Draft "Cyber Sciences" Knowledge Areas
Cyber Education Project
Learning Outcomes Committee
David Gibson and Beth Hawthorne, Co-chairs
October 2015

This paper summarizes the work of the Learning Outcomes Committee of the Cyber Education Project (CEP). After providing background information explaining the process that led to this point, the documents presents a draft list of knowledge areas (KAs) intended to inform curricular guidance for an undergraduate degree in the Cyber Sciences. The draft knowledge areas are followed by a discussion of the key issues which need resolution to aid the development of useful guidelines for a cyber education curriculum. The attachments to this document provide a prior version of draft knowledge areas and the list of reference taxonomies for cyber education and cyber workforce development. A separate attachment includes the hundreds of Learning Outcomes culled and vetted by a subset of the Learning Outcomes Committee from various sources, including ACM/IEEE-CS curricular guidelines in computer science and information technology as well as the NSA CAE Knowledge Units.

Background

Organized in July 2014, the Cyber Education Project (www.cybereducationproject.org) is an initiative supported by a diverse group of computing professionals representing academic institutions and professional societies to develop undergraduate curriculum guidelines and a case for accreditation for educational programs in the "Cyber Sciences." The CEP adopted the term "Cyber Sciences" to describe 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. 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 goal of the Learning Outcomes Committee (LOC) of the CEP is to develop learning outcomes which characterize the knowledge, skills, and abilities that should be gained by students in an undergraduate degree program in one of the Cyber Sciences. The LOC began its work by collecting and reviewing published works relevant to cyber education curricula (see

https://www.surveymonkey.com/r/CEPLOWG). Many of these works included lists of proposed areas of study and subtopics within those areas which served as reference taxonomies for the Cyber Sciences. The LOC then held four workshops in 2015 to develop Cyber Sciences learning outcomes. During these workshops, the need became clear for high-level knowledge areas to organize and categorize the low-level learning outcomes. The knowledge areas described below were primarily drawn from a synthesis of the reference taxonomies listed in Attachment 2.

Draft Knowledge Areas

The following list is the current draft of knowledge areas for an undergraduate program in the Cyber Sciences. KAs 1-5 are primarily technical subject areas which may require pre-requisite coursework in computer programming, computer networks, operating systems, information storage and retrieval and foundational mathematics. KAs 6-9 are primarily non-technical subject areas typically not required by cyber-related programs such as computer science, computer engineering, and software engineering.

1. Cyber Defense
2. Cyber Operations
3. Digital Forensics
4. Cyber Physical Systems
5. Secure Software Engineering
6. Cyber Ethics
7. Cyber Policy, Governance, and Law
8. Cyber Risk Management
9. Behavioral Science

The following paragraphs briefly described the intended content of each knowledge area. Bear in mind that this is a work in progress and these descriptions represent and early draft proposal.

Cyber Defense. The Cyber Defense KA includes topics such as cryptography, data security, network security, and information assurance. While the technical skills required for defensive cyber operations and offensive cyber operations are very similar, the focus of topics in this KA is on the protection of, rather than the exploitation of, information and information systems.

Cyber Operations. The Cyber Operations KA includes topics such as cyber attack, penetration testing, cyber intelligence, reverse engineering, and cryptanalysis. While the term "cyber operations" may generally apply to both offensive and defensive operations, the intent here is to *exclude* topics primarily focused on the protection of information and information systems included in the Cyber Defense KA described above.

Digital Forensics. The Digital Forensics KA includes topics such as hardware and software forensics, incident response, cybercrime, and cyber law enforcement.

Cyber Physical Systems. The Cyber Physical Systems KA includes technology-focused topics such as Supervisory Control and Data Acquisition (SCADA) systems, the internet-of-things, and other emerging cyber technologies not addressed in the previous KAs.

Secure Software Engineering. The Secure Software Engineering KA includes topics such as secure systems design, secure coding and the deployability, maintainability, and usability of secure information systems.

Cyber Ethics. The Cyber Ethics KA includes topics such as ethical use of information systems, privacy and anonymity, intellectual property rights, professional responsibility, and global societal impacts of information systems.

Cyber Policy, Governance and Law. The Cyber Policy, Governance and Law KA includes topics such as government and institutional cyber policy and practices, regulatory authorities for cyber systems and operations, and cyber law.

