


June 2019

Adopting the Cybersecurity Curriculum Guidelines to Develop a Secondary and Primary Academic Discipline in Cybersecurity Postsecondary Education

wasim a. alhamdani

University of the Cumberlands, wasim.alhamdani@ucumberlands.edu

Follow this and additional works at: <https://digitalcommons.kennesaw.edu/jcerp>

 Part of the [Information Security Commons](#), [Management Information Systems Commons](#), and the [Technology and Innovation Commons](#)

Recommended Citation

alhamdani, wasim a. (2019) "Adopting the Cybersecurity Curriculum Guidelines to Develop a Secondary and Primary Academic Discipline in Cybersecurity Postsecondary Education," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2019 : No. 1 , Article 2.

Available at: <https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/2>

This Article is brought to you for free and open access by DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Journal of Cybersecurity Education, Research and Practice by an authorized editor of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Adopting the Cybersecurity Curriculum Guidelines to Develop a Secondary and Primary Academic Discipline in Cybersecurity Postsecondary Education

Abstract

A suggested curriculum for secondary and primarily academic discipline in Cybersecurity Postsecondary Education is presented. This curriculum is developed based on the Association for Computing Machinery guidelines and the National Centers of Academic Excellence Cyber Operations program.

Keywords

Cybersecurity Curriculum, Postsecondary Education

Cover Page Footnote

A suggested curriculum for secondary and primarily academic discipline in Cybersecurity Postsecondary Education is presented. This curriculum is developed based on the Association for Computing Machinery guidelines and the National Centers of Academic Excellence Cyber Operations program.

Kennesaw State University

DigitalCommons@Kennesaw State University

KSU Proceedings on Cybersecurity Education,
Research and Practice

Adopting the Cybersecurity Curriculum Guidelines to Develop a Secondary and Primary Academic Discipline in Cybersecurity Postsecondary Education

Wasim AlHamdani

Follow this and additional works at <https://digitalcommons.kennesaw.edu/ccerp>



Part of the [Information Security Commons](#)

Abstract

A suggested curriculum for secondary and primarily academic discipline in Cybersecurity Postsecondary Education is presented. This curriculum is developed based on the Association for Computing Machinery guidelines and the National Centers of Academic Excellence Cyber Operations program.

Disciplines

Information Security

AlHamdani: Adopting the Cybersecurity Curriculum
Guidelines to Develop a Secondary and Primarily Academic Discipline in Cybersecurity
Postsecondary Education

Introduction

In August 2015, the Association for Computing Machinery (ACM) (ACM, 2017) education board recognized there is a need to develop a framework and base structure for cybersecurity disciplines, whether by developing full new programs, enhancing existing programs, or developing new concentrations within present programs. This recognition resulted in generating a taskforce on cybersecurity education (CSEC2017) with other professional and scientific computing societies to create comprehensive curricular guidance in cybersecurity education. The other professionals include:

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

The outcome of this work came in a report titled “Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity” (ACM, 2017). This report is based on the philosophy, “Our philosophy, shaped in part by the U.S. National Research Council Next Generation Science Standards, views cybersecurity as a body of knowledge grounded in enduring principles that are continuously extended, refined, and revised through evidence-based practice.”

The Model

The model shown has three aspects:

- Knowledge;
- Crosscutting concepts; and
- Discipline.

The first dimension covers: data, software, components, connection, system, human, organization and societal. The knowledge areas are organized flexibly to allow for the expansion and contraction of content as needed. However, the knowledge areas characterize the full frame of knowledge in the field of cybersecurity. The second domain covers confidentiality, integrity, availability, risk, adversarial thinking, and system thinking. However, the third domain covers computer science, information systems, information technology, computer engineering, software engineering, and other disciplines. Table 1 shows the three components of the ACM model

Submission to KSU Proceedings on Cybersecurity Education, Research and Practice

Discipline	Knowledge	Crosscutting concepts
Computer science Information system Information technology Computer engineering Software engineering Other disciplines	Data, software, components, connection, system, human, organization and societal	Confidentiality, integrity, availability, risk, adversarial thinking and system thinking

Table 1: ACM Model Components

The ACM's proposal of a secondary academic discipline in cybersecurity postsecondary education (i.e., a minor in cybersecurity) based on two factors :

- The student has enough knowledge to start Cybersecurity as a secondary academic discipline; and
- The student does not have enough experience to launch Cybersecurity as a secondary academic discipline.

