CSE202: Introduction to Cybersecurity for Transportation Agencies

Table of Contents

1. Module Description

The Introduction to Cybersecurity for Transportation Agencies module will provide an overview of key topics relating to cybersecurity for transportation agencies.

2. Introduction/Purpose

The module will first discuss the need for cybersecurity including typical threats that transportation agencies face to their centers, field equipment, and communications. Next, the module will introduce the NIST Cybersecurity Framework which enables organizations to apply the principles and best practices of risk management to improving security and resilience. Then the module will discuss how to apply the Framework to a transportation agency. Finally, the module will look at resources that are available to agencies for sharing information about cybersecurity threats and incidents. Additional resources on cybersecurity for the roadway transportation infrastructure will be identified.

3. Supporting Information

3.1. Critical Infrastructure

The Cybersecurity and Infrastructure Security Agency (CISA) was established November 16th, 2018. It is a standalone United States federal agency, an operational component under Department of Homeland Security (DHS) oversight. Its activities are a continuation of the National Protection and Programs Directorate (NPPD). NPPD's goal was to advance the Department's national security mission by reducing and eliminating threats to U.S. critical physical and cyber infrastructure. Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. CISA has identified 16 critical infrastructures as discussed below.

Chemical Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

Commercial Facilities Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector, which includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging.

Communications Sector

The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. The Department of Homeland Security is the Sector-Specific Agency for the Communications Sector.

Critical Manufacturing Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

Dams Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

Defense Industrial Base Sector

The U.S. Department of Defense is the Sector-Specific Agency for the Defense Industrial Base Sector. The Defense Industrial Base Sector enables research, development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements.

Emergency Services Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector. The sector provides a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response.

Energy Sector

The U.S. energy infrastructure fuels the economy of the 21st century. The Department of Energy is the Sector-Specific Agency for the Energy Sector.

Financial Services Sector

The Department of the Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

Food and Agriculture Sector

The Department of Agriculture and the Department of Health and Human Services are designated as the Co-Sector-Specific Agencies for the Food and Agriculture Sector.

Government Facilities Sector

The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

Healthcare and Public Health Sector

The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Information Technology Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

Nuclear Reactors, Materials, and Waste Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.

Transportation Systems Sector

The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Water and Wastewater Systems Sector

The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

3.2. Transportation Systems Sector

Aviation includes aircraft, air traffic control systems, and about 19,700 airports, heliports, and landing strips. Approximately 500 provide commercial aviation services at civil and joint-use military airports, heliports, and sea plane bases. In addition, the aviation mode includes commercial and recreational aircraft (manned and unmanned) and a wide variety of support services, such as aircraft repair stations, fueling facilities, navigation aids, and flight schools.

Highway and Motor Carrier encompasses more than 4 million miles of roadway, more than 600,000 bridges, and more than 350 tunnels. Vehicles include trucks, including those carrying hazardous materials; other commercial vehicles, including commercial motor coaches and school buses; vehicle and driver licensing systems; traffic management systems; and cyber systems used for operational management.

Maritime Transportation System consists of about 95,000 miles of coastline, 361 ports, more than 25,000 miles of waterways, and intermodal landside connections that allow the various modes of transportation to move people and goods to, from, and on the water.

Mass Transit and Passenger Rail includes terminals, operational systems, and supporting infrastructure for passenger services by transit buses, trolleybuses, monorail, heavy rail—also known as subways or metros—light rail, passenger rail, and vanpool/rideshare. Public transportation and passenger rail operations provided an estimated 10.8 billion passenger trips in 2014.

Pipeline Systems consist of more than 2.5 million miles of pipelines spanning the country and carry nearly all of the nation's natural gas and about 65 percent of hazardous liquids, as well as various chemicals. Above-ground assets, such as compressor stations and pumping stations, are also included.

Freight Rail consists of seven major carriers, hundreds of smaller railroads, over 138,000 miles of active railroad, over 1.33 million freight cars, and approximately 20,000 locomotives. An estimated 12,000 trains operate daily. The Department of Defense has designated 30,000 miles of track and structure as critical to mobilization and resupply of U.S. forces.

Postal and Shipping moves about 720 million letters and packages each day and includes large integrated carriers, regional and local courier services, mail services, mail management firms, and chartered and delivery services.

3.3. Types of Hackers

Black Hat Hackers

- The term “black hat” originated from Western movies, where the bad guys wore black hats and the good guys wore white hats.[1]
- A black-hat hacker is an individual who attempts to gain unauthorized entry into a system or network to exploit them for malicious reasons. The black-hat hacker does not have any permission or authority to compromise their targets. They try to inflict damage by compromising security systems, altering functions of websites and networks, or shutting down systems. They often do so to steal or gain access to passwords, financial information, and other personal data.