Cyber Risk Management. The Cyber Risk Management KA includes topics such as cyber resilience, mission assurance, disaster recovery, business continuity, security evaluations, and cyber economics.

Behavioral Science. The Behavioral Science KA includes topics such as human behavior relating to cyber systems and operations, social engineering, social networks, human-computer interaction and organizational behavior.

Key Issues to be Resolved

Based on the experiences of the CEP Learning Outcomes Committee, it is clear that there is no perfect way to classify all constituent topics of the evolving interdisciplinary Cyber Sciences into distinct knowledge areas. Any proposed organization of KAs will include redundancies and will over-emphasize some areas while under-emphasizing other areas. Work toward resolving the following issues improve the organization, clarity, specificity, and utility of current list of Cyber Sciences knowledge areas.

Criteria for Selecting Knowledge Areas. It would be very useful to have agreed upon criteria for what constitutes a knowledge area. One model for KAs is to equate their content roughly to a single academic course. This model may be convenient for curriculum development and works well for some well-defined academic topics such as cryptography. A number of people proposed

a “Cyber Security Fundamentals” KA which corresponds to an introductory course in the discipline. However, this model does not work well for wide-ranging topics such as cyber defense with content that should be addressed in multiple courses in a Cyber Sciences program. Programs should have the flexibility to decide where knowledge area content best fits into their curriculum and the extent to which the content will be covered. While some programs might cover digital forensics in a few lessons in a cyber defense course, other programs might have multiple courses dedicated to the topic. The proposed list attempts to avoid KAs which are too broad to provide a useful classification and those which are too narrow or specific, leading to over-emphasis of their importance.

Definition of Terms. It would be very useful to have a glossary defining the terms used in the knowledge area descriptions. It became clear at CEP LOC meetings that different participants defined various terms differently including the term “cyber” itself. For example, some equate “cyber” with information technology in general while others equate the term more with offensive and defensive computer network operations. Adding to potential confusion, some terms such as “Cyber Physical Systems” are relatively new and evolving terms.

Balancing Technical and Non-technical Content. Perhaps the most challenging issue to resolve is the degree to which the KAs balance technical and non-technical topics. A heavy emphasis on technical content, typically taught by engineering and science departments, seems necessary to address many of the current cyber security challenges. However, Cyber Sciences are interdisciplinary, requiring an understanding of topics such as ethics, policy, law, management, and human behavior which typically are not taught by engineering and science departments. Furthermore, graduates of social science and humanities programs who take coursework in the Cyber Sciences are likely to bring valuable alternative perspectives to the cyber workforce. Members of the CEP largely view the Cyber Sciences as computing disciplines for the purposes of potential program accreditation. Nevertheless, it is not yet clear how broad an academic audience can be usefully served by curricular guidance in the form of Cyber Sciences knowledge outcomes.

Attachment 1 – Initial CEP Draft Knowledge Areas

The following list of Cyber Sciences KAs was developed through examination of the reference taxonomies included as Attachment 2 to this document. This list was developed by members of the CEP Learning Outcomes Working Group. It was revised to the current list of KAs based on feedback received at the at CEP Learning Outcomes Workshop held at the 2015 International Security Education Workshop in Atlanta on 19 May 2015. The list is included here to provide additional insight into development of the current draft KAs.

1. Cryptography
2. Cyber Attack
3. Cyber Defense
4. Cyber Ethics
5. Cyber Intelligence
6. Cyber Physical Systems
7. Cyber Policy, Governance, and Law
8. Cyber Risk Management
9. Digital Forensics
10. Human Computer Interaction
11. Network Security
12. Privacy
13. Reverse Engineering
14. Secure Software Engineering
15. Secure Systems Design

Attachment 2 – Reference Taxonomies

Cyber Sciences Reference Taxonomies

Cyber Education Project
Learning Outcomes Working Group
May 2015

This document contains a list and descriptions of works which provide taxonomies of knowledge areas and workforce competencies relating to the Cyber Sciences. These taxonomies will be used to inform a taxonomy for organizing Cyber Sciences learning outcomes. The list currently includes 10 primary reference taxonomies. The first 6 are academically-focused knowledge area taxonomies. The last 4 are workforce-focused competency taxonomies. To be included on this list, the work should include Cyber Sciences related knowledge or competency areas and sub-areas. That is, the reference taxonomy should include at least a 2-level hierarchy of topic areas. A list of topic areas without further subdivision of the content of those topic areas does not provide sufficient insight for informing a taxonomy for the Cyber Sciences.

