CSEC Foundations Guidelines

Melissa Dark[1][0009−0001−7901−937], Philip Huff[2][0000−0003−0869−2147], Jun Dai[3][0000−0002−6890−6429], and Matt Bishop[4][0000−0002−7301−7060]

[1] Dark Enterprises, West Lafayette, IN USA
melissa.dark@darkenterprisesinc.com
[2] University of Arkansas at Little Rock, Little Rock, AR USA pdhuff@ualr.edu
[3] Worcester Polytechnic Institute, Worcester MA USA jdai@wpi.edu
[4] University of California David, Davis CA USA mabishop@ucdavis.edu

Abstract. This paper discusses a companion to the Computer Security Curriculum Guidelines 2017 (CSEC 2017). CSEC 2017 serves both introductory and advanced courses in a post-secondary program. The CSEC Foundations Guidelines focus specifically on the foundations of cybersecurity for introductory courses at the secondary and post-secondary school levels. This paper describes the methodology used to select the foundations, what those foundations are, and how the document is organized. It presents six knowledge areas based on those of CSEC 2017 (specifically, data security, network security, system security, software security, organizational security, and societal security) and makes recommendations about the sequencing and pacing of the material. Then, it provides examples of the learning outcomes for cryptography, access control, and data security topics in the Data Security knowledge area and instructional guidance for their use. The paper concludes with a discussion of the CSEC Foundations Guidelines used by the National Cybersecurity Teaching Academy and Coalition, which offers graduate certificates to US secondary school teachers to prepare them to teach cybersecurity. As a supplement to CSEC 2017, the resulting CSEC Foundations Guidelines were approved by the ACM in Jan 2025.

Keywords: cybersecurity foundations; CSEC 2017; introductory course secondary school education

1 Introduction

In 2017, a task force formed from the ACM, the IEEE Computer Society, the AIS SIGSAC, and the International Federation of Information Processing Societies Working Group 11.8, Computer Security Education and developed a set of Computer Security Curriculum Guidelines (CSEC 2017) [3]. These guidelines recommended a set of learning outcomes basic to various areas of computer security, and identified several as "essential meaning that regardless of the area of cybersecurity being studied, students should have a basic understanding of the material covered for those learning objectives.

As CSEC 2017 was a set of guidelines for post-secondary education, it did not focus on introductory courses in particular; rather, it serves a broad variety

of both introductory and advanced courses. A class in cybersecurity in secondary school, and an introductory course in post-secondary education, should focus on the foundations of cybersecurity to provide a practical basis on which learners can build knowledge.

To this end, another task force was formed to extract the foundational learning objectives from the learning essentials identified in CSEC 2017. Foundational knowledge "includes content that can be taught in an introductory course sequence without requiring prior cybersecurity knowledge" [2, p. 5]. Specifically, this task force had three objectives:

- To provide guidance to institutions setting up introductory courses in cybersecurity that focus on foundations;
- To provide foundational content based on CSEC 2017 and, where necessary, update it; and
- To provide foundational cybersecurity courses that cover common material sufficiently to allow articulation agreements among educational institutions.

The contribution of this paper is to present the methodology used to select these foundational topics, describe the knowledge domain framework used to inform course packing, and offer examples of corresponding learning outcomes.

2 Background

The cybersecurity workforce shortfall is widely known. The U.S. has several national efforts aimed at addressing the cybersecurity workforce shortfall that serve as the impetus for initial development of CSEC 2017 in and this expansion. The post-secondary CAE program in Information Security (now called "CAE in Cyber Defense" or "CAE-CD") launched in 1997 with recognition to 7 U.S. universities for producing cybersecurity graduates. Today there are nearly 500 CAE-CD colleges and universities. These schools are developing and offering a variety of academic programs in cybersecurity. A recent study found 803 certificates, associates, minors and bachelor degrees at NCAE-C institutions as of Spring 2024 as shown in table 1 [5, p. 27].

Table 1. Number and types of degrees awarded from universities and community (2-year) colleges in the US.