White Hat Hackers

- White-hat hackers, on the other hand, are deemed to be the good guys, working with organizations to strengthen the security of a system. A white hat has permission to engage the targets and to compromise them within the prescribed rules of engagement.
- White-hat hackers are often referred to as ethical hackers. This individual specializes in ethical hacking tools, techniques, and methodologies to secure an organization’s information systems.
- Unlike black-hat hackers, ethical hackers exploit security networks and look for backdoors when they are legally permitted to do so. White-hat hackers always disclose every vulnerability they find in the company’s security system so that it can be fixed before they are being exploited by malicious actors.
- Some Fortune 50 companies like Facebook, Microsoft, and Google also use white-hat hackers.

Grey Hat Hackers

- Grey hats exploit networks and computer systems in the way that black hats do, but do so without any malicious intent, disclosing all loopholes and vulnerabilities to law enforcement agencies or intelligence agencies.
- Usually, grey-hat hackers surf the net and hack into computer systems to notify the administrator or the owner that their system/network contains one or more vulnerabilities that must be fixed immediately. Grey hats may also extort the hacked, offering to correct the defect for a nominal fee.

Blue Hat Hacker

- In one word, this is the amateur. Usually, their techniques are deployed out of ill motives such as revenge attacks.

Red Hat Hacker

- The objective of a red hat hacker is to find black hat hackers, intercept and destroy their schemes.

Script Kiddie

- This refers to the newbies. They don't cause excessive damage; they use downloaded hacking software or purchased scripts to bombard traffic sites or simply disrupt the regular activity of a website.

Green Hat Hacker

- This is the set of individuals who simply want to observe and learn about the world of hacking. It comprises those who join learning communities to watch videos and tutorials about hacking.

Social Engineering Hackers

- These are hackers who use psychological manipulation to make people to divulge private contents or to perform certain actions. It is a more complex crime scheme.

Hactivists

- These are the **types of hackers** who break into systems and networks just to draw attention towards an alarming social cause.

Cyber Terrorist:

- These are politically motivated attackers who break into computer systems to stir up violence against non-combatant targets by subnational groups or clandestine agents.

State/Nation Sponsored Hackers:

- These are hackers who are employed by a country to attack the cyber sphere of another nation or international agency as a result of warfare or to retrieve/steal information.

Malicious Insider/Whistle-blower Hacker

- These are the **types of computer hackers** who leak sensitive information from within an organization, especially data under the umbrella of government agencies.

Elite Hackers

- These are individuals who are considered the "cutting-edge geniuses." They are the real experts and the innovators in the field of hacking.

3.4. Sources of Cyber Attacks

- **Bot-network operators** are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.).
- **Criminal groups** seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
- **Foreign intelligence services** use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power; impacts that could affect the daily lives of U.S. citizens across the country.

- **Hackers** break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote hacking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
- **The disgruntled organization insider** is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
- **Individuals, or small groups, who execute phishing schemes** in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
- **Individuals or organizations who distribute unsolicited e-mail** with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
- **Individuals or organizations with malicious intent carry out attacks against users** by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
- **Terrorists** seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

3.5. Types of Attacks and Threats

- **Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks** – DoS is the prevention of authorized access to resources or the delaying of time- critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.). A DDoS is a denial of service technique that uses numerous hosts to perform the attack.
- **Malware attack (including Ransomware)** – Malware is hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.
- Phishing and spear phishing attacks – Phishing is a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. Spearfishing is a colloquial term that can be used to describe any highly targeted phishing attack.

- **Man-in-the-middle (MitM) attack** – An attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.
- **Drive-by attack** – *Drive-by attack (sometimes referred to as drive-by download) means two things, each concerning the unintended download of computer software from the Internet:*
    - *Downloads which a person has authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet) automatically.*
    - *Any download that happens without a person's knowledge, often a computer virus, spyware, malware, or crimeware.*
- **Password attack** – *Password attack, sometimes called password cracking. It is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach (brute-force attack) is to repeatedly try guesses for the password and to check them against an available cryptographic hash of the password.*
- **SQL injection attack** – Attacks that look for websites that pass insufficiently-processed user input to database back-ends
- Cross-site scripting (XSS) attack – A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user-supplied data from requests or forms without sanitizing the data so that it is not executable.
- **Eavesdropping attack** – An attack in which an attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the claimant.
- **Birthday attack** – *A birthday attack is a type of cryptographic attack that exploits the mathematics behind the birthday problem in probability theory. This attack can be used to abuse communication between two or more parties.*

The definitions above are taken from the NIST Cybersecurity Glossary (regular text above) or Wikipedia (italics text above) for those entries not contained in the NIST Glossary.

3.6. NIST Cybersecurity Framework

Learning objectives 2 and 3 focus on information from the NIST Cybersecurity Framework which can be found on the NIST website at:

https://www.nist.gov/cyberframework/framework

The following overview is taken directly from the NIST Cybersecurity Framework document (National Institute of Standards and Technology (NIST) Cybersecurity Framework Version 1.1).