Reference Taxonomy List

1. **CS2013** - ACM/IEEE Information Assurance and Security Knowledge Area
2. **IT2008 -** ACM/IEEE IT2008 Information Assurance and Security Knowledge Area[1]
3. **ITiCSE** - Information Assurance Curricular Guidelines Working Group Report
4. **NICE CWF** – NICE Cybersecurity Workforce Framework
5. **DOL CCM** - U.S. Department of Labor Cybersecurity Competency Model
6. **DOE EBOK** - U.S. Department of Energy Essential Body of Knowledge
7. **CAE CO** - NSA Center of Academic Excellence in Cyber Operations
8. **CAE IA/CD** - NSA/DHS National Centers of Academic Excellence in Info Assurance/Cyber Defense
9. **State Gov** - State Government Information Security Competencies
10. **Academies** - Military Academy Cyber Education Working Group Draft Body of Knowledge

Reference Taxonomy Descriptions

CS2013 - Computer Science Curriculum 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science (2013)

Information Assurance and Security (IAS) is a new Knowledge Area (KA) in the ACM/IEEE CS2013, not present in CS2008. CS2013 recommends 3 Core-Tier1 (required) hours of IAS

[1] The first draft of an update to IT2008 is expected by November 2015 for public review and comment, and will included cyber-related concepts and learning outcomes. This volume is on schedule to be completed by 2017.

content and 6 Core-Tier 2 (minimum 80% coverage) hours of IAS-specific topics. In addition to the IAS-specific topics, CS2013 recommends and addition 32 Core-Tier1 hours and 21.5 Core-Tier2 hours of content distributed throughout 13 of the 17 other KAs for which IAS topics are either fundamental to or a supportive use case for the topic. (Only the Algorithms and Complexity, Computational Science, and Graphics and Visualization KAs do not include hours for which IAS topics are fundamental or supporting). CS2013 includes the following 11 IAS-specific topic areas.

1. Foundational Concepts in Security (1 Tier 1 hour)
2. Principles of Secure Design (1 Tier 1 and 1 Tier 2 hours)
3. Defensive Programming (1 Tier 1 and 1 Tier 2 hours)
4. Threats and Attacks (1 Tier 2 hour)
5. Network Security (2 Tier 2 hours)
6. Cryptography (1 Tier 2 hour)
7. Web Security (elective)
8. Platform Security (elective)
9. Security and Policy Governance (elective)
10. Digital Forensics (elective)
11. Secure Software Engineering (elective)

As an example of how to interpret the above list, CS2013 recommends that all Computer Science programs include at least one hour of Defensive Programming (DP), one third of a typical course, and that most Computer Science programs include two hours of DP. CS2013 also includes more specific topic lists and learning outcomes for each of the above topic areas.

IT2008 - ACM and IEEE Information Technology 2008: Curriculum Guidelines for Undergraduate Degree Programs in Information Technology (2008)

Information Assurance and Security (IAS) is one of 13 knowledge areas in the IT2008 body of knowledge which recommends 23 core IAS hours out of a total for 314 core hours. The IAS knowledge area consists of the following 11 core topics.

1. Fundamental Aspects
2. Security Mechanisms (Countermeasures)
3. Operational Issues
4. Policy
5. Attacks
6. Security Domains
7. Forensics
8. Information States

9. Security Services
10. Threat Analysis Model
11. Vulnerabilities

ITiCSE - Towards Information Assurance (IA) Curricula Guidelines Working Group Report (2010)

This working group report proposes the following 11 areas for an information assurance body of knowledge based on a survey of existing IA programs. The report provides lists of subjects for each of the 11 areas and 25 learning outcomes covering areas.