	Bachelor's Degrees	**Associate's Degrees**	**Minor/ Tracks**	**Certificate**	**Total**
University ($n = 289$)	180	19	178	68	445
Community College ($n = 157$)	12	125	46	175	358
Total ($n = 446$)	192	144	224	243	893

Another study found approximately 385 universities and 384 community colleges with a cybersecurity Classification for Instructional Programs (CIP) code

for bachelor's degrees and associate's degrees [12]. This sample included non NCAE-C schools as well. The growth in institutions and programs leads to growth in graduates. Ten-year growth in graduates from a Computer and Information Systems Security/Auditing/Information Assurance (CIP [5] Code 11.1003) is shown in Fig. 1(a). Fig. 1(b) displays 2024 graduates by degree types.

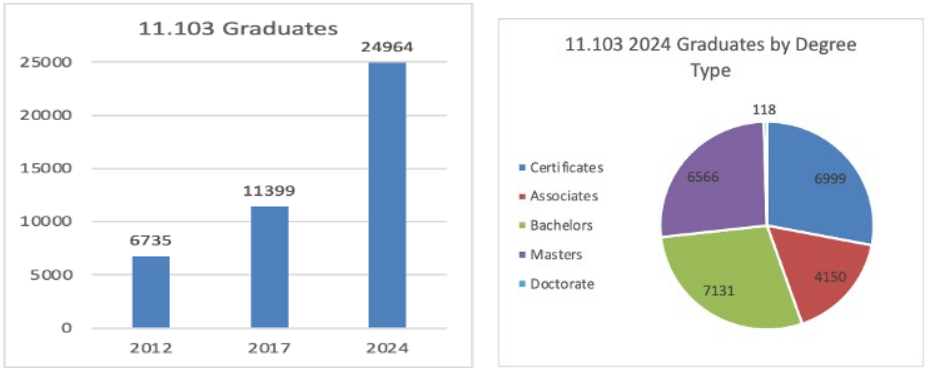

Fig. 1. (a) This shows the ten-year growth in CIP code 11.1003 (Computer and Information Systems Security/Auditing/Information Assurance) Grads. (b) shows the post-secondary graduates by degree types.

The CSEC2017 Joint Task Force on Cybersecurity Education (JTF) was officially launched in September 2015 in an effort to help standardize post-secondary cybersecurity education. The CSEC JTF published the curricular volume in 2017. The development process involved a broad global audience of stakeholders through continuous community engagement with the goals of aligning academic programs with industry needs in cybersecurity and developing curricular guidance that is comprehensive enough to support a wide range of program types. The resulting guideline rests on three cornerstones, namely knowledge areas, cross-cutting concepts, and disciplinary lens, to describes a vision of proficiency in cybersecurity. It defines 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. And it is grounded in fundamental principles that provide stability, yet is structured to provide flexibility to support evolving program needs. A recent search finds 49 ABET accredited programs using the search term "cybersecurity."

Since CSEC 2017 was published, the number of cybersecurity courses and pathways have started growing in U.S. secondary schools, spurred by pioneering programs such as GenCyber and Cyber Patriot, which are out-of-school-time curricular programs initiated between 2012–2014. When these programs were

[5] The Classification of Instructional Programs (CIP) is the taxonomic coding scheme used for instructional programs in higher education in the United States.

started, U.S. high schools were developing computer science courses and programs, but few to none had cybersecurity courses. A 2022 study found that 15% of the 23,882 public high schools in the United States offer a cybersecurity course [6]. The growth is notable.

The growth in secondary cybersecurity education presented a need to update CSEC 2017 to express foundational knowledge. This update serves as a benchmark for what students are expected to know and be able to do with respect to the foundations of cybersecurity. The purposes for the update are to guide instruction, assessment, and curriculum development to ensure consistent and appropriate learning outcomes across different schools and districts. The update can support both scalable high school to college and college to college articulation pathways nationwide whereas state standards are usually delimited to supporting local transfer.

