recommendations, along with the rationale, for the learning outcomes associated with each topic.

Chapter 5: Industry Perspectives on Cybersecurity

The field of cybersecurity is in the formative stages of development and is experiencing growing pains as the need for the discipline is recognized throughout industry. While the discipline has grown in past decades, cybersecurity has been frequently discounted or overlooked as a critical success factor across business, industry, government, services, organizations, and other structured entities that use computers to automate or drive their products or services efficiently. There is a growing consensus that this must change.

People seeking careers in cybersecurity have a great potential for success. Findings from the International Information Systems Security Certification Consortium $(ISC)^2$ workforce survey predict that by 2020 there will be a global shortage of 1.5 Million cybersecurity professionals (National Institute of Standards and Technology / National Initiative for Cybersecurity Education (NIST/NICE) Workforce Demand Report, 2015). 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 often do not have the attributes to fill the needs of industry. Perhaps they have technical skills acquired from their studies, but they lack other skills needed "to fit" within an industry or government environment.

5.1 The Academic Myth

Students who graduate from a four-year university program assume that the baccalaureate degree is a sufficient qualification to attain a position. This understanding may be true in some fields, but not necessarily in the computing disciplines nor specifically in cybersecurity. Belief in this myth has stymied many a job hunter worldwide. The degree credential is growing in importance, but it is not a sufficient condition for a position. A general understanding exists in cybersecurity and other fields that a successful professional must be a good communicator, a strong team player, and a person with passion to succeed. Hence, having a degree is not sufficient to secure employment.

Some people believe that a graduate of an cybersecurity program who has a high grade-point-average (GPA) is more likely to attain a position than one who has a lower GPA. This is another mythical belief. A graduate having a high GPA is commendable. However, if s/he does not have the passion and drive, does not work well in teams, and does not communicate effectively, chances are that the person will not pass the first interview.

5.2 Non-technical Skills

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 US 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[16]. Professional associations such as (ISC)[2] and ISACA also provide recommendations for non-technical skills required for cybersecurity professionals.

5.3 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.

5.4 Sector-based Industry Needs

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. These sector specific needs will be explored further in subsequent versions of this report.

5.5 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 both technical and soft skills exposure during their academic career.

Adaptability is a personality trait that is especially important within the cybersecurity industry, and will be very important for career success in the future. We find that adaptability describes the ability "to adjust oneself readily to different conditions"[17]. Employees 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

[16] US Chief Human Capital Officers Council Competency Model for Cybersecurity https://www.chcoc.gov/content/competency-model-cybersecurity

[17] Reference: http://www.dictionary.com/browse/adaptable

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"[18]. 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 university, 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[19].

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 desire goal of a useful cybersecurity education—to graduate and secure a position that can lead to career fulfillment and growth.

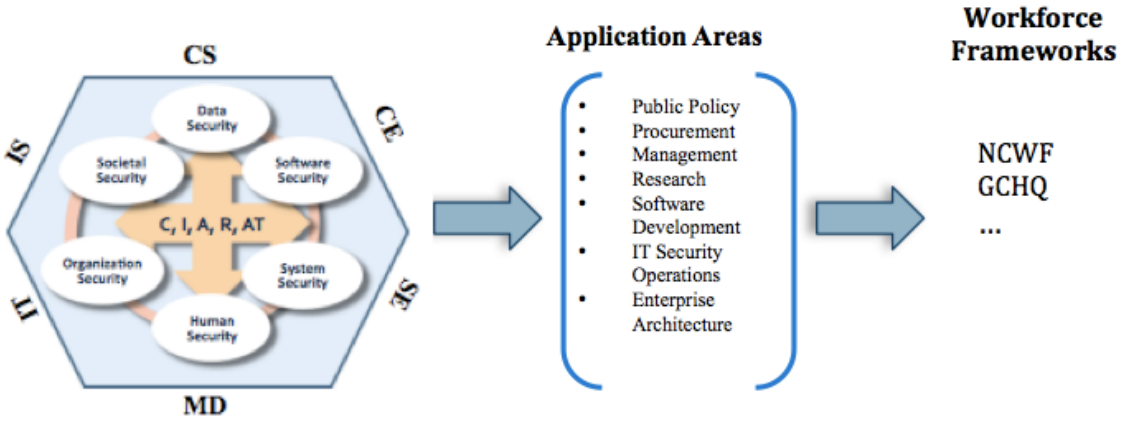
A cybersecurity advisory board can help academic programs provide students with important networking within the broader cybersecurity industry and the specific employment options in cybersecurity that will also help them to perform successfully in the interviewing process. Often, advisory boards act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

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

Chapter 6: Linking Cybersecurity Curriculum to Professional Practice

Cybersecurity practices refer to the combination of knowledge and skills required to perform in the field. Practices are a critical consideration in cybersecurity education. The CSEC2017 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. In subsequent versions of the CSEC2017 report, the contents included in each application area will be fully explored.