1. Fundamental Concepts
2. Cryptography
3. Security Ethics
4. Security Policy
5. Digital Forensics
6. Access Control
7. Security Architecture and Systems
8. Network Security
9. Risk Management
10. Attack/Defense
11. Secure Software Design and Engineering

NICE CWF - National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework (Version 2.0)

The National Initiative for Cybersecurity Education (NICE) developed the National Cybersecurity Workforce Framework (the Workforce Framework) to define the cybersecurity workforce and provide a common taxonomy and lexicon by which to classify and categorize workers. The Workforce Framework lists and defines 32 specialty areas (sub-bullets below) of cybersecurity work and provides a description of each. Each of the types of work is placed into one of seven overall categories (major bullets below). The Workforce Framework also identifies common tasks and knowledge, skills, and abilities (KSA's) associated with each specialty area. The Workforce Framework will be used as guidance to the federal government, will be made available to the private, public, and academic sectors for describing cybersecurity work and workforces, and related education, training, and professional development. The Workforce Framework is the output of a collaboration of more than 20 Federal departments and agencies and numerous national organizations from within academia and general industry.

1. Securely Provision

2. Operate and Maintain
3. Protect and Defend
4. Investigate
5. Oversee and Govern
6. Collect and Operate
7. Analyze

DOL CCM - U. S. Department of Labor Cybersecurity Competency Model

The Employment and Training Administration (ETA) has worked with the Department of Homeland Security and the more than 20 federal departments and agencies that make up the National Initiative for Cybersecurity Education (NICE) to develop a comprehensive competency model for cybersecurity. Technical and subject matter experts from education, business, and industry also contributed to the model's development. The DOL Cybersecurity Industry Model defines the latest skill and knowledge requirements needed by individuals whose activities impact the security of their organization's cyberspace. The model incorporates competencies identified in the NICE National Cybersecurity Workforce Framework and complements the Framework by including both the competencies needed by the average worker who uses the Internet or the organization's computer network, as well as cybersecurity professionals. The ETA model will be updated to reflect future changes to the Framework.

Tier 5 is identical to the NICE Framework (pre v2). Tier 4 is most relevant as a unique reference taxonomy. Within Tier 4, the five competencies each include Critical Work Functions and Technical Content Areas. The Critical Work Functions include KSAs worded like learning outcomes. The Technical Content Areas each include a useful third level of topic decomposition. Tier 2, Academic Competencies, are mostly not cyber-specific with the exception of the Fundamental IT User Skills area.

1. Tier 1 – Personal Effectiveness Competencies (the foundation)
    a. Interpersonal Skills
    b. Integrity
    c. Professionalism
    d. Initiative
    e. Adaptability and Flexibility
    f. Dependability and Reliability
    g. Lifelong Learning
2. Tier 2 – Academic Competencies
    a. Reading
    b. Writing
    c. Mathematics

   d. Science
   e. Communication
   f. Critical and Analytical Thinking
   g. Fundamental IT User Skills
3. Tier 3 – Workplace Competencies
   a. Teamwork
   b. Planning and Organizing
   c. Creative Thinking
   d. Problem Solving and Decision Making
   e. Working with Tools and Technology
   f. Business Fundamentals
4. **Industry-Wide Technical Competencies**
   a. Cybersecurity Technology
   b. Information Assurance
   c. Risk Management
   d. Incident Detection
   e. Incident Response and Remediation
5. Tier 5 – Industry-Sector Functional Areas (NICE Framework)
   a. Security Provision System
   b. Operate and Maintain IT Security
   c. Protect and Defend From Threats
   d. Investigate Threats
   e. Collect Information and Operate Cybersecurity Process
   f. Analyze Information
   g. Oversee and Govern Cybersecurity Work
6. Management Competencies and Occupation-Specific Requirements sit above Tier-5

DOE EBOK - U.S. Department of Energy Essential Body of Knowledge – A Competency and Functional Framework for Cyber Security Workforce Development (2013)

The Office of the Chief Information Officer (OCIO) utilized DOE cyber security policy, industry best practices and lessons learned, and comprehensive internal needs assessments to identify fundamental cyber security functional roles and associated responsibilities. In addition, core competencies were identified that represent the 'core' skill set needed by cyber security professionals to adequately fulfill their functional roles. This collective information was further used to define the Enterprise Essential Body of Knowledge (EBK). Components of the EBK are assigned to each functional role, and customized curriculum is determined for each key role. The OCIO has determined the following roles to be key functional cyber roles within the Department: Chief Information Officer (CIO), Information Owner/Steward, Chief Information Security Officer (CISO), Authorizing Official (AO), AO Designated Representative (AODR), Common

