MODULE 7: CYBERSECURITY

Day: 3 **Time:** 2.0 Hours **Level of Understanding:** Comprehension

Instructional Strategies:
- Lecture
- Large-Group Discussion

Module Equipment/Facilities:
- Standard Classroom Setup

Participant Materials/Handouts:
- Workbook 7.1: Evaluating Cybersecurity
- Terrorist Tactics and Trends Handbook

Terminal Learning Objective

By the end of this module, you will be able to explain cyberthreats to your organization.

Introduction

Cyberspace and its underlying infrastructure are vulnerable to a wide variety of risks from both physical hazards and cyberthreats. Terrorists and criminals are moving traditional crimes to cyberspace by exploiting vulnerabilities to steal information and money. They are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. Of growing concern is the cyberthreat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, the risk increases for wide scale or high-consequence events that could cause harm or disrupt services. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace remains an important mission.

This module will provide you with a brief overview of cybersecurity, strategies to use to protect against cyberthreats, and information about cybersecurity policies and procedures.

Module Topics

An outline of key topics and an approximate time plan are shown below.

Topic	Enabling Learning Objectives	Approximate Time
Module Introduction	▪ Not Applicable	5 minutes
Cybersecurity Overview	▪ Define cybersecurity.	25 minutes
Protecting against Cyberthreats	▪ Describe how cybersecurity is used to respond to ongoing cyberthreats.	50 minutes
Cybersecurity Policies and Procedures	▪ Explain cybersecurity policies and procedures.	30 minutes

Topic	Enabling Learning Objectives	Approximate Time
Module Summary	▪ Not Applicable	10 minutes

The module times are guidelines only. The actual time required may vary based on the experience level and interest of the participants or other factors encountered during the training session.

Key Terms

Key Term	Description
Application whitelisting	A proactive security technique where only a limited set of approved programs are allowed to run, while all other programs (including most malicious software) are blocked from running by default; enables only the administrators, not the users, to decide which programs are allowed to run
Critical infrastructure	The systems and assets, whether physical or virtual, so vital to a nation that the incapacity or destruction of such systems and assets would have a debilitating effect on security, national economic security, national public health or safety, or any combination of those matters
Cross-border infrastructure	Any critical services such as banking or telecommunications that are located in another country or have a crucial dependency on information systems outside of a given country's jurisdiction
Cyberattack	An intrusion into electronic and digital information systems, by way of cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information
Cyberinfrastructure	Electronic or digital information and communication systems and databases, and the information contained in these systems; organizational intranets, shared networks, and the Internet are all part of cyberinfrastructure
Cybersecurity	Preventing damage to, unauthorized use of, or exploitation of electronic information and communication systems and databases and the information contained therein to ensure confidentiality, integrity, and availability; and restoring electronic information and communications systems in the event of a terrorist attack or natural disaster

Key Term	Description
Cybersecurity engineer	A personnel role in the information technology department that aids in cybersecurity by determining who requires access to which information; plans, coordinates, and implements information security programs; and helps protect against Internet threats that facilitate cybercrime
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
Cyberinterdependency	The compatibility and commonality of computer operating systems, networks, and databases across many systems
Cyberthreat	Any circumstance or event with the potential to adversely affect an information system by way of unauthorized access, destruction, disclosure, modification of information, or denial of service
Firewall	A network security system designed to provide protection against outside attackers by shielding your computer or network from malicious or unnecessary network traffic and preventing malicious software from accessing the network
Hacker	A person who seeks to gain unauthorized access to the computer data of another person or organization
Information system	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information
Information system-related security risks	Those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider the effect on the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the nation
Information technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by a law enforcement agency — this includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources

Key Term	Description
Insider threat	An authorized user of a computer system who attacks the system after logging in, exceeds their computer privileges, or violates organizational security policy or laws; may be a dissatisfied employee or a contractor with system access
Intrusion detection	The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents
Intrusion detection and prevention	The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents
Intrusion detection and prevention system	Software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents
Intrusion detection system	Software that automates the intrusion detection process; may or may not be detectible to the intruder
Intrusion prevention	*See* intrusion detection and prevention
Intrusion prevention system	*See* intrusion detection and prevention system
Network	A group of electronic components that share information or interact with each other in order to perform a function