3 Methodology

3.1 Deriving Foundational Topics from CSEC 2017

This work began by examining the essential topics identified in CSEC 2017, which are the knowledge areas and corresponding topics introduced early in a cybersecurity program regardless of specialization. Although these essentials offered a starting point, not all essential topics aligned with the goal of establishing foundational knowledge, which here means content that does not require prerequisite cybersecurity expertise. Consequently, the CSEC 2017 essential topics were mapped to those that could be introduced in a typical entry-level cybersecurity course.

Several CSEC 2017 knowledge areas were then merged to refine the foundational scope. Component Security was incorporated into System Security, based on the idea that systems comprise multiple components, and Human Security was similarly placed under Societal Security with the connection between individuals and society. A full review of CSEC 2017 also identified additional topics not officially labeled as essential but still appropriate for foundational instruction, including cross-border cyber law, ethics, and network hardware architecture. In contrast, topics such as data erasure were omitted upon determining that they were too advanced for entry-level instruction or no longer represented a widely required skill.

Many decisions regarding which topics to retain or revise were influenced by evolving industry trends and societal shifts, including the widespread adoption of social media, increasing privacy concerns, and the expanding global reach of supply chains, as evidenced by the new security control families introduced in NIST Special Publication 800-53 Revision 5 [10]. Moreover, technological advances since the re-lease of CSEC 2017 have been substantial, with global cloud computing growing at an annual rate of 20% [8] and AI expanding by 27% [10]. Although AI was recognized as an increasingly important theme, its coverage was kept minimal in the cur-rent curriculum due to the concurrent development of dedicated AI curricular standards.

3.2 Structuring and Aligning Learning Outcomes

The guidelines build on the knowledge areas and topics outlined in CSEC 2017 but diverge by organizing these topics into structured units designed for course packaging. Unlike CSEC 2017, which includes the entire body of knowledge in cybersecurity, this supplement emphasizes the foundational learning outcomes for course packaging. A second topical level was added under the knowledge area to better group common topics that span multiple knowledge areas. For example, the topic of *Attacks* spans Network Security, Software Security, and Societal Security knowledge areas.

The update retains the cross-cutting concepts from CSEC 2017, including Confidentiality, Integrity, Availability, Risk, Adversarial Thinking, and Systems Thinking, while introducing the additional principle of Defense in Depth. These concepts are explicitly mapped to each learning outcome to reinforce core principles and foster a cohesive understanding of the security mindset throughout the curriculum. To define the appropriate cognitive level for each outcome, Bloom's Taxonomy, as adapted for computing [1], is employed to ensure the outcomes align with the depth of knowledge expected in an introductory cybersecurity course. Fig. 2 shows these relationships pictorially.

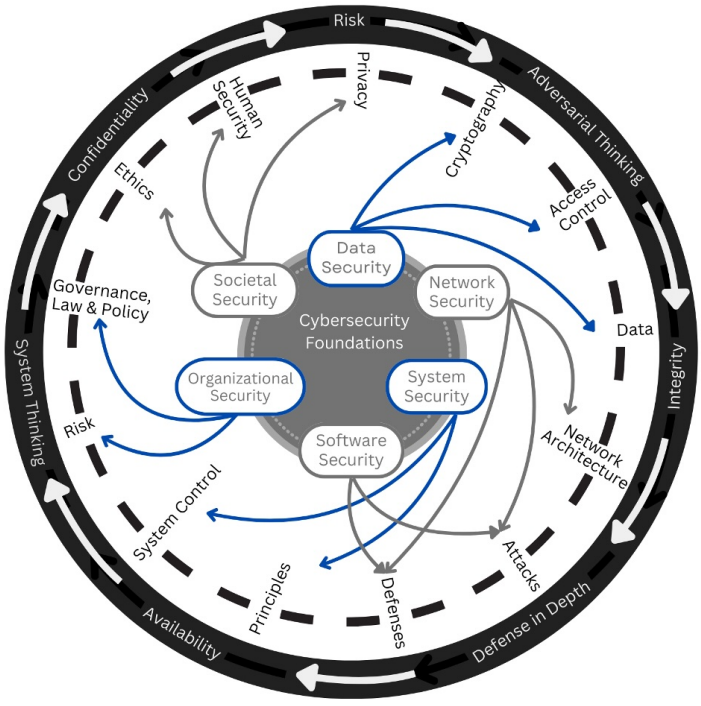

Fig. 2. Relationship among foundational concepts and knowledge areas.