Control Provider, Information System Owner, Cyber Security Program Manager (CSPM), Information System Security Officer (ISSO), Information Security Architect, Information System Security Engineer, and the Security Control Assessor. The DHS National Cyber Security Division (NCSD) Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development was used as the foundational document for the DOE-specific EBK. Additionally, the DOE EBK incorporates other established bodies of knowledge and managerial, technical, assurance, and operational concepts and requirements from DOE Directives and OCIO reference baselines.

For each of the following 13 competency areas, work functions are categorized for Manage, Design, Implement, and Evaluate. Appendix 1 of the document provides extensive lists of key terms and concepts for each competency area. These lists provide additional granularity to each of the competencies but do not quite form a second level in the taxonomy.

1. Data Security
2. Continuity of Operations
3. Incident Management
4. Cyber Security Training and Awareness
5. IT Systems Operations and Maintenance
6. Network and Telecommunications Security
7. Personal Security
8. Physical and Environmental Security
9. Procurement
10. Regulatory and Standards Compliance
11. Risk Management
12. Strategic Security Management
13. System and Application Security

CAE CO - NSA Center of Academic Excellence in Cyber Operations

The CAE-Cyber Operations program is intended to be a deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science (CS), computer engineering (CE), and/or electrical engineering (EE) disciplines, with extensive opportunities for hands-on applications via labs/exercises. The CAE-Cyber Operations program complements the existing Centers for Academic Excellence (CAE) in Information Assurance Education (CAE-IAE) and Research (CAE-R) programs, providing a particular emphasis on technologies and techniques related to specialized cyber operations (e.g., collection, exploitation, and response), to enhance the national security posture of our Nation. These technologies and techniques are critical to intelligence, military and law enforcement organizations authorized to perform these specialized operations.

Mandatory Program Content (10 of 10 knowledge units required)

1. Low Level Programming Languages
    a) C
    b) Assembly Language (for x86, ARM, MIPS or PowerPC)
2. Software Reverse Engineering
    a) Reverse engineering techniques
    b) Reverse engineering for software specification recovery
    c) Reverse engineering for malware analysis
    d) Reverse engineering communications
    e) Deobfuscation of obfuscated code
    f) Common tools for software reverse engineering
3. Operating System Theory
    a) Privileged vs. non-privileged states; and transitions between them (domain switching)
    b) Concurrency and synchronization
    c) Processes and threads, process/thread management, synchronization, inter-process communications
    d) Memory management, virtual memory, hierarchical memory schemes
    e) Uni-processor and multi-processor interface and support
    f) CPU Scheduling
    g) File Systems
    h) IO issues
    i) Distributed OS issues
4. Networking
    a) Routing, network and application protocols
    b) Network architectures
    c) Network security
    d) Wireless network technologies
    e) Network traffic analysis
    f) Protocol analysis
    g) Network mapping techniques
5. Cellular and Mobile Technologies
    a) Overview of smart phone technologies
    b) Overview of embedded operating systems
    c) Wireless technologies
    d) Infrastructure components
    e) Mobile protocols
    f) Mobile logical channel descriptions
    g) Mobile registration procedures
    h) Mobile encryptions standards
    i) Mobile identifiers
    j) Mobile and Location-based Services

6. Discrete Math
    a) Searching and sorting algorithms
    b) Complexity theory
    c) Regular expressions
    d) Computability
    e) Mathematical foundations for cryptography
    f) Entropy
7. Overview of Cyber Defense
    a) Identification of reconnaissance operations
    b) Anomaly/intrusion detection
    c) Anomaly identification
    d) Identification of command and control operations
    e) Identification of data exfiltration activities
    f) Identifying malicious code based on signatures, behavior and artifacts
    g) Network security techniques and components
    h) Cryptography and its uses in cybersecurity
    i) Malicious activity detection
    j) System security architectures and concepts
    k) Defense in depth
    l) Trust relationships
    m) Distributed/Cloud
    n) Virtualization
8. Security Fundamental Principles (“First Principles”)
    a) General Fundamental Design Principles
    b) Security Design Principles
    c) Methods for Reducing Complexity
9. Vulnerabilities
    a) Vulnerability taxonomies
    b) Buffer overflows
    c) Privilege escalation attacks
    d) Input validation issues
    e) Password weaknesses
    f) Trust relationships
    g) Race conditions
    h) Numeric over/underflows
    i) User-space vs. kernel-space vulnerabilities
    j) Local vs. remote access
10. Legal
    a) International Law
    b) U.S. Laws