Topic: Module Introduction — 5 Minutes

Slide 1 Cybersecurity

- Title Slide

Graphic Description: US Flag and Seal

Module Preparation

- **Timing and Methods:** Use the suggested time plan at the beginning of the module. As with all modules in this course, read all the content (Facilitator Guide and PowerPoint slides) and familiarize yourself with each facilitator note before class.
- Be thoroughly prepared for exercises, discussions, or other activities required for the module. Follow all facilitator notes. Use a combination of lecture, large-group discussion, small-group activities, and TeachBack moments.
- Check the link on Slide 19 to test connectivity in the classroom prior to presenting the module.
  - If link and navigation work, show participants what is described in facilitator notes.
  - If link does not work, describe the elements of the website listed in the facilitator notes and write the link on flip-chart paper and post in the classroom.

Orientation to Participant Guide

- When beginning this module:
  - Refer participants to the beginning of this module in the Participant Guide.
  - Note the list of addendums participants will use during this module.
  - Review the key terms before beginning the module.

Slide 2 Module Objective

- By the end of this module, you will be able to explain cyberthreats to your organization

Graphic Description: No Graphic

- Briefly discuss the terminal learning objective.
- Highlight the key topics to be presented:
  - Cybersecurity Overview
  - Protecting against Cyberthreats
  - Cybersecurity Policies and Procedures
- Tell the participants that the information in this module can be used to explain the types of measures an agency should have in place and policies, processes, and procedures that should be developed to reduce cyberthreats in their agencies.

Topic: Cybersecurity Overview	**25 Minutes**

Enabling Learning Objective:
- Define cybersecurity.

Slide 3 Cybersecurity Overview — Important Definitions

- **Information system**
- **Cyberspace**
- **Cyberinfrastructure**
- **Cyberthreat**
- **Cyberattack**
- **Cybersecurity**

Graphic Description: Two men looking at a computer

- Tell participants that it is important to review and have a common understanding of these important cyber-related definitions before continuing in the module.
- Define the following terms:
  - **Information system:** a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information
  - **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
  - **Cyberinfrastructure:** electronic or digital information and communication systems and databases, and the information contained in these systems; organizational intranets, shared networks, and the Internet are all part of cyberinfrastructure
  - **Cyberthreat:** any circumstance or event with the potential to adversely affect an information system by way of unauthorized access, destruction, disclosure, modification of information, or denial of service
  - **Cyberattack:** an intrusion into electronic and digital information systems, by way of cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information
  - **Cybersecurity:** preventing damage to, unauthorized use of, or exploitation of electronic information and communication systems and databases and the information contained therein to ensure confidentiality, integrity, and availability; and restoring electronic information and communications systems in the event of a terrorist attack or natural disaster

Slide 4 Discussion Question
▪ What types of critical infrastructure in your nation require cybersecurity?
Graphic Description: No Graphic

- Remind participants of the definition of **critical infrastructure** discussed in *Module 2: Introduction to Critical Infrastructure Security and Resilience***:** the systems and assets, whether physical or virtual, so vital to a nation that the incapacity or destruction of such systems and assets would have a debilitating effect on security, national economic security, national public health or safety, or any combination of those matters.
- Ask participants the following discussion question: **What types of critical infrastructure in your nation require cybersecurity?**
- Acknowledge responses and write on flip-chart paper to post in classroom. *If not provided by participants, add the following:*
  - *Examples of critical infrastructure that require cybersecurity include all types of critical infrastructure, such as:*
    - *Agriculture*
    - *Food*
    - *Water*
    - *Public health facilities*
    - *Emergency services*
    - *Government*
    - *Defense industrial base*
    - *Information and telecommunications*
    - *Energy*
    - *Transportation*
    - *Banking and finance*
    - *Chemical industry*
    - *Postal and shipping*

Slide 5 Cybersecurity Trends (1 of 3)
▪ Repeated cyberattacks on critical infrastructure ▪ Cyberthreat to critical infrastructure continues to grow ▪ Cyberinterdependency
Graphic Description: No Graphic