3.3 Review and Feedback Process

Two formal review periods were conducted to gather public feedback on the learning outcomes across the domains of Data Security, Network Security, System Security, Organizational Security, and Societal Security. Reviewers raised several key issues:

- **Clarity and Specificity:** Feedback indicated that learning outcomes in areas such as cryptography, networking protocols, and system hardening were overly general and ambiguous.
- **Content Gaps and Level:** Respondents noted missing topics — such as key management and public key infrastructure (PKI) — and observed that many outcomes were set at too low a level of detail for foundational instruction.

In response, the drafting team revised the learning outcome language to emphasize higher-order abilities. They improved clarity by combining overlapping outcomes, filling content gaps with new outcomes, and updating instructional guidance, references, and course sequencing.

During the second comment period, additional feedback encouraged a broader treatment of emerging concerns and the integration of hands-on activities. Overall, reviewers were favorable of the changes in response to the first round of comments, but requested more detailed coverage of AI security, mobile and cloud security, digital forensics, and case studies of actual breaches.

Consequently, the instructional guide was further expanded to incorporate more lab-based exercises, recommendations to cover most of the emerging technologies re-quested, and the inclusion of case studies on data breaches to illustrate ethical and societal implications. However, while suggestions to include advanced topics like digital forensics and hybrid cloud configurations were considered, these were ultimately judged to fall outside the intended scope of foundational instruction.

4 The Document

4.1 Document Structure and Features

This CSEC 2017 supplement, approved by the ACM in January 2025, organizes the guidelines into knowledge areas. Each area is divided into topics. For every topic, there is a concise learning outcome summary that can help instructors or curriculum planners shape course objectives or module outlines. Each learning outcome is assigned a unique identifier to facilitate cross referencing throughout the curriculum.

The tables of learning outcomes also include references to the cross-cutting concepts. This approach highlights the shared principles that connect the knowledge are-as. Many learning outcomes include a link to more detailed instructional guidance. Since the guidelines are intended for secondary schools, colleges, universities, and professional training, these additional materials clarify definitions,

provide background information, and offer illustrative examples. Users of the guidelines can navigate through links between the concise outcomes and the more detailed supplementary guidance.

4.2 Knowledge Areas and Topics

The guidelines draw on CSEC 2017 but refine or merge topics where appropriate to maintain a foundational focus.

1. Data Security is divided into Access Control and Cryptography, followed by a broader view of data protection. Access Control and Cryptography covers authorization and encryption methods. Data Security is also a topic area focusing on protecting data in different states, such as at rest, in transit, or in use.
2. Network Security is organized into Network Architecture, Attacks, and Defense. Network Architecture introduces essential networking concepts, including the five-layer Internet model[6], routing, and standard protocols. Attacks examines the methods used to compromise networks, and Defense explores countermeasures and how they address the identified threats. A similar structure appears in Software Security and Societal Security when discussing attacks and defenses, so instructors can reinforce connections across these topics.
3. System Security includes Security Principles and System Controls and Lifecycle. Security Principles covers confidentiality, integrity, availability, trust, and defense in depth. System Controls and Lifecycle addresses how to design, build, and maintain systems with security as a central consideration. Access control also reappears here, but at a system level rather than a data level.
4. Software Security addresses fundamental ideas in secure software that focus on the software development lifecycle, common vulnerabilities, and defensive strategies. Attacks and defenses in software are introduced at a level appropriate for learners without programming experience. Topics include the nature of software weaknesses and awareness of frequent exploits, along with the basics of secure design practices.
5. Organizational Security concentrates on risk management and policy. This area explains how organizations address and mitigate security risks through formal processes and frameworks. A related topic is Governance, Law, and Policy, which overlaps with Societal Security but is approached here in terms of organizational structures, internal regulations, and practical enforcement.
6. Societal Security covers a broad set of fundamentals that frame cybersecurity in everyday life. Attacks in this context emphasize how adversaries affect people and institutions at a societal level. Ethics introduces principles of right and wrong behavior in cybersecurity, while Governance, Law, and Policy looks at major legal, regulatory, and policy considerations. Human Security,

[6] This is the same as the four layer model, with a physical layer added.

originally its own area in CSEC2017, is now part of Societal Security to underscore its close links with social and legal questions. Privacy is also highlighted, given the prominence of regulations such as the General Data Protection Regulation and recent updates to NIST guidelines.