Optional Program Content (10 of 18 knowledge units required)

1. Programmable Logic Languages
    a) Hardware Design Languages
    b) Hardware Programming Languages
2. FPGA Design
    a) Synthesize, simulate and implement a programmable logic program on a programmable logic device
3. Wireless Security
    a) Describe the unique security and operational attributes in the wireless environment and their effects on network communications
    b) Identify the unique security implications of these effects and how to mitigate security issues associated with them
4. Virtualization
    a) Virtualization techniques
    b) Type 1 and Type 2 virtual machine architectures
    c) Uses of virtualization for security, efficiency, simplicity and resource savings
5. Large Scale Distributed Systems
    a) Cloud Computing/Cloud Security
6. Risk Management of Information Systems
    a) Models
    b) Processes
7. Computer Architecture
    a) Define devices of electronic digital circuits
    b) Describe how these components are interconnected
    c) Integrate individual components into a more complex digital system
    d) Understand the data path through a CPU
8. Microcontroller Design
    a) Integrate discrete components into a single processor element
    b) Describe ways of achieving performance efficiencies through combining components
    c) Identify trade-offs associated with microcontroller optimization
9. Software Security Analysis
    a) Source code analysis
    b) Binary code analysis
    c) Static code analysis techniques
    d) Dynamic code analysis techniques
    e) Testing methodologies
10. Secure Software Development
    a) Secure programming principles and practices
    b) Constructive techniques

11. Embedded Systems
    a) Define requirements which lead to the design and fabrication of an embedded system
    b) Program the microcontrollers to achieve an application-specific design
    c) Identify the security concerns associated with resource constrained devices
12. Forensics and Incident Response or Media Exploitation
    a) Operating system forensics
    b) Media forensics
    c) Network forensics
    d) Component forensics
13. Systems Programming
    a) Kernel internals
    b) Device drivers
    c) Multi-threading
    d) Use of alternate processors
14. Applied Cryptography
    a) Identify the appropriate uses of symmetric and asymmetric encryption
    b) Assign some measure of strength to cryptographic algorithms and the associated keys
    c) Identify what level of algorithm strength is needed for particular applications and the implementation factors related to its suitability for use
    d) Understand the common pitfalls associated with the implementation of cryptography, and will the challenges and limitations of various key management systems
15. SCADA Systems
    a) Describe how embedded systems are employed in industrial infrastructures and control systems
    b) Identify means for capturing instrument telemetry and identifying feedback controls
    c) Describe methods for managing distributed nodes
    d) Identify potential security vulnerabilities associated with the use of such systems, and means for mitigating these vulnerabilities
16. HCI/Usable Security
    a) Understand user interface issues that will affect the implementation of, and perception of security mechanisms and the behavioral impacts of various security policies
    b) Understand the tension between user security and convenience
17. Offensive Cyber Operations
    a) Understand the phases of a cyber operation, what each phase entails, who has authorities to conduct each phase and how operations are assessed after completion
18. Hardware Reverse Engineering
    a) Understand basic fundamental procedures such as probing, measuring and data collection to identify functionality and to affect modifications to the hardware functionality

CAE IA/CD - NSA/DHS National Centers of Academic Excellence in Information Assurance/Cyber Defense

The intent of the modifications to the academic requirements of the CAE IA programs was to update them to better reflect the state to which the discipline of IA has evolved since the original publication of the training standards. The framework of Knowledge Units (KUs) and Focus Areas (FAs) was chosen to make the requirements easier to update in the future and to allow differentiation amongst the schools by recognizing the specific areas in which they focus their research and/or educational offerings (e.g., Digital Forensics, Systems Security Engineering, Secure Software Development).

