The State Board of Education (SBOE) proposes the repeal of §126.36 and new §126.36, concerning Texas Essential Knowledge and Skills (TEKS) for technology applications. The proposed repeal and new section would update the TEKS for the Digital Forensics course and the amount of credit available for the course.

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 science, technology, engineering, and mathematics (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 August 2018, a committee of secondary and postsecondary educators and business and industry representatives was selected to develop recommendations for TEKS for new cybersecurity courses for the required 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 TEKS for the new courses, and in December 2018 draft TEKS for the proposed courses were sent to interested stakeholders to provide feedback. 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 TEKS for the two new courses.

At the January-February 2019 meeting, the SBOE approved for first reading and filing authorization proposed new TEKS for Foundations of Cybersecurity and Cybersecurity Capstone. At that meeting, the SBOE agreed with the cybersecurity TEKS committee's suggestion to make additional recommendations for amendments to the Digital Forensics course. In March 2019, the committee participated in another face-to-face meeting to review and make recommendations for adjustments to the Digital Forensics course.

Proposed new §126.36 would provide updated TEKS for Digital Forensics and award students one credit for successful completion of the course.

The SBOE approved the proposed repeal and new section for first reading and filing authorization at its April 5, 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 would be fiscal implications for state government. For fiscal year 2019, the estimated cost to the Texas Education Agency (TEA) to reimburse the cybersecurity TEKS committee members for travel to review 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 revised TEKS. Any professional development that is created would be based on whether the 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 revised 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 a revised Digital Forensics course that better aligns with the proposed cybersecurity pathway to increase flexibility for students 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 May 3, 2019, and ends June 7, 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/. 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 June 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 May 3, 2019.

STATUTORY AUTHORITY. The repeal is 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; 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 repeal implements Texas Education Code, §§7.102(c)(4); 28.002(a), (c), and (f)(2); and 28.025(a), (c-1)(1), and (c-10).

<rule>

§126.36. Digital Forensics (One-Half to One Credit), Beginning with School Year 2012-2013.

*n

STATUTORY AUTHORITY. The new section is 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; 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 section implements Texas Education Code, §§7.102(c)(4); 28.002(a), (c), and (f)(2); and 28.025(a), (c-1)(1), and (c-10).

<rule>

§126.36. Digital Forensics (One Credit), Beginning with School Year 2019-2020.

(a) General requirements. Students shall be awarded one credit for successful completion of this course. The prerequisite for this course is proficiency in the knowledge and skills relating to Technology Applications, Grades 6-8. This course is recommended for students in Grades 9-12.

(b) Introduction.

(1) Digital forensics is an evolving discipline concerned with analyzing anomalous activity on computers, networks, programs, and data. As a discipline, it has grown with the emergence of a globally-connected digital society. As computing has become more sophisticated, so too have the abilities of malicious agents to access systems and private information. By evaluating prior incidents, digital forensics professionals have the ability to investigate and craft appropriate responses to disruptions to corporations, governments, and individuals. Whereas cybersecurity takes a proactive approach to information assurance to minimize harm, digital forensics takes a reactive approach to incident response.

(2) Digital Forensics introduces students to the knowledge and skills of digital forensics. The course provides a survey of the field of digital forensics and incident response.

(3) 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 identifies necessary skills for career development and employment opportunities. The student is expected to:

(A) investigate the need for digital forensics;

(B) research careers in digital forensics along with the education and job skills required for obtaining a job in both the public and private sector;

(C) identify job and internship opportunities as well as accompanying duties and tasks;

(D) identify and discuss certifications for digital forensics careers;

(E) explain ethical and legal responsibilities in relation to the field of digital forensics;

(F) identify and describe businesses and government agencies that use digital forensics;

(G) identify and describe the kinds of crimes investigated by digital forensics specialists; and

(H) solve problems and think critically.

(2) Employability skills. The student communicates and collaborates effectively. The student is expected to:

(A) apply effective teamwork strategies;

(B) collaborate with a community of peers and professionals;

(C) create, review, and edit a report summarizing technical findings; and

(D) present technical information to a non-technical audience.

