

The State Board of Education (SBOE) proposes new §126.51 and §126.52, concerning Texas Essential Knowledge and Skills (TEKS) for Technology Applications. The proposed new sections would add TEKS for two new technology applications courses in cybersecurity for implementation in the 2019-2020 school year.

BACKGROUND INFORMATION AND JUSTIFICATION: The 85th Texas Legislature, Regular Session, 2017, passed House Bill (HB) 3593, adding Texas Education Code (TEC), §28.002(f)(2), to require that the SBOE approve courses in cybersecurity for credit for high school graduation. HB 3593 amended TEC, §28.025(c-1)(1), to add cybersecurity and computer coding to the courses to be included in a STEM endorsement. HB 3593 also added TEC, §28.025(c)(10), to require that the SBOE adopt or select five technology applications courses on cybersecurity to be included in a cybersecurity pathway for the STEM endorsement.

In spring 2015, a new Principles in Cybersecurity innovative course was approved by the commissioner of education for use beginning with the 2016-2017 school year. School districts and open-enrollment charter schools may offer any state-approved innovative course for elective credit with the approval of the local board of trustees.

In August 2018, a committee of secondary and postsecondary educators and business and industry representatives were selected to develop recommended TEKS for new cybersecurity courses for the pathway. The committee convened for the first face-to-face meeting in Austin in September 2018 to begin working on recommendations for a TEKS-based foundational course in cybersecurity based on the Principles in Cybersecurity innovative course. The committee participated in an additional face-to-face meeting in October 2018 to develop recommendations for a second cybersecurity course that would serve as a capstone for the cybersecurity pathway. At the November 2018 meeting, the SBOE discussed proposed new 19 TAC §126.51 and §126.52. Draft TEKS for the proposed new courses were sent to interested stakeholders to provide feedback in December 2018. In January 2019, the committee participated in another face-to-face meeting to review comments provided by interested stakeholders and to finalize recommendations for the two cybersecurity courses.

The proposed new sections would add §126.51, Foundations of Cybersecurity (One Credit), and §126.52, Cybersecurity Capstone (One Credit), to the TEKS for technology applications.

The SBOE approved the new sections for first reading and filing authorization at its February 1, 2019 meeting.

FISCAL IMPACT: Monica Martinez, associate commissioner for standards and support services, has determined that for the first five-year period the proposal is in effect there will be fiscal implications for state government. For fiscal year 2019, the estimated cost to Texas Education Agency (TEA) to reimburse committee members for travel to review and streamline the TEKS is \$10,000. There would also be implications for the TEA if the state creates professional development to help teachers and administrators understand the new TEKS. Any professional development that is created would be based on whether TEA receives an appropriation for professional development in the next biennium.

The proposal may have fiscal implications for school districts and charter schools to implement the new TEKS. The costs may include the need for professional development and revisions to district-developed databases, curriculum, and scope and sequence documents. Since curriculum and instruction decisions are made at the local district level, it is difficult to estimate the fiscal impact on any given district.

LOCAL EMPLOYMENT IMPACT: The proposal has no effect on local economy; therefore, no local employment impact statement is required under Texas Government Code, §2001.022.

SMALL BUSINESS, MICROBUSINESS, AND RURAL COMMUNITY IMPACT: The proposal has no direct adverse economic impact for small businesses, microbusinesses, or rural communities; therefore, no regulatory flexibility analysis specified in Texas Government Code, §2006.002, is required.

COST INCREASE TO REGULATED PERSONS: The proposal does not impose a cost on regulated persons, another state agency, a special district, or a local government and, therefore, is not subject to Texas Government Code, §2001.0045.

TAKINGS IMPACT ASSESSMENT: The proposal does not impose a burden on private real property and, therefore, does not constitute a taking under Texas Government Code, §2007.043.

GOVERNMENT GROWTH IMPACT: TEA staff prepared a Government Growth Impact Statement assessment for this proposed rulemaking. The proposed rulemaking would not create or eliminate a government program; would not require the creation of new employee positions or elimination of existing employee positions; would not require an increase or decrease in future legislative appropriations to the agency; would not require an increase or decrease in fees paid to the agency; would not create a new regulation; would not expand, limit, or repeal an existing regulation; would not increase or decrease the number of individuals subject to its applicability; and would not positively or adversely affect the state's economy.