"The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: The Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each

Framework component reinforces the connection between business/mission drivers and cybersecurity activities. These components are explained below.

- *The **Framework Core** is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.*

- ***Framework Implementation Tiers** ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.*

- *A **Framework Profile** ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations. "*

The Framework Core is composed of a set of categories, subcategories and informative references within each of five basic functions. The Appendix provides a table that shows these functions, categories, and subcategories exactly as described in the Framework Document.

The descriptions above are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each subcategory. The references presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process." The following are the informative references from the framework:

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx

- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*: https://www.incibe-cert.es/en/blog/iec62443-evolution-of-isa99
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: https://www.isa.org
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*: https://www.iso.org/standard/54534.html
- NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (including updates as of January 22, 2015). https://doi.org/10.6028/NIST.SP.800-53r4.

4. Reference to Other Standards

- NEMA TS 8-2018: Cyber and Physical Security for Intelligent Transportation Systems (ITS) https://www.nema.org/Standards/view/Cyber-and-Physical-Security-for-Intelligent-Transportation-Systems-ITS

5. Glossary

To include additional descriptions/acronyms used in the module. Definitions of terms are taken from NIST Internal or Interagency Report (NISTIR) 7298 Revision 3: *Glossary of Key Information Security Terms* unless otherwise indicated.

Term	Definition
AASHTO	American Association of State Highway and Transportation Officials
Attack Vector	An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome. www.WhatIs.com
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. [NISTIR 7298 Rev 3]
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber-attacks. [NISTIR 7298 Rev 3]
Cyberspace	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. [NISTIR 7298 Rev 3]
DDOS	Distributed denial-of-service
DE	Detect- one of five NIST Framework functions
DHS	Department of Homeland Security
DOS	Denial-of-service

Term	Definition
DOT	Department of Transportation
EO	Executive Order
FHWA	Federal Highway Administration
ICS-CERT	Industrial Control Systems Cyber Emergency Readiness Team
ID	Identify- one of five NIST Framework functions
IOO	Infrastructure owner/operators
ISAC	Information Sharing and Analysis Center
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation System
JPO	Joint Program Office
MitM	Man-in-the-middle
MS-ISAC	Multi-State ISAC
NCCIC	National Cybersecurity and Communications and Integration Center
NEMA	National Equipment Manufacturer's Association
NFCA	National Fusion Center Association
NIST	National Institute of Standards and Technology
NTCIP	National Transportation Communications for ITS Protocol
PPD	Presidential Policy Directive
PR	Protect - one of five NIST Framework functions
RC	Recover- one of five NIST Framework functions
Resilience	The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning. [NISTIR 7298 Rev 3]
RS	Respond- one of five NIST Framework functions
SLTT	State, local, territorial and tribal
ST-ISAC	Surface Transportation ISAC
USA	United States of America
USDOT	United States Department of Transportation

6. References

- NIST Cybersecurity Framework, Ver. 1.1: Framework for Improving Critical Infrastructure Cybersecurity
- NIST Special Publication 800-63-3: *Digital Identity Guidelines*, June 2017
- ISO/Guide 73:2009: Risk management — Vocabulary
- "National Connected Vehicle Infrastructure Footprint Analysis Final Report v1," American Association of State Highway and Transportation Officials, June 27, 2014
- *Transportation Management Center Information Technology Security*, *Final Report* September 2019 FHWA-HOP-19-059
- *DHS Cybersecurity Resources Road Map, A Guide for Critical Infrastructure*
- *Federal Highway Administration Cybersecurity Program Handbook*, December 2017
- *Cybersecurity and Intelligent Transportation Systems: Best Practice Guide*, FHWA-JPO-19-763: https://www.its.dot.gov/press/2019/its_publications.htm

- The 20 CIS Controls & Resources: Center for Internet Security, DHS, https://www.cisecurity.org/controls/cis-controls-list/
- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
- IEC 62443: Evolution of the ISA 99 https://www.incibe-cert.es/en/blog/iec62443-evolution-of-isa99
- ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems -- Requirements: https://www.iso.org/standard/54534.html
- NIST SP 800-53 Rev. 4 - *NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (including updates as of January 22, 2015). https://doi.org/10.6028/NIST.SP.800-53r4
- "NIST Internal or Interagency Report (NISTIR) 7298 Revision 3: Glossary of Key Information Security Terms." https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/final

7. Study Questions

To include the quiz/poll questions and answer choices as presented in the PowerPoint slide to allow students to either follow along with the recording or refer to the quiz at a later date in the supplement.