CORE Knowledge Units (4-year programs)

1. Basic Data Analysis
2. Basic Scripting or Introductory Programming (4 yr core)
3. Cyber Defense
4. Cyber Threats
5. Fundamental Security Design Principles
6. IA Fundamentals
7. Intro to Cryptography
8. IT Systems Components
9. Networking Concepts
10. Policy, Legal, Ethics, and Compliance
11. System Administration
12. Databases
13. Network Defense
14. Networking Technology and Protocols
15. Operating Systems Concepts
16. Probability and Statistics
17. Programming

Optional Knowledge Units

1. Advanced Cryptography
2. Advanced Network Technology and Protocols
3. Algorithms
4. Analog Telecommunications
5. Cloud Computing
6. Cybersecurity Planning and Management
7. Data Administration

8. Data Structures
9. Database Management Systems
10. Digital Communications
11. Digital Forensics (device, host, media, network)
12. Embedded Systems
13. Forensic Accounting
14. Formal Methods
15. Fraud Prevention and Management
16. Hardware Reverse Engineering
17. Hardware/Firmware Security
18. IA Architectures
19. IA Compliance
20. IA Standards
21. Independent/Directed Study/Research
22. Industrial Control Systems
23. Intro to Theory of Computation
24. Intrusion Detection
25. Life-Cycle Security
26. Low Level Programming
27. Mobile Technologies
28. Network Security Administration
29. Operating Systems Hardening
30. Operating Systems Theory
31. Overview of Cyber Operations
32. Penetration Testing
33. QA / Functional Testing
34. RF Principles
35. Secure Programming Practices
36. Security Program Management
37. Security Risk Analysis
38. Software Assurance
39. Software Reverse Engineering
40. Software Security Analysis
41. Supply Chain Security
42. Systems Programming
43. Systems Certification and Accreditation
44. Systems Security Engineering
45. Virtualization Technologies
46. Vulnerability Analysis
47. Wireless Sensor Networks

State Gov - STATE GOVERNMENT INFORMATION SECURITY COMPETENCIES

The State Government Information Security Workforce Development Model, a competency-based and functional information security workforce development framework was initiated at the grassroots level by a State Government Information Security Workforce Development Advisory Council, comprised of six (6) pilot states (California, Florida, Michigan, Minnesota, New York and Texas) and the Information Technology Center of Excellence, a non-profit organization supporting technology best practice and education. The information security competencies defined below comprise The State Government Information Security Model competency areas.

1. Data (Information) Security
2. Digital Forensics
3. Enterprise Architecture
4. Enterprise Continuity (Disaster Recovery)
5. Incident Management
6. IT Systems Operations and Maintenance
7. Network and Telecommunications Security
8. Physical and Personnel Security
9. Privacy
10. Policies, Standards and Compliance (Information Assurance)
11. Procurement
12. Security Risk Management
13. Strategic Security Management
14. Systems and Application Security

Academies - Military Academy Cyber Education Working Group Draft Body of Knowledge (v IB 2 March 2015)

This work comes from a cyber operations perspective with the target audience of military service academies. It divides the discipline into the 9 knowledge areas listed below. For each knowledge area, learning outcomes are provided for three groups: **all** students at the institution, **some** students who are interested in the material but no pursuing a cyber degree, and the **few** who do major in the discipline and earn a cyber degree.

1. Cyberspace Domain
2. Cyberspace Risk Management
3. Cyberspace Operations, Planning, and Management
4. Cyber Attack
5. Cyber Defense

6. Authorities, Policies, and Law
7. Human Factors
8. Personal Responsibility and Ethics
9. Technology

There are many other curricular and workforce guidelines which focus on a single discipline which may be part of a broader cyber education curriculum. These guidelines may be useful in further refining elements of the top-level of a cyber education taxonomy. Several examples of these are listed below.

- Cyber Crime
  - CYBERBOK, CYBERPOL Cyber Crime Security Essential Body of Knowledge
- Software Assurance
  - Software Assurance Curriculum Project Volume I: Master of Software Assurance Reference Curriculum (CMU SEI)
- Industrial Control Systems/Supervisory Control and Data Automation
  - Certification of Cyber Security Skills of ICS/SCADA Professionals (EU ENISA)
- Digital Forensics
  - Computer Network Defense-Forensics Analyst Curriculum (US DoD)