6.1 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 management (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. As the design of a system, and the process in which the organization uses it, affect the way compliance is implemented and tested,

they must understand the basics of design. This leads to the need to understand what a computing system can, and (perhaps more importantly) cannot, so. 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 project(s) 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 in order to ensure 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, both by understanding 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 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.

6.2 Training and Certifications

In the field of cybersecurity, knowledge acquisition and skill development, even at the undergraduate level, occurs in both formal higher education settings and professional development training and certification space. The relationship between these educational settings, and recommendations for collaborative initiatives will be explored in subsequent versions of this report.

6.3 Workforce Frameworks

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; within the context of the larger economic environment. In the field of cybersecurity, nations have begun to develop workforce frameworks to outline skill requirements and support workforce development initiatives. In the US, the National Initiative for Cybersecurity Education

National Cybersecurity Workforce Framework (NCWF)[20] is being developed as a comprehensive resource to describe cybersecurity work.

6.4 NCWF Implementation Roadmaps

The final version of this report will provide course roadmap exemplars that describe a pathway for knowledge acquisition that links the ACM CSEC2017 Curricular Guidance to the US National Cybersecurity Workforce Framework. The first exemplar will focus on linking the foundational KSA - *K0004: Knowledge of Cybersecurity Principles* as outlined in the NCWF to Work Roles within the *Oversee and Govern (OV)* category and will develop course roadmaps for the work roles in the six specialty areas within the *Oversee and Govern (OV)* category.

Specialty Area	**Work Roles**
Legal Advice and Advocacy (LG)	Cyber Legal Advisor; Privacy Compliance Manager
Training, Education, and Awareness	Cyber Instructional Curriculum Developer; Cyber Instructor
Cybersecurity Management	Information Systems Security Manager; COMSEC Manager
Strategic Planning and Policy	Cyber Workforce Development and Manager; Cyber Policy and Strategy Planner
Executive Cyber Leadership	Executive Cyber Leadership
Acquisition and Program/Project Management (PM)	Program Manager; IT Project Manager; Product Support Manager; IT Investment/Portfolio Manager; IT Program Auditor

Each course roadmap will (a) provide a rationale for knowledge and its importance for the specific work role; (b) identify and describe relevant courses and course modules; (c) outline strategies for obtaining the knowledge when specific courses are not available or accessible within the institution; and (d) highlight challenges (and associated strategies to overcome them) to following the suggested course of study.

[20] National Cybersecurity Workforce Framework: http://csrc.nist.gov/nice/framework/

The above graphic shows how the roadmaps will link the curricular guidance and the workforce framework. Below, each roadmap element is described in greater detail.

6.4.1 KSA Rationale

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

6.4.2 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 will be critical to include specific content in this section, not simply a listing of course titles. This section of the roadmaps will also include strategies for independent study courses and other customizable options.

6.4.3 Knowledge Acquisition Strategies.

Universities have 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 will 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” and online from various resources within and outside of GW, 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 multi-disciplinary understanding and application of cybersecurity principles.
- Utilizing the multi-disciplinary 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 on line and in the "live" 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.

6.4.4 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 will outline specific challenges and suggest strategies to overcome them.

Chapter 7: Institutional Implementation

Chapter 7 will provide advice for institutions seeking to implement recommendations from the CSEC2017 curricular volume. The following sections will be discussed:

- Local adaptation and variations between institutional types
- Technical resource requirements (onsite facilities, virtual laboratory environments)
- Faculty recruitment and retention strategies
- Obtaining institutional support
- Broadening participation
- Maintaining curricular currency
- Leveraging local and regional resources

[End of CSEC2017 v. 0.75]

Public Review and Comment period ends July 3, 2017
Provide feedback at: http://csec2017.org