PUBLIC BENEFIT AND COST TO PERSONS: Ms. Martinez has determined that for each year of the first five years the proposal is in effect, the public benefit anticipated as a result of enforcing the proposal would be the addition of two new TEKS-based courses for students and an increase in flexibility in meeting graduation requirements. There is no anticipated economic cost to persons who are required to comply with the proposal.

DATA AND REPORTING IMPACT: The proposal would have no new data and reporting impact.

PRINCIPAL AND CLASSROOM TEACHER PAPERWORK REQUIREMENTS: TEA has determined that the proposal would not require a written report or other paperwork to be completed by a principal or classroom teacher.

PUBLIC COMMENTS: The public comment period on the proposal begins February 22, 2019, and ends March 29, 2019. A form for submitting public comments is available on the TEA website at [https://tea.texas.gov/About_TEA/Laws_and_Rules/SBOE_Rules_\(TAC\)/Proposed_State_Board_of_Education_Rules/](https://tea.texas.gov/About_TEA/Laws_and_Rules/SBOE_Rules_(TAC)/Proposed_State_Board_of_Education_Rules/). Comments on the proposal may also be submitted to Cristina De La Fuente-Valadez, Rulemaking, Texas Education Agency, 1701 North Congress Avenue, Austin, Texas 78701. The SBOE will take registered oral and written comments on the proposal at the appropriate committee meeting in April 2019 in accordance with the SBOE board operating policies and procedures. A request for a public hearing on the proposal submitted under the Administrative Procedure Act must be received by the commissioner of education not more than 14 calendar days after notice of the proposal has been published in the *Texas Register* on February 22, 2019.

STATUTORY AUTHORITY. The new sections are proposed under Texas Education Code (TEC), §7.102(c)(4), which requires the State Board of Education (SBOE) to establish curriculum and graduation requirements; TEC, §28.002(a), which identifies the subjects of the required curriculum; TEC, §28.002(c), which requires the SBOE to by rule identify the essential knowledge and skills of each subject in the required curriculum that all students should be able to demonstrate and that will be used in evaluating instructional materials and addressed on the state assessment instruments; TEC, §28.002(f)(2), which requires the SBOE to approve courses in cybersecurity for credit for high school graduation; TEC, §28.025(a), which requires the SBOE to by rule determine the curriculum requirements for the foundation high school graduation program that are consistent with the required curriculum under TEC, §28.002, and to designate the specific courses in the foundation curriculum that are required under the foundation high school program; TEC, §28.025(c-1)(1), which establishes that an endorsement may be earned in science, technology, engineering, and mathematics (STEM), which includes courses related to science, including environmental science; technology, including computer science, cybersecurity, and computer coding; engineering; and advanced mathematics; and TEC, §28.025(c-10), which requires the SBOE to adopt or select five technology applications courses on cybersecurity to be included in a cybersecurity pathway for the STEM endorsement.

CROSS REFERENCE TO STATUTE. The new sections implement Texas Education Code, §§7.102(c)(4), 28.002, and 28.025.

<rule>

§126.51. Foundations of Cybersecurity (One Credit).

- (a) General requirements. Students shall be awarded one credit for successful completion of this course. This course is recommended for students in Grades 9-12.

(b) Introduction.

- (1) Career and technical education instruction provides content aligned with challenging academic standards and relevant technical knowledge and skills for students to further their education and succeed in current or emerging professions.
- (2) Cybersecurity is an evolving discipline concerned with safeguarding computers, networks, programs, and data from unauthorized access. As a field, it has gained prominence with the emergence of a globally-connected society. As computing has become more sophisticated, so too have the abilities of malicious agents looking to penetrate networks and seize private information. By evaluating prior incidents, cybersecurity professionals have the ability to craft appropriate responses to minimize disruptions to corporations, governments, and individuals.
- (3) In the Foundations of Cybersecurity course, students will develop the knowledge and skills needed to explore fundamental concepts related to the ethics, laws, and operations of cybersecurity. Students will examine trends and operations of cyberattacks, threats, and vulnerabilities. Students will review and explore security policies designed to mitigate risks. The skills obtained in this course prepare students for additional study in cybersecurity. A variety of courses are available to students interested in this field. Foundations of Cybersecurity may serve as an introductory course in this field of study.
- (4) Statements that contain the word "including" reference content that must be mastered, while those containing the phrase "such as" are intended as possible illustrative examples.

(c) Knowledge and skills.