For the first category, computer science students or computer engineering students would have enough mathematical, communication, software, and system knowledge to start the secondary subject. However, the second category means the students would not have enough experience to start the secondary discipline.

The report is very detailed and expresses the body of knowledge and its particular frame of information required to satisfy cybersecurity as a secondary academic discipline or even a major academic discipline. However, the report left the door open for any prerequisite to support the subject or to prepare the student to do the cybersecurity track.

This work identifies the prerequisite required knowledge to start the academic discipline for the five categories of control mentioned in the report (computer science, information systems, information technology, computer engineering, and software engineering) and the others. The prerequisites are the required knowledge that the learner needs to have before going into the cybersecurity track, which will act as a control for the flow of experience to the learners.

The work identifies that many current textbooks in the academic market are not sufficient to build the academic discipline and the need for new books that cover such a curriculum.

ACM body of knowledge components

The collection of knowledge components presented in the ACM report covers the following domains:

AlHamdani: Adopting the Cybersecurity Curriculum
Guidelines to Develop a Secondary and Primarily Academic Discipline in Cybersecurity
Postsecondary Education

- **Data Security** which includes cryptography concepts, digital forensics, end-to-end secure communications, data integrity and authentication, and information storage security.
- **Software Security** which covers the components of fundamental design principles, including least privilege, open design, and abstraction; security requirements and their role in the design; implementation issues; static and dynamic testing; configuring and patching ethics in development; testing; and vulnerability disclosure.
- **Component Security** which covers the components of vulnerabilities of system components, component lifecycle, secure component design principles, supply chain management security, security testing, and reverse engineering.
- **Connection Security** which covers the elements of systems, architecture, models, and standards; physical component interfaces; software component interfaces; connection attacks; and transmission attacks.
- **System Security** which covers the components of a holistic approach, security policy, authentication, access control, monitoring, recovery, testing, and documentation.
- **Human Security** which covers the components of identity management, social engineering, awareness and understanding, social behavioral privacy and security, personal data privacy, and security.
- **Organizational Security** which includes risk management, governance and policy, laws, ethics, compliance, strategy, and planning.
- **Societal Security** which covers the components of cybercrime, cyberlaw, cyber ethics, cyber policy, and privacy.

These domains are the center of cybersecurity education. The angle of these domains is entirely different from the National Centers of Academic Excellence in Cyber Defense or Cyber Operations (nsa.gov, 2018). However, looking deeper into the details and cross-references between the two curricula, there are many common topics. In another work, the underlying philosophy is different for ACM report philosophy, as it “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 Standards¹¹, views cybersecurity as a body of knowledge grounded in enduring principles that are continuously extended, refined, and revised through evidence-based practice ” (ACM, 2017 Page 19). However, the education goals of the National Centers of Academic Excellence (CAE) are: “The CAE in Cyber Defense program aims to reduce vulnerabilities in our national information

Submission to KSU Proceedings on Cybersecurity Education, Research and Practice

infrastructure, while the CAE in Cyber Operations program, sponsored by NSA, focuses on technologies and techniques related to specialized cyber operations to enhance the national security posture of the Nation.” (niccs.us-cert.gov, 2018). A crosswalk to map the CAE to cybersecurity curriculum is beyond this work because this work focuses on mapping the latest curriculum developed by ACM and published in 2017.

A possible prerequisite for the body of knowledge

The report went into detail to express the frame of knowledge and the information required to satisfy cybersecurity as a major academic discipline or secondary academic discipline. However, the report went open end for any prerequisite to assistance the discipline or to train the students to do the cybersecurity track. The report mentioned some of the required knowledge in very short notes, such as in data security, and the report suggested the mathematical background needed to cover number theory. The prerequisite body of knowledge required to start the cybersecurity track is categorized as the Knowledge Area, as expressed in Table 2 (the table is a suggestion for a possible prerequisite body of knowledge required).