Page intentionally left blank

Appendix A: Contributors

Sherly Abraham, Georgia Gwinnett College
Joshua Adams, Saint Leo University
Sara Akers, Terra State Community College
Wasim Al Hamdani, University of Dammam
Wasim Alhamdani, Imam Abdulrahman bin Faisal University
Thibaud Antignac, Chalmers University of Technology
Flo Appel, Saint Xavier University
Alvaro E. Arenas, IE Business School
lbert Ball, Hodges University
Masooda Bashir, UIUC
Shannon Beasley, Middle Georgia State University
Scott Bell[1], North West Missouri State University
Kimberly Bertschy, Northwest Arkansas Community College
Diana Bidulescu, HISD
David Biros[21], Oklahoma State
Chutima Boonthum-Denecke, Hampton University
Brandi Boucher Fabel, Ivy Tech Community College
Eric Braun[21], Rosemount, Inc - Emerson Process Management
Linda Brock, IBM
William (Bill) Caelli, QUT / GU
Roy Campbell, University of Illinois at Urbana-Champaign
Martin Carlisle, Carnegie Mellon University
Melissa Carlton, Florida State University
Lillian N. Cassel, Villanova University
John Chandy, University of Connecticut
Ankur Chattopadhyay, University of Wisconsin - Green Bay
Zhen Chen, Tsinghua University
Li-Chiou Chen, Pace University
Jessica Chisholm, Valencia College
KP Cho[22], Hong Kong University
Karla Clarke, KPMG LLP
Timothy Cullen, Private sector
Kevin Daimi, University of Detroit Mercy
Emily Darraj[1], Northrop Grumman
Ruth Davis, Santa Clara University
Bostjan Delak, ITAD
Ravi Dhungel, Intuit
Angel Diaz[21], Technical Services Corp
Stephen Dill[21], Lockheed Martin Information Sys
Bill Doherty, Truckee Meadows Community College
Lynette Drevin, North-West University
Laurie Dringus, Nova Southeastern University

[21] Industry Advisory Board Member
[22] Global Advisory Board Member

Ashutosh Dutta[21], AT&T
Barbara Endicott-Popovsky, University of Washington
Burkhard Englert, CSULB
Leslie D. Fife,
Dave Filer, New River Community College
Dianne Fodell[21], IBM - Cyber Security Innovation
Guillermo Francia III, Jacksonville State University
Robert Francis, Federal Reserve Bank of New York
Lothar Fritsch, Karlstad University
Steven Furnell, Plymouth University
Janos Fustos, MSU Denver
Lynn Futcher, Nelson Mandela Metropolitan University
Thoshitha Gamage, Southern Illinois University Edwardsville
Catherine Garcia van Hoogstraten, The Hague University of Applied Sciences
Jim Gast, ITT Tech
Dickie George, JHUAPL
Duane Gerstenberger, Marion Technical College
Joseph Giordano, Utica College
Bonnie Goins, Illinois Institute of Technology
Kartik Gopalan, Binghamton University
Mark Graff [21], Tellagraff, LLC
Andy Green, Kennesaw State University
Steve Hailey, CyberSecurity Academy
H. Hall, Athens Technical College
Robert Hambly, Department of Defense
K Harisaiprasad, Manhindra
Danis J. Heighton, Clark State Community College
Jim Helm, ASU
Morgan Henrie, MH Consulting Inc.
Jayantha Herath, St. Cloud State University
Erik Hjelmås, NTNU
Dwayne Hodges[21], International Information Systems Security Certification Consortium
Kenneth Hoganson,
Marko Hölbl, University of Maribor, Faculty of Electrical Engineering and Computer Science
Adrianna Holden-Gouveia, Northern Essex Community College
Susan Holland, University of Massachusetts Lowell
Micaela Hoskins, Cisco Systems
Grant Hudson, United States Postal Service
Angel L Hueca, Nova Southeastern University
Andrew Hurd, Excelsior College
John Impagliazzo, Hofstra University
Stephen Itoga, University of Hawaii at Manoa
Murray Jennex, San Diego State University
Sonja Johnson,
Audun Jøsang, The University of Oslo