- (1) Employability skills. The student demonstrates necessary skills for career development and successful completion of course outcomes. The student is expected to:
 - (A) identify and demonstrate employable work behaviors such as regular attendance, punctuality, maintenance of a professional work environment, and effective written and verbal communication;
 - (B) identify and demonstrate positive personal qualities such as authenticity, resilience, initiative, and a willingness to learn new knowledge and skills;
 - (C) solve problems and think critically;
 - (D) demonstrate leadership skills and function effectively as a team member; and
 - (E) demonstrate an understanding of ethical and legal responsibilities in relation to the field of cybersecurity.
- (2) Employability skills. The student identifies various employment opportunities and requirements in the cybersecurity field. The student is expected to:
 - (A) identify job and internship opportunities as well as accompanying duties and tasks;
 - (B) research careers in cybersecurity and information assurance along with the education and job skills required for obtaining a job in both the public and private sectors;
 - (C) identify and discuss certifications for cybersecurity-related careers; and
 - (D) research and develop resumes, digital portfolios, or professional profiles in the cybersecurity field.
- (3) Ethics and laws. The student understands ethical and current legal standards, rights and restrictions governing technology, technology systems, digital media, and the use of social media. The student is expected to:
 - (A) demonstrate and advocate for ethical and legal behaviors both online and offline among peers, family, community, and employers;
 - (B) research local, state, national, and international cyber law such as the PATRIOT Act of 2001, General Data Protection Regulation, and Digital Millennium Copyright Act;

- (C) research historic cases or events regarding cyber;
 - (D) demonstrate an understanding of ethical and legal behavior when presented with various scenarios related to cyber activities;
 - (E) define and identify techniques such as hacking, phishing, social engineering, online piracy, spoofing, and data vandalism; and
 - (F) identify and use appropriate methods for citing sources.
- (4) Ethics and laws. The student identifies the consequences of ethical versus malicious hacking. The student is expected to:
- (A) identify motivations for hacking;
 - (B) identify and describe the impact of cyberattacks on the global community, society, and individuals;
 - (C) distinguish between a cyber attacker and a cyber defender;
 - (D) differentiate types of hackers such as black hats, white hats, and gray hats;
 - (E) determine possible outcomes and legal ramifications of ethical versus malicious hacking practices; and
 - (F) debate the varying perspectives of ethical versus malicious hacking.
- (5) Ethics and laws. The student identifies and defines cyberterrorism and counterterrorism. The student is expected to:
- (A) define cyberterrorism, state-sponsored cyberterrorism, and hacktivism;
 - (B) compare and contrast physical terrorism and cyberterrorism, including domestic and foreign actors;
 - (C) define and explain intelligence gathering and counterterrorism;
 - (D) identify the role of cyber defenders in protecting national interests and corporations;
 - (E) identify the role of cyber defense in society and the global economy; and
 - (F) explain the importance of protecting public infrastructures such as electrical power grids, water systems, pipelines, transportation, and nuclear plants.
- (6) Digital citizenship. The student understands and demonstrates the social responsibility of end users regarding significant issues related to digital technology, digital hygiene, and cyberbullying. The student is expected to:
- (A) identify and understand the nature and value of privacy;
 - (B) analyze the positive and negative implications of a digital footprint and the maintenance and monitoring of an online presence;
 - (C) discuss the role and impact of technology on privacy;
 - (D) identify the signs, emotional effects, and legal consequences of cyberbullying and cyberstalking; and
 - (E) identify and discuss effective ways to prevent, deter, and report cyberbullying.
- (7) Cybersecurity skills. The student understands basic cybersecurity concepts and definitions. The student is expected to:
- (A) define information security and cyber defense;
 - (B) identify basic risk management and risk assessment principles related to cybersecurity threats and vulnerabilities;