4.3 Sequencing and Pacing

Because the foundational topics are extensive, the guidelines recommend splitting them into a two course sequence called Cybersecurity I and Cybersecurity II. Cybersecurity I should begin with security principles and ethics, followed by technical foundations in topics like cryptography and access control. This prepares learners for deeper exploration of topics for attacks and defenses.

Cybersecurity II, as proposed in the guideline, focuses on conceptual foundations and covers topics such as attacks, defenses, data security, and risk management. It then transitions into broader societal themes, including law, policy, and ethics. The course sequence is designed to respect dependencies between foundational topics. For instance, understanding data security builds on knowledge of cryptography and net-work security, while all topics rely on core security principles such as confidentiality, integrity, and availability. This structured progression ensures that learners develop a strong technical foundation in Cybersecurity I, enabling them to apply that knowledge effectively to more complex and abstract top-ics in Cybersecurity II.

The guidelines propose weekly segment recommendations for both secondary and post-secondary institutions using a credit hour system in which one unit of credit represents approximately three hours of academic work per week over a 15-week semester [11]. Consequently, a three-credit-hour course translates to about nine hours of combined in-class and out-of-class instruction each week. The guidelines also include a breakdown of these weekly instructional hours by topic and estimates the number of hours based on the quantity and complexity of specific learning outcomes. For instance, the security principles topic comprises seven learning outcomes and is projected to require about three weeks of instruction in the credit hour system, compared to six weeks at the secondary level. In general, the estimated instructional hours are doubled for secondary schools to compensate for the additional holidays, attendance mandates, and testing requirements that reduce total classroom time. In fact, one study suggests that only around half of the available time in secondary schools is used for direct in-class instruction [7]. Altogether, the guidelines recommend approximately 28 instructional hours over a 15-week semester in the credit hour system. When exam periods are factored in, this aligns with the full 30-week duration of two three-credit-hour courses commonly offered at post-secondary institutions.

Finally, while these courses do not require prerequisites, secondary schools may have the opportunity to develop preparatory pathways leading to dual-credit or concurrent-credit cybersecurity courses. Likewise, the guidelines map topic areas to the Computer Science Curricula 2023 knowledge areas [9]. For instance, cryptography benefits from foundational knowledge in mathematics and statistics, such as sets, relations, and modular arithmetic. Although these

are not required prerequisites, students with prior exposure to these topics are likely to benefit significantly.

5 Examples

The foundational learning outcomes are organized by knowledge areas, aligned with the CSEC 2017 structure, and then by topics to facilitate curriculum development. Topics have a summary learning outcome, suitable for course syllabi, while the core instructional focus is detailed through component learning outcomes, each labeled with unique IDs for easy reference. Most component learning outcomes link to corresponding guidance statements in the Instructional Guidance section, with the electronic version enabling seamless navigation between guidance and outcomes. These guidelines support educators and curriculum developers by ensuring consistent terminology, increasing awareness of reference materials, and highlighting cross-cutting concepts that connect themes across knowledge and topic areas.

The following uses Data Security as an example to illustrate the structure of the knowledge area and its corresponding instructional guidance. Similarly, other knowledge areas—such as Network Security, System Security, Software Security, Organizational Security, and Societal Security—are outlined in the same manner.