Connie Justice, Indiana University Purdue University Indianapolis
Thomas Kaczmarek, Marquette University
Chris Kadlec, Georgia Southern University
Andrew Kalafut, Grand Valley State University
Alan Katerinsky, Hilbert College
Jonathan Katz, University of Maryland
Josh Kebbel-Wyen[21], Adobe
Walter Kerner, Fashion Institute of Technology
Rami Khasawneh, Lewis University
Valentin Kisimov, University National and World Economy Bulgaria
Stewart Kowalsky[22], Gjøvik University College
Donald Kraft, Colorado Technical University and U.S. Air Force Academy
Mark Kuhr[21], Synack
Ojoung Kwon, California State University at Fresno
Mischel Kwon[21], Mischel Kwon and Assocates LLC
David Lanter, Temple University
Stephen Larson, Slippery Rock University of PA
Margaret Leary, Northern Virginia Community College
Roy Levow, Florida Atlantic University
Peng Li, East Carolina University
Heather Lipford, University of North Carolina at Charlotte
Xun Luo, China Computer Federation
Phillip Mahan, Private sector
William Mahoney, University of Nebraska Omaha
Qutaibah Malluhi, Qatar University
David Manz[21], Pacific Northwest National Laboratory
Fabio Massacci, University of Trento
Cory A. Mazzola[21], Mandiant, a FireEye Company
Andrew McGettrick, University of Strathclyde
Mark-David McLaughlin[21], Cisco
Nancy Mead, Carnegie Mellon University
Mark Merkow, Charles Schwab and Co. Inc.
NG Mien Ta, Wizlearn Technologies Pte Ltd
Natalia Miloslavskaya[22], National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)
Dustin Mink, University of West Florida
Michael Moorman, Saint Leo University
Mike Murphy, retired
Igor Muttik[21], McAfee
Mark Mykytishyn[21], Tangible Security
Priyadarsi Nanda, University of Technology Sydney (Australia)
Stephen Olechnowicz, Institute for Defense Analysis
Robert Olson, Rochester Institute of Technology
Jacques Ophoff, University of Cape Town
Bernardo Palazzi, Brown University
Hyungbae Park, University of Central Missouri

Sameer Patil, Indiana University
Malcolm Pattinson, University of Adelaide
Kimberly Perez, Tidewater Community College
Mathew (Pete) Peterson,
Amelia Phillips, Highline College
Joe Pilla, Liberty Tax
Mathias R. Plass, Lewis University
Christine Pommerening, George Mason University
Damira Pon, University at Albany State University of New York
Michael Brian Pope, Independent Scholar
Randy Purse, Communications Security Establishment - Government of Canada
Portia Pusey[23]
Srini Ramaswamy[22]
Alan Rea, Western Michigan University
Thomas Reddington, New York University (NYU)
Randy Reid, UWF
Tiina Rodrigue[21], US Department of Education/George Washington University
Matt Rosenquist[21], Intel
Andrew Rozema, Grand Rapids Community College
Gerry Santoro, Penn State University
Angela Sasse[22], University College, London
Carter Schoenberg[21], Cybersecurity Services at CALIBRE
Hossain Shahriar, Kennesaw State University
Gordon Shenkle, Private sector
Daniel Shoemaker, University of Detroit Mercy
Neelu Sinha, Fairleigh Dickinson University
Jill Slay[22], UNSW Canberra
James N. Smith, Nova Southeastern University
S Srinivasan, Texas Southern University
Nelbert C. St.Clair, Middle Georgia State University
Gerhard Steinke, Seattle Pacific University
Mark Stockman, University of Cincinnati
S. M. Taiabul Haque, University of Central Missouri
April Tanner, Jackson State University
David Tobey, Indiana University South Bend
Samir Tout, Eastern Michigan University
Kim Tracy, Michigan Technological University
Rick Tracy[21], Telos Corporation
Ray Trygstad, Illinois Institute of Technology
Michael Tu, Purdue University Northwest
Zach Tudor[21], US Department of Energy Idaho National Laboratory
Douglas Twitchell, Boise State University
Johan van Niekerk[22], Nelson Mandela Metropolitan University
Randal Vaughn, Baylor University
Harald Vranken, Open University of the Netherlands

[23] Evaluator

Paul Wagner, University of Wisconsin - Eau Claire
James Walden, Northern Kentucky University
Charles Walker, US Federal Government
David Wang, DePaul University
Xinli Wang, Michigan Technological University
Matt Warre[22], Deakin University
Alan B. Watkins, National University
Deanne Wesley, Forsyth Technical Community College
Mike Westra[21], Ford
Doug White, Roger Williams University
Michael Whitman, Kennesaw State University
Brett Williams[22], IronNet
Patrea Wilson, University of Maryland University College
Steven Wong[22], Singapore Institute of Technology
Scott Woodison, University System of Georgia (Ret)
Carol Woody, Software Engineering Institute
Tom Worthington, Australian National University
Bill Wright[21], Symantec
Johnathan Yerby, Middle Georgia State University
Louise Yngstrom[22], Stockholm University
Xiaodong Yue, University of Central Missouri
Neal Ziring, NSA
Natalia, NRNU MEPhI
ZhangXuan, Shandong Police College

Page intentionally left blank