Lesson Plan

LESSON TITLE: **Module 1: Introduction to Cyber Security**

SUMMARY:

Topic Outline

- Cybersecurity and implementation approaches
- Principles of Cyber Security
- CIA Triad and the CNSS security model
- Cybersecurity roles, careers, organizations and certifications

GRADE BAND:

☐ K-2 ☒ 6-8

☐ 3-5 ☒ High School

Time Required: 60 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

- Understand and discuss the 10 Cybersecurity Principles;
- Gain an understanding of the CIA triad and the CNSS security model;
- Acquire a general knowledge of cybersecurity roles and careers.

Materials List:

1. GenCyber Posters and Flash cards

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Describe the Teacher Instruction

We adopt the following best instructional practices and strategies to facilitate learning:

- Multimodal presentation of information
- Cooperative active learning
- Team building
- Periodic checking for understanding

This lesson includes:

☒ Mapping to Cyber Security First Principles
☒ Learning Objectives
☒ Assessments

Mapping to Cyber Security First Principles:

☒ Domain Separation
☒ Abstraction
☒ Process Isolation
☒ Data Hiding
☒ Resource Encapsulation
☒ Layering
☒ Modularity
☒ Simplicity
☒ Least Privilege
☒ Minimization

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Oral Questioning Observation Choose an item. Choose an item. Choose an item.	Online pop-quiz/survey using gosoapbox.com will be utilized to check understanding of key indicators. Key Indicators of Understanding • Basic knowledge of the 10 Cyber Security principles • Recognition of Cyber Security Principle involved • Familiarity with the CIAA triad and the CNSS Security model Hands-on exercises will be conducted to reinforce learning.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

We provide digital videos with closed captions of software tools and hands-on exercises.

Description of Extension Activity(ies):

Background Materials

Cyber Security

According to the Department of Homeland Security's (DHS) National Infrastructure Protection Plan (NIPP) (2013) Vision states, "A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened" (p. 5). The definition of cybersecurity was established in the 2009 NIPP and reaffirmed in 2013:

Cybersecurity is the prevention of damage to, unauthorized use of, or exploitation of, and if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems (p. 30)

President Obama (2013) issued Executive Order 13636: Improving Critical Infrastructure Cybersecurity that calls for a technology-neutral cybersecurity framework. This the design of the framework will (1) reduce cyber risk to critical infrastructure; (2) promote and incentivize the adoption of strong cybersecurity practices; (3) increase the volume, timeliness, and quality of information sharing related to cyber threats; and (4) incorporate protection for privacy and civil liberties into the critical infrastructure security (as cited by the NIPP, 2013, p. 9). Executive Order 13636 and the NIPP closely align with Presidential Policy Directive 8 (PPD-8), National Preparedness.

The National Preparedness Plan includes 5 mission areas "aimed at strengthening the security and resiliency of the United States through systematic preparations that pose the greatest risk to the security of the nation… Prevention, Protection, Mitigation, Response, and Recovery" (PPD-8, National Recovery Framework, 2013, p.1). The White House also issued a Cybersecurity Strategy & Implementation Plan (CSIP) (2015) which listed five implementation approaches, which are: (1) prioritized identification and

protection of high value information and assets, (2) timely detection of and rapid response to cyber incidents, (3) rapid recovery from incidents when they occur and accelerated adoption of lessons learned from the assessment, (4) recruitment and retention of the most highly-qualified members of the cybersecurity workforce your organization can obtain, and (5) efficient and effective acquisition and deployment of existing and emerging technology.

CIA Triad

From the mainframe to present, the CIA Triad, has been the industry standard in computer security and information assurance (Maconachy, Schou, Ragsdale, & Welch, 2001; Whitman & Mattford, 2016) The CIA Triad includes (1) confidentiality, (2) integrity, and (3) availability, which are defined as:

* Confidentiality is "the assurance that information is not disclosed to unauthorized persons, processes, or devices";

* Integrity is "the quality of an information system reflecting logical correctness and reliability of an operating system; the logical completeness of the hardware and software implementing the protection mechanisms' and the consistency of the data structures and occurrence of the stored data";

* Availability is the "timely, reliable access to data and information services for authorized users" (Maconachy, et al., 2001, p. 307-308).

Although confidentiality, integrity, and availability are critical components to computer security, the rapid advancement of technology and threat level has rendered the model as inadequate. The robust model of the C.I.A. Triad now includes key information security concepts such as access, asset, attack, control, safeguard or countermeasure, exploit, exposure, loss, protection profile, risk, subjects and objects, threat, threat agent, and vulnerability (Whitman & Mattford, 2016).

CNSS Security Model

John McCumber developed an image that represented the architecture employed in computer and information security (Maconachy, Schou, Ragsdale, & Welch, 2001; Whitman & Mattford, 2016). The National Training Standard for Information Systems Security Professionals, NSTISSI No. 4011 defines how information security is based within the CNSS Model (Whitman & Mattford, 2016). The CNSS Security Model which is represented through McCumbers Cube is a 3x3x3 cube that creates 27 zones within information security that need to be properly addressed and/or safeguarded, as shown below:

Security Roles, Careers, Professional Organizations and Certifications

With the rapid development and release of new technologies, increasing threats against physical and cyber critical infrastructure, the roles and careers within information technology, information assurance, and cybersecurity are rapidly expanding. Likewise organizations and agencies committed to the professional development of IT and Security professionals are providing certifications and other forums to promote collaboration on this critical topic. This session outlines the current roles, careers, professional organizations and certifications that are available in the industry today.

Associated Hands-on Exercises:

I. Hands-on exercise using the GenCyber Flash cards

With the Flash cards, we will review the 10 Principles and test their knowledge on the hand signals. The participants will break up into teams to discuss and answer the questions from the flash cards. The team that receives the most points will be the winner.

II. Hands-on exercise on the CNSS Model/McCumber Cube

Participants will break up into 3 teams and each team will discuss how to implement a security model for their school based on the CNSS Model/McCumber Cube:
The CIA Triad:
1] Confidentiality
2] Integrity
3] Availability

Information States:
4] Storage
5] Processing
6] Transmission

Measures:
7] Policy
8] Education
9] Technology
Each team will be assigned to protect one of the following: 1) personal information 2) exams and tests 3) e-learning system

Acknowledgements:

- Department of Homeland Security
- White House Press Release and Executive Orders
- National Preparedness Plan
- Maconachy, Schou, Ragsdale, and Welch, 2001
- Whitman and Mattford, 2016