Slide 6 Cybersecurity Trends (2 of 3)
▪ **Insider threats** to computer systems ▪ Foreign ownership of infrastructure ▪ Serious national security challenges for a nation to confront
Graphic Description: No Graphic

- Explain that repeated and continuing cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity.
- Define **cyberinterdependency:** the compatibility and commonality of computer operating systems, networks, and databases across many systems
- Explain that interdependency makes computer networks and systems vulnerable to cyberattacks because of the interconnected and interdependent nature of these systems.
  - Attacks capable of spreading quickly with a debilitating effect
  - Increase vulnerability through the connectivity of Internet
  - Decrease control over technology shared by way of cyberspace in global economy
- Define **insider threat:** an authorized user of a computer system who attacks the system after logging in, exceeds their computer privileges, or violates organizational security policy or laws; may be a dissatisfied employee or a contractor with system access.
- Explain that the threats to computer systems from insiders — current or former employees or contractors in an organization — may account for up to one third of security breaches in computer systems.
  - Insiders pose a security threat because of their knowledge about or access to organizational computer systems and databases.
  - The exact percentage of attacks is unknown due to under reporting of these crimes because of insufficient information to prosecute or concern about negative publicity for the organization.
  - Examples include employees who have:
    - Not received expected promotions
    - Not received credit for achievements or developments that aided the organization
    - Been terminated from the organization
  - Terrorist organizations target such individuals to help gain access to critical infrastructure computer systems and databases.
- Explain that ownership of critical infrastructure by entities outside of a nation can be a threat because of not only a direct physical or cyberattack or the interdependency of the computer systems, but because the owner may simply stop the functioning of the site for malicious reasons.
- Tell participants that the cyberthreat to critical infrastructure and to all computer systems continues to grow and represents one of the most serious national security challenges any nation must confront. The national and economic security of a nation depends on the reliable functioning of the nation's critical infrastructure and the computers that run it despite such threats.

Slide 7 Cybersecurity Trends (3 of 3)

- Goals to address trends:
  - Enhance security and resilience of a nation’s critical infrastructure
  - Maintain an efficient cyberenvironment that promotes safety and privacy
  - Partner with infrastructure owners and operators to improve information sharing

Graphic Description: Man in a café using a laptop computer

- Explain that these cybersecurity goals help address the trends:
  - Enhance the security and resilience of the nation's critical infrastructure
  - Maintain a cyberenvironment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties
  - Partner with the owners and operators of critical infrastructure to:
    - Improve cybersecurity information sharing
    - Collaborate to develop and implement risk-based standards

Slide 8 Discussion Question
▪ If any of your critical infrastructure experienced a successful cyberattack and stopped operations, what would be the consequences for your nation?
Graphic Description: No Graphic

- Ask participants the following discussion question: **If any of your critical infrastructure experienced a successful cyberattack and stopped operations, what would be the consequences for your nation?**
- Acknowledge responses. *Responses will vary.*
- Refer to the posted list of participants' critical infrastructure discussed earlier.

Topic: Protecting against Cyberthreats	**50 Minutes**

Enabling Learning Objective:
- Describe how cybersecurity is used to respond to ongoing cyberthreats.

Slide 9 Protecting against Cyberthreats (1 of 2)
▪ Using **information technology** ▪ Checking backgrounds of all personnel and contractors ▪ Involving the entire agency — senior leadership, mid-level leaders, front-line officers, and analysts
Graphic Description: No Graphic

- Define **information technology:** any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by a law enforcement agency — this includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

- Explain how the use of background checks may help alert organizations to unsuitable or potentially dangerous personnel:
  - For applicants for employment or contract work
  - On a rotating system for all current employees to indicate any changes from time of hire
- Explain that protecting an organization's critical and cyberinfrastructure involves the whole agency:
  - Senior leadership provides an agency's strategic vision, goals, and objectives for information technology
  - Mid-level leaders planning and managing for security and risk management
  - Front-line officers and analysts who operate the information systems

Slide 10 Protecting against Cyberthreats (2 of 2)
▪ Building community partnerships ▪ Determining critical and cyberinfrastructure ▪ Decentralizing critical and cyberinfrastructure ▪ Incorporating technology to protect technology
Graphic Description: A community of people