1. Which of the following is a true statement?
    a) Modern transportation controllers are less sophisticated than other cyber devices and easier to protect
    b) Cybersecurity is an IT responsibility only
    c) Traffic Ops needs to protect external any cloud-based systems used
    d) Transportation infrastructure could be a target for a state-sponsored cyber attack
2. Which of the following is NOT one of the NIST Functions?
    a) Identify
    b) Defend
    c) Detect
    d) Respond
    e) Recover
3. Which of the following is a correct statement?
    a) A Tier represents the maturity level of the organization
    b) Profiles always represent cybersecurity outcomes currently achieved
    c) Outcomes from using the Framework should reflect in operations
    d) Self-assessment is a one-time step at the beginning of a cyber program
4. Which group cannot be a member of MS-ISAC?
    a) State Transportation Agencies
    b) Municipal Transportation Agencies
    c) ITS Vendors
    d) County Transportation Agencies

Appendix: NIST Functions, Categories, and Subcategories

Function	Category	Subcategory
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried
		ID.AM-2: Software platforms and applications within the organization are inventoried
		ID.AM-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated

Function	Category	Subcategory
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)
	Governance (ID. GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
		ID.GV-4: Governance and risk management processes address cybersecurity risks
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources

Function	Category	Subcategory
		ID.RA-3: Threats, both internal and external, are identified and documented
		ID.RA-4: Potential business impacts and likelihoods are identified
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
		ID.RA-6: Risk responses are identified and prioritized
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
		ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process

Function	Category	Subcategory
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
		PR.AC-2: Physical access to assets is managed and protected
		PR.AC-3: Remote access is managed
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

Function	Category	Subcategory
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained
		PR.AT-2: Privileged users understand their roles and responsibilities
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
		PR.AT-4: Senior executives understand their roles and responsibilities

Function	Category	Subcategory
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected
		PR.DS-2: Data-in-transit is protected
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
		PR.DS-4: Adequate capacity to ensure availability is maintained
		PR.DS-5: Protections against data leaks are implemented
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
		PR.DS-7: The development and testing environment(s) are separate from the production environment

Function	Category	Subcategory
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)
		PR.IP-2: A System Development Life Cycle to manage systems is implemented
		PR.IP-3: Configuration change control processes are in place
		PR.IP-4: Backups of information are conducted, maintained, and tested
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
		PR.IP-6: Data is destroyed according to policy
		PR.IP-7: Protection processes are improved

Function	Category	Subcategory
		PR.IP-8: Effectiveness of protection technologies is shared
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
		PR.IP-10: Response and recovery plans are tested
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
		PR.IP-12: A vulnerability management plan is developed and implemented
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

Function	Category	Subcategory
		PR.PT-2: Removable media is protected and its use restricted according to policy
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
		PR.PT-4: Communications and control networks are protected
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected, and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed
		DE.AE-2: Detected events are analyzed to understand attack targets and methods
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors
		DE.AE-4: Impact of events is determined

Function	Category	Subcategory
		DE.AE-5: Incident alert thresholds are established
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
		DE.CM-4: Malicious code is detected
		DE.CM-5: Unauthorized mobile code is detected
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
		DE.CM-8: Vulnerability scans are performed

Function	Category	Subcategory
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability
		DE.DP-2: Detection activities comply with all applicable requirements
		DE.DP-3: Detection processes are tested
		DE.DP-4: Event detection information is communicated
		DE.DP-5: Detection processes are continuously improved
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed
		RS.CO-2: Incidents are reported consistent with established criteria

Function	Category	Subcategory
		RS.CO-3: Information is shared consistent with response plans
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated
		RS.AN-2: The impact of the incident is understood
		RS.AN-3: Forensics are performed
		RS.AN-4: Incidents are categorized consistent with response plans
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers)

Function	Category	Subcategory
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained
		RS.MI-2: Incidents are mitigated
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned
		RS.IM-2: Response strategies are updated
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned
		RC.IM-2: Recovery strategies are updated
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed
		RC.CO-2: Reputation is repaired after an incident
		RC.CO-3: Recovery activities are communicated to internal and external

Function	Category	Subcategory
		stakeholders as well as executive and management teams

8. Icon Guide

The following icons are used throughout the module to visually indicate the corresponding learning concept listed out below, and/or to highlight a specific point in the training material.

1) **Background information:** General knowledge that is available elsewhere and is outside the module being presented. This will be used primarily in the beginning of slide set when reviewing information readers are expected to already know.

2) **Tools/Applications:** An industry-specific item a person would use to accomplish a specific task and applying that tool to fit your need.

3) **Remember:** Used when referencing something already discussed in the module that is necessary to recount.

4) **Refer to Student Supplement:** Items or information that are further explained/detailed in the Student Supplement.

5) **Example:** Can be real-world (case study), hypothetical, a sample of a table, etc.

6) **Checklist:** Use to indicate a process that is being laid out sequentially.