Knowledge Area	Prerequisite
Data Security: cryptography concepts, digital forensics, end-to-end secure communications, data integrity and authentication, information storage security	Discrete Mathematics with a focus on Number Theory, Principles Networking, and Network Protocols
Software Security: fundamental design principles including least privilege, open design, and abstraction, security requirements and their role in the design, implementation issues, static and dynamic testing, Configuring and patching, ethics in development, testing and vulnerability disclosure	Programming languages, software analysis, and design, principles of software engineering,
Component Security: vulnerabilities of system components, component lifecycle, secure component design principles, supply chain management	Software testing principles, the principle of data management, principles of supply chain management, the principle of warehousing

AlHamdani: Adopting the Cybersecurity Curriculum
Guidelines to Develop a Secondary and Primarily Academic Discipline in Cybersecurity
Postsecondary Education

security, security testing, reverse engineering	
Connection Security: systems, architecture, models, and standards, physical component interfaces, software component interfaces, connection attacks, transmission attacks.	Computer architecture, hardware design, hardware software interface, the principle of system software, operating system design, Database principles, and design
System Security: Holistic approach, Security policy, Authentication, Access control, Monitoring, Recovery, Testing, Documentation.	
Organizational Security: risk management, governance and policy, laws, ethics, and compliance, strategy, and planning	Principles of organization management
Human Security: Identity management, social engineering, awareness and understanding, social behavioral privacy and security, personal data privacy and security	
Societal Security: cybercrime, cyberlaw, cyber ethics, cyber policy, privacy	

Table 2: A possible prerequisite for knowledge areas

The possible prerequisite courses are:

Number theory (3 hours/lecture/Semester)
Divisibility, Prime numbers, Greatest common divisor, Euclidean algorithm, Unique factorization, Congruence, Modular arithmetic, Euler's phi function, Fermat's, Euler's and Wilson's, theorems, Chinese remainder theorem Quadratic Reciprocity, Quadratic residues, Legendre and Jacobi symbols Law of quadratic

Submission to KSU Proceedings on Cybersecurity Education, Research and Practice

reciprocity, Additional Topics, Pythagoras, Fermat, Lagrange's Theorem, Primality testing

Statistics for data Science (3 hours/lecture/Semester)

Probability; distributions, expectation, variance, covariance, portfolios, statistical inference of univariate data; Statistical inference for bivariate data inference for intrinsically linear simple regression models; Residual analysis; Data transformations; simple regression model (SRM); inference and prediction in SRM; regression diagnostics; trends in time series; and models for time series

Programing language (2 hours/lecture/2 labs/Semester)

Programming Languages Overview, Control Flow, Subprograms, Program Structure, Object-Oriented Programming (name binding, scope, control flow, data types, type systems, object orientation, scripting languages, functional languages, and possibly runtime systems, polymorphism, and concurrency)

Computer architecture and design (3 hours/lecture/Semester)

Fundamentals of Computer Design, Instruction-Level Parallelism and Its Exploitation, Multiprocessors and Thread-Level Parallelism, Memory Hierarchy Design, Storage Systems, Pipelining: Basic and Intermediate Concepts

Networking and network protocols (3 hours/lecture/Semester)

Layered network architectures and the TCP/IP model; Link layer error and flow control mechanisms; Packet switching; Wired and wireless local and wide area networks; Medium access control procedures; Internetworking with switches, bridges, and routers; Routing algorithms; Network security

System software and the principle of operating system design (3 hours/lecture/Semester)

System software types, compiler design, interrupt service, process states and transitions, spooling, management of memory and disk space, virtual storage, processes and threads, scheduling processes, devices, file systems(local file systems, network file systems, distributed file systems), protection, the synchronization and communication of cooperating processes, UNIX system software, debug concurrent programs, debug complex systems and low-level software

System analysis design and testing (3 hours/lecture/Semester)

AlHamdani: Adopting the Cybersecurity Curriculum
 Guidelines to Develop a Secondary and Primarily Academic Discipline in Cybersecurity
 Postsecondary Education

Introduction to systems analysis and design, analyzing the business case, managing systems, requirements, data and process, object, development, user interface design, data design, system architecture, managing systems, implementation, systems support and security, structural testing, functional technique categories, verification, validation, static testing, dynamic testing, test administration, test planning, test process, budgeting, scheduling

The principle of management, operation, and supply of chain (3 hours/lecture/Semester)

The functions of management, organizational theories, operations management, HR management, marketing management, managing information, managing financial resources, ethics, survey of supply chain management including defining the scope of service, procurement and purchasing, and material management, return on investment, value chain principles, contracts and legal issues, and operations management

There are some flows of knowledge (Al-Hamdani, 2006) that also need to be accounted for when implanting this course, as shown in Fig. 1.