- Explain that partnering with the private sector includes:
  - Building trust and communication because no single organization can address the response and resilience needs resulting from a terrorist attack or natural disaster
  - Sharing information, ideas, protocols, and procedures about cybersecurity best practices and solutions
  - Planning security and resource allocation in the event of attacks or natural disasters
  - Encouraging public awareness
  - Developing a unified system between government, industry, and the private sector to increase awareness of threats to a nation's critical infrastructure
- Remind participants of the list of critical infrastructure introduced in the last topic and the definition of cyberinfrastructure in the list of module terms.
- Explain that deciding and prioritizing what infrastructure is critical will assist in planning both budgets and planning for protection and resilience.
- Explain that because areas of control for most critical infrastructure are in one place — centralized — an attack or natural disaster at that one location will have a cascading effect at other sites.
- Explain that decentralizing critical and cyberinfrastructure can become one form of security because an attack at one site will not force the entire system to shut down.
- Explain that technology already plays a role in the physical protection of critical infrastructure, including access point identification verification systems and camera and motion sensor monitoring of spaces and perimeters — technology must also be used to protect itself.
- Tell participants you will discuss examples of cyberinfrastructure protection technology next.

Slide 11 Intrusion Detection and Prevention (1 of 2)
▪ The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents
Graphic Description: No Graphic

Slide 12 Intrusion Detection and Prevention (2 of 2)
▪ Advantages: • Monitors traffic and alerts on what is unusual about an aspect of the traffic • Alerts on a computer signature that is listed in a database of threats ▪ Disadvantages: • Provides information about a suspected intrusion after it has occurred • Contains information that becomes outdated quickly • Tends to generate a greater number of false alarms than real attacks — resulting in real attacks being missed or ignored
Graphic Description: No Graphic

- Tell participants that it is no longer a matter of **if** an intrusion into their computer systems will take place, but **when** an intrusion will take place.
- Define:
  - **Intrusion detection:** the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents
  - **Intrusion detection system:** software that automates the intrusion detection process; may or may not be detectible to the intruder
  - **Intrusion detection and prevention:** the process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents
  - **Intrusion detection and prevention system:** software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents
- Explain the advantages and disadvantages of an intrusion detection system:
  - Monitors traffic and alerts on what is unusual about an aspect of the traffic
  - Alerts on a computer signature that is listed in a database of threats
  - Provides information about a suspected intrusion after it has occurred
  - Contains information that becomes outdated quickly
  - Tends to generate a greater number of false alarms than real attacks — resulting in real attacks being missed or ignored
- Tell participants that agencies and organizations should consider:
  - Using multiple types of intrusion detection and prevention technology and systems to achieve more comprehensive and accurate detection and prevention of malicious activity
  - Separating (segregating or containing) systems into sections to stop hostile intruders from expanding their access if they break into one system and limiting possible damage

- Tell participants that more information about these actions will be covered later in this module.

Slide 13 Intrusion Detection and Resilience
▪ Preventing an intrusion avoids the need to rebuild systems and reconstruct data ▪ Separating systems makes incident cleanup significantly less costly ▪ Maintaining a resiliency plan of response ▪ Executing prepared responses quickly ▪ Broadcasting advance public awareness in case of total shutdown response
Graphic Description: No Graphic

- Explain the connections between intrusion detection and prevention and resilience:
  - Using intrusion detection and prevention systems can help prevent terrorist and other criminal activity, thus avoiding the need to rebuild systems and reconstruct data after an intrusion
  - Separating each of the systems and the servers and networks that host the systems makes incident cleanup significantly less costly
  - Maintaining and training network defense teams to execute a resilience response plan to a detected intrusion may help ensure that all teams are prepared to respond
  - Executing well-planned responses will enable network defense teams quickly and effectively counter and expel a hostile intrusion
  - Providing the public with general information in advance about intrusion responses before any intrusions happen may enable community cooperation in the event of a cyber intrusion when a total shutdown of critical infrastructure may be necessary

Slide 14 Firewall (1 of 3)
▪ A network security system designed to provide protection against outside attackers by shielding your computer or network from malicious or unnecessary network traffic and preventing malicious software from accessing the network
Graphic Description: No Graphic

- Explain that firewalls are necessary prevention method to block data from certain locations or applications while allowing relevant and necessary data through.
- Define **firewall:** a network security system designed to provide protection against outside attackers by shielding your computer or network from malicious or unnecessary network traffic and preventing malicious software from accessing the network.