- (C) explain the fundamental concepts of confidentiality, integrity, availability, authentication, and authorization;
 - (D) describe the inverse relationship between privacy and security;
 - (E) identify and analyze cybersecurity breaches and incident responses;
 - (F) identify and analyze security concerns in areas such as physical, network, cloud, and web;
 - (G) define and discuss challenges faced by cybersecurity professionals;
 - (H) identify common risks, alerts, and warning signs of compromised computer and network systems;
 - (I) understand and explore the vulnerability of network-connected devices; and
 - (J) use appropriate cybersecurity terminology.
- (8) Cybersecurity skills. The student understands and explains various types of malicious software (malware). The student is expected to:
- (A) define malware, including spyware, ransomware, viruses, and rootkits;
 - (B) identify the transmission and function of malware such as Trojans, worms, and viruses;
 - (C) discuss the impact malware has had on the cybersecurity landscape;
 - (D) explain the role of reverse engineering for detecting malware and viruses;
 - (E) compare free and commercial antivirus software alternatives; and
 - (F) compare free and commercial anti-malware software alternatives.
- (9) Cybersecurity skills. The student understands and demonstrates knowledge of techniques and strategies to prevent a system from being compromised. The student is expected to:
- (A) define system hardening;
 - (B) demonstrate basic use of system administration privileges;
 - (C) explain the importance of patching operating systems;
 - (D) explain the importance of software updates;
 - (E) describe standard practices to configure system services;
 - (F) explain the importance of backup files; and
 - (G) research and understand standard practices for securing computers, networks, and operating systems.
- (10) Cybersecurity skills. The student understands basic network operations. The student is expected to:
- (A) identify basic network addressing and devices, including switches and routers;
 - (B) analyze incoming and outgoing rules for traffic passing through a firewall;
 - (C) identify well known ports by number and service provided, including port 22 (ssh), port 80 (http), and port 443 (https);
 - (D) identify commonly exploited ports and services, including ports 20 and 21 (ftp) and port 23 (telnet); and
 - (E) identify common tools for monitoring ports and network traffic.
- (11) Cybersecurity skills. The student identifies standard practices of system administration. The student is expected to:

- (A) define what constitutes a secure password;
 - (B) create a secure password policy, including length, complexity, account lockout, and rotation;
 - (C) identify methods of password cracking such as brute force and dictionary attacks; and
 - (D) examine and configure security options to allow and restrict access based on user roles.
- (12) Cybersecurity skills. The student demonstrates necessary steps to maintain user access on the computer system. The student is expected to:
- (A) identify the different types of user accounts and groups on an operating system;
 - (B) explain the fundamental concepts and standard practices related to access control, including authentication, authorization, and accounting;
 - (C) compare methods for single- and dual-factor authentication such as passwords, biometrics, personal identification numbers (PINs), and security tokens;
 - (D) define and explain the purpose of an air-gapped computer; and
 - (E) explain how hashes and checksums may be used to validate the integrity of transferred data.
- (13) Cybersecurity skills. The student explores the field of digital forensics. The student is expected to:
- (A) explain the importance of digital forensics to law enforcement, government agencies, and corporations;
 - (B) identify the role of chain of custody in digital forensics;
 - (C) explain the four steps of the forensics process, including collection, examination, analysis, and reporting;
 - (D) identify when a digital forensics investigation is necessary;
 - (E) identify information that can be recovered from digital forensics investigations such as metadata and event logs; and
 - (F) analyze the purpose of event logs and identify suspicious activity.
- (14) Cybersecurity skills. The student explores the operations of cryptography. The student is expected to:
- (A) explain the purpose of cryptography and encrypting data;
 - (B) research historical uses of cryptography; and
 - (C) review simple cryptography methods such as shift cipher and substitution cipher.
- (15) Risk assessment. The student understands information security vulnerabilities, threats, and computer attacks. The student is expected to:
- (A) define and describe vulnerability, payload, exploit, port scanning, and packet sniffing as they relate to hacking;
 - (B) define and describe cyberattacks, including man-in-the-middle, distributed denial of service, and spoofing;
 - (C) explain how computer vulnerabilities leave systems open to cyberattacks;
 - (D) identify threats to systems such as back-door attacks and insider threats;
 - (E) differentiate types of social engineering attacks such as phishing, shoulder surfing, hoaxes, and dumpster diving;
 - (F) explain how users are the most common vehicle for compromising a system at the application level; and