Data Security (*Knowledge Area*) Cryptography (*Topic*)

Learning Outcome Summary: Understand and apply the fundamental principles of cryptography to ensure the confidentiality, integrity, availability, and non-repudiation of data, while recognizing and utilizing cryptographic methods and secure protocols in practical scenarios. (*Summary Learning Outcome*)
Access Control (*Topic*)

Learning Outcome Summary: Understand and differentiate key access control models and terminologies, and explain how identification, authentication, and authorization work together to enforce effective access control mechanisms in various organizational contexts. (*Example Summary Learning Outcome*)
Data Security (*Topic*)

Example Instructional Guidance for Data Security

Unless otherwise specified, all definitions come from the NICCS Glossary of Common Cybersecurity Words and Phrases [4].

LO	Guidance

LO	Guidance
DS1	Please see SS1 for definitions of confidentiality, integrity, and availability. The McCumber Cube and CIA Triad could be used to facilitate the explanation. The E-MATE 2.0 has an interactive lesson about "The McCumber Cube and CIA Triad" here:mhttps://www.ncyte.net/faculty/cybersecurity-curriculum/college- curriculum/interactive-lessons/the-mccumber-cube-and-cia-triad To provide additional context, the MITRE ATT&CK framework[7] enumerates specific threats and impacts to data security within the Impact tactic. These include threats such as data destruction, manipulation, theft, and corruption. Each of these threats directly aligns with potential losses in confidentiality, integrity, or availability, which reinforces the need for cryptography as countermeasures to these threats. Add hands-on exercise: encrypting a word or message using a very simple encryption algorithm. Similarly, students can decrypt a small encrypted data set.
DS2	The E-MATE 2.0 has an interactive lesson about "Cryptography" here, which can be helpful: https://www.ncyte.net/faculty/cybersecurity-curriculum/college- curriculum/interactive-lessons/cryptography
DS3	Add hands-on applications to help learners with this challenging concept. **Cipher** refers to cryptographic algorithm, a well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. Cryptographic keys include symmetric key, public key, private key. **Encrypt** refers to the process of transforming plaintext into ciphertext. **Decrypt** refers to the process of transforming ciphertext into its original plaintext. **Cryptanalysis** refers to the operations performed in defeating or circumventing cryptographic protection of information by applying mathematical techniques and without an initial knowledge of the key employed in providing the protection. **Cryptographic hashing** refers to a process of applying a mathematical algorithm against a set of data to produce a numeric value (a hash value) that represents the data. **Non-repudiation** refers to a property achieved through cryptographic methods to protect against an individual or entity falsely denying having performed a particular action related to data. **Cryptology** refers to the mathematical science that deals with crypt- analysis and cryptography.
DS4	Add hands-on exercise: encrypting a word or message using a symmetric encryption algorithm, such as a DES or AES algorithm.

[7] https://attack.mitre.org

LO	Guidance
DS5	Add hands-on exercise: encrypting a word or message using an asymmetric encryption algorithm, such as an RSA algorithm. The exercise includes the generation of an RSA key pair (i.e., public key and private key), followed by RSA encryption and decryption based on them. A recommended resource for further understanding is the NIST Hash Functions Project[8], which provides guidance on secure algorithms robust enough for use in modern systems. While detailed knowledge of specific algorithms is not required at this foundational level, understanding the concept of secure hashing is essential. To reinforce learning, students can experiment with Python scripts to generate cryptographic hash values and explore real-world examples, such as hashing in blockchain or cryptocurrencies.
DS7	Explain that HTTPS and SSH use cryptography to protect communications. Add hands on exercise: use wireshark to observe encrypted vs. unencrypted traffic.
DS8	Present a case study on the DigiNotar PKI failure, illustrating how poor key management led to a major security breach. Have students engage in a role-play exercise to simulate setting up a PKI, where they act as a Certificate Authority (CA), generate keys, and issue certificates, reinforcing the key components of secure key management.
DS9	**Identities** refer to who or what is requesting access. Credentials refer to the information used to prove identity. **Authentication** refers to the process of verifying the identity or other attributes of an entity (user, process, or device). **Authorization** refers to a process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Controls for these can be physical as well. Examples: physical ID validation, visitor control, door locks, warning signs.