(3) Ethics and laws. The student recognizes and analyzes ethical and current legal standards, rights, and restrictions related to digital forensics. The student is expected to:

(A) develop a plan to advocate for ethical and legal behaviors both online and offline among peers, family, community, and employers;

(B) research local, state, national, and international law such as the Electronic Communications Privacy Act of 1986, Title III (Pen Register Act); USA PATRIOT Act of 2001; and Digital Millennium Copyright Act;

(C) research historic cases or events regarding digital forensics or cyber;

(D) examine ethical and legal behavior when presented with confidential or sensitive information in various scenarios related to cyber activities;

(E) analyze case studies of computer incidents;

(F) use the findings of a computer incident investigation to reconstruct the incident;

(G) identify and discuss intellectual property laws, issues, and use;

(H) contrast legal and illegal aspects of information gathering;

(I) contrast ethical and unethical aspects of information gathering;

(J) analyze emerging legal and societal trends affecting digital forensics; and

(K) discuss how technological changes affect applicable laws.

(4) Digital citizenship. The student understands and demonstrates the social responsibility of end users regarding digital technology, safety, digital hygiene, and cyberbullying. The student is expected to:

(A) identify and use digital information responsibly;

(B) use digital tools responsibly;

(C) identify and use valid and reliable sources of information; and

(D) gain informed consent prior to investigating incidents.

(5) Digital forensics skills. The student locates, processes, analyzes, and organizes data. The student is expected to:

(A) identify sources of data;

(B) analyze and report data collected;

(C) maintain data integrity;

(D) examine metadata of a file; and

(E) examine how multiple data sources can be used for digital forensics, including investigating malicious software (malware) and email threats.

(6) Digital forensics skills. The student understands software concepts and operations as they apply to digital forensics. The student is expected to:

(A) compare software applications as they apply to digital forensics;

(B) describe the purpose of various application types such as email, web, file sharing, security applications, and data concealment tools;

(C) identify the different purposes of data formats such as pdf, wav, jpeg, and exe;

(D) describe how application logs and metadata are used for investigations;

(E) describe digital forensics tools;

(F) select the proper software tool based on appropriateness, effectiveness, and efficiency for a given digital forensics scenario; and

(G) describe components of applications such as configurations settings, data, supporting files, and user interface.

(7) Digital forensics skills. The student understands operating systems concepts and functions as they apply to digital forensics. The student is expected to:

(A) compare various operating systems;

(B) describe file attributes, including access and creation times;

(C) describe how operating system logs are used for investigations;

(D) compare and contrast the file systems of various operating systems;

(E) compare various primary and secondary storage devices; and

(F) differentiate between volatile and non-volatile memory.

(8) Digital forensics skills. The student understands networking concepts and operations as they apply to digital forensics. The student is expected to:

(A) examine networks, including Internet Protocol (IP) addressing and subnets;

(B) describe the Open Systems Interconnection (OSI) model;

(C) describe the Transmission Control Protocol/Internet Protocol (TCP/IP) model;

(D) use network forensic analysis tools to examine network traffic data from sources such as firewalls, routers, intrusion detection systems (IDS), and remote access logs; and

(E) identify malicious or suspicious network activities such as mandatory access control (MAC) spoofing and rogue wireless access points.

(9) Digital forensics skills. The student explains the principles of access controls. The student is expected to:

(A) define the principle of least privilege;

(B) describe the impact of granting access and permissions;

(C) identify different access components such as passwords, tokens, key cards, and biometric verification systems;

(D) explain the value of an access log to identify suspicious activity;

(E) describe the risks of granting third parties access to personal and proprietary data on social media and systems;

(F) 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; and

(G) identify various access control methods such as MAC, role-based access control (RBAC), and discretionary access control (DAC).

(10) Incident response. The student follows a methodological approach to prepare for and respond to an incident. The student is expected to:

(A) define the components of the incident response cycle, including preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity;

(B) describe incident response preparation;

(C) discuss incident response detection and analysis;

(D) discuss containment and eradication of and recovery from an incident;

(E) describe post-incident activities such as reflecting on lessons learned, using collected incident data, and retaining evidence of an incident;

(F) develop an incident response plan; and

(G) describe ways a user may compromise the validity of existing evidence.

(11) Incident response. The student objectively analyzes collected data from an incident. The student is expected to:

(A) identify the role of chain of custody in digital forensics;

(B) describe safe data handling procedures;

(C) explain the fundamental concepts of confidentiality, integrity, availability, authentication, and authorization;

(D) identify and report information conflicts or suspicious activity;

(E) identify events of interest and suspicious activity by examining network traffic; and

(F) identify events of interest and suspicious activity by examining event logs.

(12) Incident response. The student analyzes the various ways systems can be compromised. The student is expected to:

(A) analyze the different signatures of cyberattacks; and

(B) identify points of weakness and attack vectors such as online spoofing, phishing, and social engineering.