- (G) identify various types of application-specific attacks.
- (16) Risk assessment. The student understands, identifies, and explains the strategies and techniques of both ethical and malicious hackers. The student is expected to:
- (A) identify internal and external threats to computer systems;
- (B) identify the capabilities of vulnerability assessment tools, including open source tools;
and
- (C) explain the concept of penetration testing, tools, and techniques.
- (17) Risk assessment. The student evaluates the risks of wireless networks. The student is expected to:
- (A) compare risks associated with connecting devices to public and private wireless networks;
- (B) explain device vulnerabilities and security solutions on a wireless network;
- (C) compare wireless encryption protocols;
- (D) debate the broadcasting or hiding of a wireless service set identifier (SSID); and
- (E) research and discuss wireless threats such as MAC spoofing and war driving.
- (18) Risk assessment. The student analyzes threats to computer applications. The student is expected to:
- (A) define application security;
- (B) identify methods of application security such as secure development practices;
- (C) discuss methods of online spoofing such as web links in email, instant messaging, social media, and other online communication with malicious links;
- (D) explain the purpose and function of vulnerability scanners;
- (E) explain how coding errors may create system vulnerabilities; and
- (F) analyze the risks of distributing insecure programs.
- (19) Risk assessment. The student understands the implications of sharing information and access with others. The student is expected to:
- (A) describe the impact of granting applications unnecessary permissions;
- (B) describe the risks of granting third parties access to personal and proprietary data on social media and systems; and
- (C) describe the risks involved with accepting Terms of Service (ToS) or End User License Agreements (EULA) without a basic understanding of the terms or agreements.

§126.52. Cybersecurity Capstone (One Credit).

- (a) General requirements. Students shall be awarded one credit for successful completion of this course. This course is recommended for students in Grades 11 and 12. Recommended prerequisite: Foundations of Cybersecurity.
- (b) Introduction.
- (1) Career and technical education instruction provides content aligned with challenging academic standards and relevant technical knowledge and skills for students to further their education and succeed in current or emerging foundations.
- (2) Cybersecurity is an evolving discipline concerned with safeguarding computers, networks, programs, and data from unauthorized access. As a field, it has gained prominence with the emergence of a globally-connected society. As computing has become more sophisticated, so too have the abilities of malicious agents looking to penetrate networks and seize private information.

By evaluating prior incidents, cybersecurity professionals have the ability to craft appropriate responses to minimize disruptions to corporations, governments, and individuals.

- (3) In the Cybersecurity Capstone course, students will develop the knowledge and skills needed to explore advanced concepts related to the ethics, laws, and operations of cybersecurity. Students will examine trends and operations of cyberattacks, threats, and vulnerabilities. Students will develop security policies to mitigate risks. The skills obtained in this course prepare students for additional study toward industry certification. A variety of courses are available to students interested in the cybersecurity field. Cybersecurity Capstone may serve as a culminating course in this field of study.
- (4) Statements that contain the word "including" reference content that must be mastered, while those containing the phrase "such as" are intended as possible illustrative examples.

(c) Knowledge and skills.

- (1) Employability skills. The student demonstrates necessary skills for career development and successful completion of course outcomes. The student is expected to:
 - (A) identify and demonstrate employable work behaviors such as regular attendance, punctuality, maintenance of a professional work environment, and effective written and verbal communication;
 - (B) identify and demonstrate positive personal qualities such as authenticity, resilience, initiative, and a willingness to learn new knowledge and skills;
 - (C) solve problems and think critically;
 - (D) demonstrate leadership skills and function effectively as a team member; and
 - (E) demonstrate an understanding of ethical and legal responsibilities in relation to the field of cybersecurity.
- (2) Employability skills. The student identifies various employment opportunities in the cybersecurity field. The student is expected to:
 - (A) develop a personal career plan along with the education, job skills, and experience necessary to achieve career goals;
 - (B) develop a resume or a portfolio appropriate to a chosen career plan; and
 - (C) illustrate interview skills for successful job placement.
- (3) Ethics and laws. The student evaluates ethical and current legal standards, rights and restrictions governing technology, technology systems, digital media and information technology, and the use of social media in the context of today's society. The student is expected to:
 - (A) analyze and apply to a scenario local, state, national, and international cyber law such as David's Law and Digital Millennium Copyright Act;
 - (B) evaluate historic cases or events regarding cyber; and
 - (C) explore compliance requirements such as Section 508 of the Rehabilitation Act of 1973, Family Educational Rights and Privacy Act of 1974 (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Gramm-Leach-Bliley Act (GLBA).
- (4) Digital citizenship. The student understands and demonstrates the social responsibility of end users regarding significant issues relating to digital technology, safety, digital hygiene, and cyberbullying. The student is expected to:
 - (A) debate the relationship between privacy and security; and
 - (B) identify ethical or unethical behavior when presented with various scenarios related to cyber activities.