Slide 15 Firewall (2 of 3)
▪ Characteristics: • May be hardware or software type • Must be properly configured for desired level of security • Limits traffic between networks

Graphic Description: A series of digital locks, one of them unlocked

Slide 16 Firewall (3 of 3)

- Stops intrusive traffic from entering
- Does not protect against installed malicious programs
- Does not signal an intrusion
- Use with anti-virus software and safe computing practices

Graphic Description: No Graphic

- Explain the characteristics of a firewall:
  - May be an external device between the Internet or a network connection and your computer or a multiple-computer system or it may be a built-in feature of your computer's operating system — your software firewall should always be enabled for added protection even if you have a hardware firewall
  - Commercially available firewalls are pre-configured, but the user must determine whether the default settings on your firewall are sufficient to protect your critical infrastructure system — the configurations may need strengthening
  - Limits outside access between networks to prevent intrusions
  - Monitors outwardly for intrusion traffic to stop the traffic from entering your system
  - Does not protect against malicious programs that enter your system along with other software or against malicious software you accidently install on your computer
  - Does not signal or alert system operators of an intrusion from inside the network
  - Use with anti-virus software and safe computing practices to strengthen resistance to intrusions and cyberattacks

Slide 17 Response — Cybersecurity Engineer

- A personnel role in the information technology department that aids in cybersecurity by determining who requires access to which information; plans, coordinates, and implements information security programs; and helps protect against Internet threats that facilitate cybercrime

Graphic Description: Hands typing on a computer keyboard

- Explain that an intrusion detection and prevention system should have a cybersecurity engineer.
- Define **cybersecurity engineer:** a personnel role in the information technology department that aids in cybersecurity by determining who requires access to which information; plans, coordinates, and implements information security programs; and helps protect against Internet threats that facilitate cybercrime.

Slide 18 Cybercrime Sources

- Primary sources of critical infrastructure cybercrime:
  - National governments
  - Terrorists
  - Industrial spies and organized crime groups

Graphic Description: A world map with digital computer code language over it

- Explain that some of the primary sources of critical infrastructure cybercrime may be:
  - **National governments:**
    - Threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption
    - Only nation states appear to have the discipline, commitment, tradecraft, and resources to fully develop capabilities to attack critical infrastructure
  - **Terrorists:**
    - Less developed in computer network capabilities and propensity to pursue cyber-type means than are other types of hostile intruders — likely to pose only a limited cyberthreat
    - Bombs more effective at this point, so terrorists are likely to stay focused on tradition attack methods in near term
    - Anticipate more substantial cyberthreats as a future possibility because a more technically competent generation is entering the terrorist ranks
  - **Industrial spies and organized crime groups:**
    - Pose a medium- to large-level threat to critical infrastructure due to the ability to conduct industrial espionage and large-scale monetary theft as well as the ability to hire or develop **hacker** talent; a **hacker** is a person who seeks to gain unauthorized access to the computer data of another person or organization.
    - Primary goals are profit based
    - Secondary goals include theft of trade secrets and gaining access to information on critical infrastructure individuals for purposes of blackmail to use potential public exposure as a threat

Slide 19 Stop.Think.Connect

- Public awareness campaign to increase the understanding of cyberthreats and empower the public to be safer and more secure online
- Website includes tips and tools, videos, blog, and promotional materials
- More information at www.dhs.gov/about-stopthinkconnect

Graphic Description: A world map with digital computer code language over it

- Check the link again to test connectivity prior to presenting the slide.
  - If link and navigation work, show participants what is described in facilitator notes.
  - If link does not work, describe the elements of the website listed in the facilitator notes and write the link on flip-chart paper and post in the classroom.