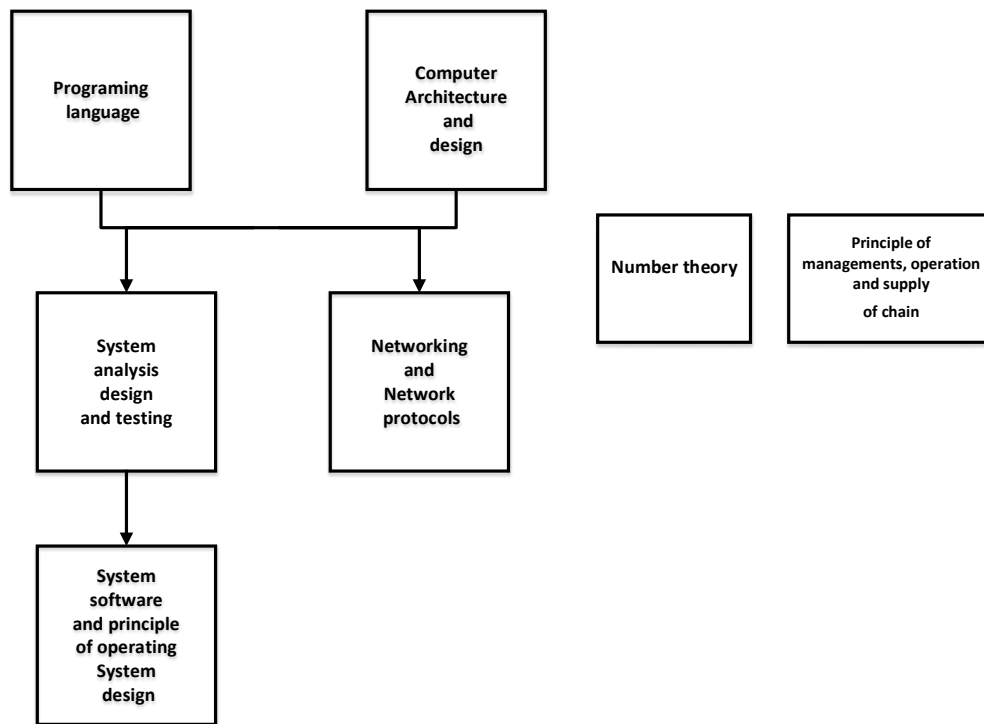


Figure 1. Knowledge Flow for Prerequisite Courses

Submission to KSU Proceedings on Cybersecurity Education, Research and Practice

The Second Academic Discipline in Cybersecurity

The cybersecurity track body, if built on eight domains, includes some of the following challenges. In this curriculum, some of the areas have no textbook currently on the market that can cover the required contents or its collection of topics is not strictly related, such as the data security curriculum, which includes:

- Cryptography concepts;
- Digital forensics;
- End-to-end secure communications;
- Data integrity and authentication; and
- Information storage security.

Looking at these topics, there are four domains covered:

- Cryptography;
- Network security;
- Data and storage security; and
- Digital forensics.

There currently are no textbooks that could cover these topics.

Another example is Component Security:

- Vulnerabilities of system components;
- Component lifecycle;
- Secure part;
- Design principles;
- Supply chain management security;
- Security testing; and
- Reverse engineering.

The best solution to this problem is to create a cross-reference between the suggested curriculum topics and the ACM curriculum. Suggested courses are:

Cryptography Algorithms (3 hours/lecture/Semester)

Prerequisite: number theory and programming language

Classical encryption, block cipher AES, public key, digital signature, hashing, and cryptography key management, cryptography standards cryptography legal issues

Data Science for Security (3 hours/lecture/Semester)

AlHamdani: Adopting the Cybersecurity Curriculum
Guidelines to Develop a Secondary and Primarily Academic Discipline in Cybersecurity
Postsecondary Education

Learning, intelligence, and machine learning, knowledge representations, exhaustive search, heuristic search, genetic algorithms, Attribute quality measures, data preprocessing, supervised symbolic and statistical learning, basics of artificial neural networks, unsupervised learning and cluster analysis, data classification data clustering, classification and clustering validity testing, data masking, data obfuscation techniques, data erasures, data storage security, data forensics, security policy