[8] https://csrc.nist.rip/projects/hash-functions

LO	Guidance
DS10	Cover the existence of DAC and MAC access control models. Describe **Discretionary Access Control (DAC)** as a form of access control where the owner of the resource determines access. Include instructional guidance on applying access control methodologies. Describe **Mandatory Access Control (MAC)** as a form of access control where access is governed by a centralized authority based on predefined rules. Describe **Role-Based Access Control (RBAC)** as a form of access control that restricts access based on the roles and responsibilities within an organization. The states of data include the following: – Data-at-rest refers to data stored on devices or systems that are not actively accessed or transferred, such as information on hard drives, databases, or flash drives. Example mechanisms used to secure data-at-rest: encryption, access control. Data-in-motion refers to data traveling between devices or networks, including information sent via web browsing, file transfer, email communication, or instant messaging. Example mechanisms used to secure data-in-motion: HTTPS, VPN. – Data-in-use refers to data that is actively accessed, processed, or read by a user or software, such as data retrieved and processed during a SQL query. Example mechanisms used to secure data-in-use: memory encryption, sandboxing, access control, and masking. Anonymization techniques enhance confidentiality and privacy across all states of data by removing or obscuring personally identifiable information (PII) and sensitive attributes. These techniques ensure that even if data is accessed, it cannot be attributed to specific individuals or entities.

6 Implementation

The CSEC 2017 update is already being used in the U.S. by an initiative called NCTAC (National Cybersecurity Teaching Academy and Coalition). NCTA was launched in 2021 with funding from NSA/NCAE-C to DePaul University, the University of Arkansas Little Rock (UALR), the University of Louisville, and DARK Enterprises. California State University-Sacramento joined in 2022 with additional NSA/NCAE-C support. These four universities developed and offer a graduate certificate to high school teachers that prepares them for teaching cybersecurity courses. The NCTA goals are:

1. increase teachers' cybersecurity content knowledge (teachers cannot teach what they do not know);
2. expand national capacity for dual credit in cybersecurity; and
3. enhance the quality of high school cybersecurity courses.

ID	Component Learning Outcomes	Cross-Cutting Concepts
DS1	Explain cryptography including its relationship to confidentiality, integrity, and availability of data. [Guidance]	CIA
DS2	Encrypt a small data set using a simple encryption algorithm. [Guidance]	CIA
DS3	Describe basic cryptography terms, including ciphers, cryptographic keys, encrypt, decrypt, cryptanalysis, cryptographic hashing, non-repudiation, and cryptology. [Guidance]	CIA
DS4	Use symmetric ciphers with a shared secret key to transform plaintext to ciphertext. [Guidance]	CIA
DS5	Use asymmetric ciphers with a public key to transform plaintext to ciphertext. [Guidance]	CIA
DS6	Use cryptographic hash functions to create one-way transformations that convert data of arbitrary length into fixed-length hash values. [Guidance]	CIA
DS7	Recognize secure protocols, like HTTPS and SSH, which use cryptography to protect communication. [Guidance]	CIA, Systems thinking, Adversarial thinking
DS8	Recognize the critical role of key management and public key infrastructure (PKI) for ensuring the secure generation, distribution, and storage of cryptographic keys. [Guidance]	CIA, Systems thinking

ID	Component Learning Outcomes	Cross-Cutting Concepts
DS9	Differentiate between identification, authentication, and access authorization of people and devices. [Guidance]	CIA, Systems thinking, Adversarial thinking
DS10	Articulate the basic differences between the following forms of access control: Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC). [Guidance]	CIA, Systems thinking

ID	Component Learning Outcomes	Cross-Cutting Concepts
DS11	Summarize the different states of data (data-at-rest, data-in-motion, and data-in-use) and the mechanisms used to secure each. [Guidance]	Systems thinking

The graduate certificate initially included 12-credit hours and expanded to 18-credit hours to support dual enrollment requirements. To date, 64 teachers matriculated in 2022 and have completed the graduate certificate, 20 matriculated in 2023 and will graduate in summer 2025, and 38 teachers matriculated in summer 2024 and will graduate in summer 2026.

