moved text

(B)~~(C)~~	distinguish between the types of threat actors such as hacktivists, criminals, state-sponsored actors, and foreign governments~~ a cyber attacker and a cyber defender~~;	Group wanted to distinguish between the types of threat actors (industry use) such as hacktivists, criminals, nation state actors, and foreign governments Group suggests threat actor instead of cyber attacker.
(D)	differentiate between industry terminology for types of hackers such as black hats, white hats, and gray hats; and	Group was concerned with language used by industry may end up being revised and wanted to include such as
(E)	determine possible outcomes and legal ramifications of ethical versus malicious hacking practices.~~ ; and~~	
~~(F)~~	~~debate the varying perspectives of ethical versus malicious hacking.~~	Delete and adding wording into (A)
(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;~~	Removed “and counterterrorism” because it is redundant from above.
(D)	explain ~~identify~~ the role of cyber defense ~~defenders~~ in protecting national interests and corporations;	Group increase rigor by explaining and wanted to match with cyber defense instead of defenders.
(E)	explain ~~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 power generation facilities ~~nuclear plants~~.	Remove nuclear plants and use power generation facilities to cover more than one power source.
(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)

(9)~~(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 trojan horses ~~Trojans~~, worms, and viruses;	Correcting the trojan horses language.
(C)	discuss the impact of malware ~~has had on the cybersecurity landscape~~;	Simplified sentence
(D)	explain the role of reverse engineering for the detection of ~~detecting~~ malware and viruses; and	
(E)	describe ~~compare~~ free and commercial antivirus and software. ~~alternatives; and~~	Combined E and F
~~(F)~~	~~compare free and commercial software alternatives.~~	

(10)~~(9)~~

(C)~~(B)~~	analyze incoming and outgoing rules for traffic passing through a firewall;	
(D)~~(C)~~	identify well known ports by number and service provided, including port 22 (ssh), port 80 (http), and port 443 (https);	
(E)~~(D)~~	identify commonly exploited ports and services, including ports 20 and 21 (ftp) and port 23 (telnet); and	
(F)~~(E)~~	identify common tools for monitoring ports and network traffic.	
(12)~~(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.	
(13)~~(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 (AAA);	
(C)	compare methods for single- and multi- ~~dual~~ -factor authentication such as passwords, biometrics, personal identification numbers (PINs), and secure ~~security~~ tokens;	Change: multi-factor instead of dual. Updated language from security tokens to secure tokens
(D)	define and explain the purpose and benefits of an air-gapped computer; and	Students knowing the purpose and the benefits
(E)	explain how hashes and checksums may be used to validate the integrity of transferred data.	
(14)~~(13)~~	Cybersecurity skills. The student explores the field of digital forensics. The student is expected to:	
(A)	explain the importance of digital forensics to organizations, private citizens, and the public sector ~~law enforcement, government agencies~~, ~~and~~ ~~corporations~~;	Added additional language to be more inclusive. Organizations includes corporations and is more encompassing
(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.	

(15)~~(14)~~ Cybersecurity skills. The student explores the operations of cryptography. The student is expected to:

(B)~~(F)~~	explain how users are the most common vehicle for compromising a system at the application level; ~~and~~	This becomes B
(G)	identify various types of application-specific attacks such as cross-site scripting and injection attacks.	Unpatched vulnerabilities
~~(16)~~	~~Vulnerabilities, threats, and attacks Risk assessment. The student understands, identifies, and explains the strategies and techniques of both ethical and malicious hackers. The student is expected to:~~	KS and SEs found in other places
~~(A)~~	~~identify internal and external threats to computer systems;~~	
~~(B)~~	~~identify the capabilities of vulnerability assessment tools, including open source tools; and~~	
~~___~~	~~_____~~	Moved to 7K to fit better with the KS 7
(17)	Vulnerabilities, threats, and attacks ~~Risk assessment~~. The student evaluates the vulnerabilities ~~risks~~ of ~~wireless~~ networks. The student is expected to:	Change risk to vulnerabilities so the KS category matches the content.
(A)	compare vulnerabilities ~~risks~~ associated with connecting devices to public and private ~~wireless~~ networks;	Including all types of networkers
(B)	explain device vulnerabilities and security solutions on ~~a~~ ~~wireless~~ networks such as supply chain security and counterfeit products;	Added further detail to build out the idea of device and the implications therein
(C)	compare and contrast ~~wireless~~ ~~encryption~~ protocols such as HTTP versus HTTPS;	Understanding secure vs non-secure

(D)~~(E)~~ explain how coding errors may create system vulnerabilities

TEKS with edits	Work Group Comments/Rationale

(a)

(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;	

(7)	Cybersecurity skills. The student understands the concept of system ~~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.	CCRS SS: I.F.1;

(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;	CCRS SS: IV.B.3, V.A.1

(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)	demonstrate adherence to local Acceptable Use Policy (AUP) when using digital tools; ~~use digital tools responsibly;~~	Aligns to new technology applications K-8 standards.
(C)	identify and use valid and reliable sources of information; and	
(D)	identify the importance of and need for ~~gain~~ informed consent prior to investigating incidents.	Edited to clarify the language.
(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)		

(A)	analyze ways to identify different threat actors such as ~~the different~~ signatures of cyberattacks; and	Clarified language
(B)	identify points of weakness and attack vectors such as online spoofing, phishing, and social engineering.	