Digital Forensics (3 hours/lecture/Semester)

Computer crimes, evidence, extraction, preservation, an overview of hardware and operating systems, data recovery, digital evidence controls, computer forensic tools, network forensics, mobile network forensic, software reverse engineering, computer crime, and legal issues and ethical issues

Secure Software Development (3 hours/lecture/Semester)

Current state of software security, vulnerabilities during implementation, consequences, and prevention, consideration, for legacy C applications and web applications, secure software design and coding, software assurance, software security standards and tools, secure software engineering lifecycle, risk management in software development, software security testing, mobile applications, ethics, security policy

Communication and network security (3 hours/lecture/Semester)

Networking principles, network architecture, transmission Control, IEEE 802/ISO networks, protocol/Internet protocol, IETF networks and TCP/IP, naming and addressing (Domain Name System), data, encoding/decoding techniques, link layer protocols, routing protocols, transport layer, services, congestion control, quality of service, network services, Software Defined Networks (SDNs), programmable routers and overlay networks, wireless and mobile, networking, security in computer networks, multimedia networking, and network, management, high performance computing, virtualization and virtual hypervisor architecture, service models (client-server, peer-to-peer), service protocol concepts (IPC, APIs, IDLs)

Cybersecurity management (3 hours/lecture/Semester)

Governance and security policy, threat and vulnerability management, incident management, risk management, information leakage, crisis management and business continuity, legal and compliance, security awareness and security implementation considerations, analysis of information security & risk

Submission to KSU Proceedings on Cybersecurity Education, Research and Practice

management, access control, physical security, security architecture & design, business continuity & disaster recovery planning, application security, operations security, law, compliance & investigations

This course also reviews the building blocks of information systems and cryptography to reinforce the scope of security management.

Human and social security (3 hours/lecture/Semester)

Relationship to traditional security, relations with the development approach, economic insecurity measurements, The Human Security “Network”, Measuring “Human Security”, human security as programmatic and policy tool, Identity management, social engineering, Awareness and understanding, Social behavioral privacy and security, Personal data privacy and security, cybercrime, cyberlaw, cyber ethics, cyber policy, privacy.

A mapping between the ACM report and the suggested curriculum are as in Table 2:

ACM report Domains	Cryptograph	Data Science for Security	Secure Software Development	Digital Forensics	Communication and network security	Cybersecurity management	Human and social security
Data Security	X	X		X		X	
Software Security			X				
Component Security			X		X	X	
Connection Security			X		X		
System Security		X	X	X	X	X	
Human Security						X	X
Organizational Security				x		X	X
Societal Security				x		X	X

AlHamdani: Adopting the Cybersecurity Curriculum
Guidelines to Develop a Secondary and Primarily Academic Discipline in Cybersecurity
Postsecondary Education

Table 3: Cross courses with ACM Body of Knowledge

The suggested are seven courses with 21 credits/semester. Combining both the courses and the prerequisites will result in 45 credits.

Major Academic Discipline in Cybersecurity

To cover significant studies in cybersecurity, the 21 credits above need to be supported by another set of courses to reach the cumulative credits of 45–48 or maybe 50 credits/semester; suggested courses are listed below with a course overview description and expected student learning outcomes (SLOs).

Access Control

(3 hours/lecture/Semester)

Access control framework, risk and its impact on access control, business drivers for access controls, access control policies, standards, procedures, and guidelines, unauthorized access and security breaches, human nature, organizational behavior, and considerations, access control for information systems, physical access control, access control in the enterprise, system implementations, access control for remote workers, public key infrastructure and encryption, testing, access control assurance

Information Security and Risk Management (3 hours/lecture/Semester)

Risk management fundamentals, managing risk: threats, vulnerabilities, and exploits, maintaining compliance, developing a risk management plan, defining approaches, performing a risk assessment, identifying assets and activities to be protected, identifying and analyzing threats, vulnerabilities, and exploits, analyzing risk mitigation security controls, planning risk mitigation throughout the organization, mitigating risk with a business impact analysis, mitigating risk with a business continuity plan, mitigating risk with a disaster recovery plan, mitigating risk with a computer incident response team plan

Application Security (3 hours/lecture/Semester)