In 2024 the NCTA coalition expanded to include Dakota State University, the University of Arizona, the University of Maryland Global Campus, and Worcester Polytechnic Institute and formed the National Cybersecurity Teaching Coalition (NCTC). NCTC will continue to offer NCTA graduate certificates with 175 scholarships available in 2025 and another 175 scholarships in 2026.

An eight-credit course based on the CSEC Supplement will be implemented in the 2025-2026 academic year at four high schools in Arkansas and at the University of Arkansas at Little Rock. This implementation will pilot test the application of the CSEC Supplement for dual credit in the United States. In addition, the new cohort of NCTA teacher scholars will learn the foundations of cybersecurity expressed in the CSEC supplement in summer 2025 so that NCTAC can launch additional dual credit cybersecurity courses in the 2026–2027 academic year.

7 Conclusion

Building educational opportunities in cybersecurity is important to developing a sustainable supply chain of cybersecurity talent. The United States educational system has focused on expanding post-secondary educational programs over the past 25 or more years. As cybersecurity has matured into a discipline, this expansion included not only more programs, but growth in the types of programs. Specifically, cybersecurity is now found 1) in a variety of disciplines, such as computer science, computer engineer-ing, information systems, information technology and business, and 2 at a variety of levels, such as baccalaureate, associate, and now secondary. The growth is exciting but also presents challenges in that there are no clear pathways for students to follow across disciplines and levels. The updated CSEC 2017 guidelines that specify the foundations of cybersecurity are well-poised to support educational pathways in the U.S.

Acknowledgments. This work was supported by an award from the ACM. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the ACM or any other organization.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. ACM Committee for Computing Education in Community Colleges (CCECC): Bloom's for Computing: Enhancing Bloom's Revised Taxonomy with Verbs

for Computing Disciplines. ACM, New York, NY, USA (Aug 2023). https://doi.org/10.1145/3587276
2. ACM Task Group: Supplement to csec 2017: Foundational cybersecurity content and instructional guidance for secondary and postsecondary cybersecurity education. Technical report, ACM, New York, NY, USA (Jan 2025)
3. ACM/IEEE-CS/AIS SIGSEC/IFIP WG 11.8 Joint Task Force: Cybersecurity curricula 2017: Curriculum guidelines for undergraduate degree programs in cybersecurity. Tech. Rep. Version 1.0, ACM, New York, NY, USA (Dec 2017). https://doi.org/10.1145/3184594
4. for Cybersecurity Careers, N.I., Studies: Explore terms: A glossary of common cybersecurity words and phrases (Apr 2024), https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary
5. Dark, M., Daugherty, J.: E3c: A report of early college cybersecurity credit. Technical report, Dark Enterprises, Inc., West Lafayette, IN, USA (May 2024), https://teachcyber.org/e3c/
6. Dark, M., *et al.*: Cybersecurity education: Availability & access in public high schools (Dec 2023), https://cybersupply.org/
7. Fisher, D.: The use of instructional time in the typical high school classroom. The Educational Forum **73**(2), 1689–176 (Apr 2009). https://doi.org/10.1080/00131720902739650
8. Gartner, I.: Forecast: Public cloud services, worldwide, 2022-2028, 2q24 update. Technical Report 5541595, Gartner Research (Jun 2024), https://www.gartner.com/en/documents/5541595
9. Kumar, A.N., Raj, R.K., Aly, S.G., Anderson, M.D., Becker, B.A., Blumenthal, R.L., Eaton, E., Epstein, S.L., Goldweber, M., Jalote, P., Lea, D., Oudshoorn, M., Pias, M., Reiser, S., Servin, C., Simha, R., Winters, T., Xiang, Q.: Computer Science Curricula 2023. ACM, New York, NY, USA (Jan 2024). https://doi.org/10.1145/3664191
10. Statista: Artificial intelligence (2023), https://www.statista.com/outlook/tmo/artificial-intelligence/worldwide
11. Wolanin, T.R.: The student credit hour: An international exploration. New Directions for Higher Education **2003**(122), 99–117 (Summer 2003). https://doi.org/10.1002/he.113