- (5) Cybersecurity skills. The student explains the importance and process of penetration testing. The student is expected to:
- (A) define the phases of penetration testing, including plan, discover, attack, and report;
 - (B) develop a plan to gain authorization for penetration testing;
 - (C) identify commonly used vulnerability scanning tools such as port scanning, packet sniffing, and password crackers;
 - (D) develop a list of exploits based on results of scanning tool reports; and
 - (E) prioritize a list of mitigations based on results of scanning tool reports.
- (6) Cybersecurity skills. The student understands common cryptographic methods. The student is expected to:
- (A) evaluate symmetric and asymmetric algorithms such as substitution cipher, Advanced Encryption Standard (AES), Diffie-Hellman, and Rivest-Shamir-Adleman (RSA);
 - (B) explain the purpose of hashing algorithms, including blockchain;
 - (C) explain the function of password salting;
 - (D) explain and create a digital signature; and
 - (E) explain steganography.
- (7) Cybersecurity skills. The student understands the concept of cyber defense. The student is expected to:
- (A) explain the purpose of establishing system baselines;
 - (B) evaluate the role of physical security;
 - (C) evaluate the functions of network security devices such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and intrusion detection prevention systems (IDPS);
 - (D) analyze log files for anomalies; and
 - (E) develop a plan demonstrating the concept of defense in depth.
- (8) Cybersecurity skills. The student demonstrates an understanding of secure network design. The student is expected to:
- (A) explain the benefits of network segmentation, including sandboxes, air gaps, and virtual local area networks (VLAN);
 - (B) investigate the role of software-managed networks, including virtualization;
 - (C) discuss the role of honeypots and honeynets in networks; and
 - (D) create an incoming and outgoing network policy for a firewall.
- (9) Cybersecurity skills. The student integrates principles of digital forensics. The student is expected to:
- (A) identify cyberattacks by their signatures;
 - (B) explain proper data acquisition;
 - (C) examine evidence from devices for suspicious activities; and
 - (D) research current cybercrime cases involving digital forensics.
- (10) Cybersecurity skills. The student explores emerging technology. The student is expected to:
- (A) describe the integration of artificial intelligence and machine learning in cybersecurity;

- (B) investigate impacts made by predictive analytics on cybersecurity; and
 - (C) research other emerging trends such as augmented reality and quantum computing.
- (11) Cybersecurity skills. The student uses various operating system environments. The student is expected to:
 - (A) issue commands via the command line interface (CLI) such as ls, cd, pwd, cp, mv, chmod, ps, sudo, and passwd;
 - (B) describe the file system structure for multiple operating systems;
 - (C) manipulate and edit files within the CLI; and
 - (D) determine network status using the CLI with commands such as ping, ifconfig/ipconfig, traceroute/tracert, and netstat.
- (12) Cybersecurity skills. The student clearly and effectively communicates technical information. The student is expected to:
 - (A) collaborate with others to create a technical report;
 - (B) create, review, and edit a report summarizing technical findings; and
 - (C) present technical information to a non-technical audience.
- (13) Risk assessment. The student analyzes various types of threats, attacks, and vulnerabilities. The student is expected to:
 - (A) differentiate types of attacks, including operating systems, software, hardware, network, physical, social engineering, and cryptographic;
 - (B) explain blended threats such as combinations of software, hardware, network, physical, social engineering, and cryptographic;
 - (C) discuss risk response techniques, including accept, transfer, avoid, and mitigate;
 - (D) develop a plan of preventative measures to address cyberattacks;
 - (E) describe common web vulnerabilities such as cross-site scripting, buffer overflow, injection, spoofing, and denial of service;
 - (F) describe common data destruction and media sanitation practices such as wiping, shredding, and degaussing; and
 - (G) develop an incident response plan for a given scenario or recent attack.
- (14) Risk assessment. The student understands risk management processes and concepts. The student is expected to:
 - (A) describe various access control methods such as mandatory access control (MAC), role-based access control (RBAC), and discretionary access control (DAC);
 - (B) develop and defend a plan for multi-factor access control using components such as biometric verification systems, key cards, tokens, and passwords; and
 - (C) review a disaster recovery plan (DRP) that includes backups, redundancies, system dependencies, and alternate sites.
- (15) Risk assessment. The student investigates the role and effectiveness of environmental controls. The student is expected to:
 - (A) explain commonly used physical security controls, including lock types, fences, barricades, security doors, and mantraps; and
 - (B) describe the role of embedded systems such as fire suppression; heating, ventilation, and air conditioning (HVAC) systems; security alarms; and video monitoring.