Information security and how it applies to the Microsoft Windows operating system and Linux system, security features, implement secure access controls, set up encryption, group policy controls, audit tools, backup and restore operations, networks from security vulnerabilities, security administration, apply best practices for handling operating system and application incidents

Operations Security

(3 hours/lecture/Semester)

Submission to KSU Proceedings on Cybersecurity Education, Research and Practice

Information as a military asset, targets and combatants, cyberwarfare, law, and ethics, intelligence operations in a connected world, offensive and defensive cyber warfare, the evolving threat, social engineering and cyberwarfare, defense-in-depth strategies, cryptography, and cyberwar, defending endpoints, defending networks, defending data, the Future of cyberwarfare

Security Architecture and Design (3 hours/lecture/Semester)

Threat modeling, security architecture, STRIDE, countermeasure, attack tree, computer security, information security, threat vulnerability, software security assurance

Business Continuity Planning and Disaster Recovery Planning (3 hours/lecture/Semester)

Business continuity and disaster recovery overview, legal and regulatory obligations regarding data and information security, project initiation, business impact analysis, risk mitigation strategy development, business continuity/disaster recovery plan development, emergency response and recovery, BC/DR plan maintenance, resource allocation, and cost-benefit analysis

Legal Regulations, Compliance, and Investigation (3 hours/lecture/Semester)

Licensing and intellectual property (e.g., copyright, trademark), professional ethics, support organization's code of ethics, investigations, policy, roles and responsibilities, Incident handling and response, evidence collection and handling, reporting and documenting, forensic procedures, media analysis, network analysis, software analysis, hardware/embedded device analysis, compliance requirements and procedures, regulatory environment, audits, reporting

Physical Security (3 hours/lecture/Semester)

Influence of physical design, introduction to vulnerability assessment, security Surveys and the audit, approaches to physical security, protective barriers/physical barriers, use of locks in physical crime prevention, security lighting & intrusion detection systems, alarms: intrusion detection systems, video technology, biometrics characteristics/access control and badges, stages of fire & standards, regulations, & guidelines, information technology systems infrastructure, security officers and equipment, monitoring/glass and windows/doors, physical security/fiber optics and robots

Information Security Project (3 hours/lecture/Semester)

Hands-on research work focused on security technology

<https://digitalcommons.kennesaw.edu/ccerp>

12

AlHamdani: Adopting the Cybersecurity Curriculum
Guidelines to Develop a Secondary and Primarily Academic Discipline in Cybersecurity
Postsecondary Education

Future direction

As we finalized, this work abet has adopted the cybersecurity track which based on Data Security, Software Security, System Security, Human Security, Organizational Security, and Societal Security. These are precisely the ACM base curriculum, and in addition, the Abet specifies the student outcome focus.

Across work is needed to bring the ACM curriculum and CAE guidance together to develop a combined curriculum satisfies both guidelines, and satisfies the based body of knowledge.

Conclusion

Recently, ACM's leading group of organizations built a framework curriculum for cybersecurity, where the suggested curriculum focused on eight domains. These domains are the center of cybersecurity education. The contribution of these domains is entirely different; however, both aim to build a framework for cybersecurity education. As a student graduates from higher academic education, that student can enhance his/her education depending on the work environment's requirements. This work suggested a curriculum for a major academic discipline and a second academic discipline that is designed to fulfill the ACM requirements for the second discipline, and in the case of the essential academic discipline, the curriculum meets the National Centers of Academic Excellence Cyber Operations program requirements.

References

- ACM. (2017). *Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education)*. New York, NY 10121-0701: Version 1.0 Report 31 December 2017.
- Al-Hamdani, W. A. (2006). Knowledge flow with information assurance track. *InfoSecCD '06 Proceedings of the 3rd annual conference on Information security curriculum development* (pp. Pages 52-57). Kennesaw, Georgia — September 22 - 23, 2006: ACM New York, NY, USA.
- niccs.us-cert.gov. (2018, 7 3). *A national initiative for cybersecurity careers and studies*. Retrieved from <https://niccs.us-cert.gov/formal-education/national-centers-academicexcellence-cae>

Submission to KSU Proceedings on Cybersecurity Education, Research and Practice

nsa.gov. (2018, July 3). *Center of Academic Excellence (CAE)*. Retrieved from <https://www.nsa.gov/resources/studentseducators/centers-academic-excellence/#ops>