- Explain the importance of creating public awareness for cyberthreats using the Department of Homeland Security's Stop.Think.Connect Campaign as an example.
  - The Stop.Think.Connect. Campaign is a national public awareness effort in the US that increases the understanding of cyberthreats and empowers the public to be safer and more secure online.
    - More and more people are using new technologies and spending more time online.
    - Our growing dependence on technology, coupled with the increasing threat of cyberattacks, demands greater security in our online world.
    - This presents the need for simple, easy-to-understand resources and tips to help ensure their safety and security.
    - The campaign provides access to these types of resources to give the public the tools they need to make more informed decisions when using the Internet.
  - It encourages the public to view Internet safety as a shared responsibility–at home, in the workplace, and in our communities.
  - The campaign provides access to these types of resources to give the public the tools they need to make more informed decisions when using the Internet.
  - It is a unique public-private partnership, implemented in coordination with the National Cyber Security Alliance.
  - The campaign goals are to:
    - Elevate the nation's awareness of cybersecurity and its association with national security and the safety of our personal lives.
    - Engage the public, the private sector, and state and local governments in our nation's effort to improve cybersecurity.
    - Communicate approaches and strategies for the public to keep themselves, their families and their communities safer online
  - Stop.Think.Connect has a website that provides tips and tools for being safe online, a blog, videos, and promotional materials to use at work and in the community.
  - More information can be found at: https://www.dhs.gov/about-stopthinkconnect.
- Ask participants if they have a similar program in their country. If not, ask them how they might be able to implement this type of program.

Slide 20 Evaluating Cybersecurity for Resilience (1 of 3) (Workbook 7.1)

- Does the agency or organization:
  - Use a security technique that limits what programs can run at one time?
  - Ensure that all program downloads and upgrades come from verified sources?
  - Isolate networks from any untrusted networks, especially the Internet?

Graphic Description: No Graphic

Slide 21 Evaluating Cybersecurity for Resilience (2 of 3) (Workbook 7.1)

- Separate its computer system into distinct parts?
- Have a strict policy for issuing and authenticating access credentials to the system?
- Control remote access with strong credentials and time limits?

Graphic Description: No Graphic

Slide 22 Evaluating Cybersecurity for Resilience (3 of 3) (Addendum 7.1)

- Monitor the system continuously and respond immediately to intrusion incidents?
- Ongoing and evolving challenge
- Resilience is part of our defense

Graphic Description: No Graphic

- Explain that cyber intrusions into critical infrastructure systems are happening with increased frequency.
- Refer participants to **Workbook 7.1: Evaluating Cybersecurity.**
- Discuss each of the questions on the slide using the addendum to the level of detail the facilitators think is appropriate for the experience of participants.
- Explain that defense against the modern threat requires applying measures to protect not only the perimeter of the critical infrastructure but also the interior — and it is an ongoing and evolving challenge.
- Explain that as a part of a proactive defense, a clearly defined cybersecurity framework will provide the necessary resilience to ensure that an organization's information systems continue to operate in an environment protected from a terrorist or other criminal's malicious attempts to gain access.

Slide 23 Large-Group Discussion: Insider Threats

- The most predominant threats that exist to an agency are **insider threats**
- What cybersecurity issues could involve an insider?
- What do you think are some of the personal motivations of an insider?
- What could an agency or organization do to reduce the possibility of insider threats?

Graphic Description: No Graphic

- Tell participants that now they have a greater understanding of how to protect against cyberthreats, you will now discuss how to do this for the growing trend of insider threats.
- Explain that although the majority of this module so far has focused on external hostile intruder activity, the insider threat is one of the most predominant threats that exist to an agency or organization.
- Ask participants the following discussion question: **What cybersecurity issues could involve an insider?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Unauthorized use of a government computer or device*
  - *Sharing user credentials, login identifications, and passwords or multiple users on one account*
  - *Accessing prohibited websites*
  - *Theft or loss of government property*
  - *Unauthorized release of or access to proprietary information*
  - *Unauthorized release of or access to sensitive or classified information*

  - *Downloading, storing, or transmitting classified information to unauthorized software, hardware, or system*
  - *Introduction of hardware, software, or media without authorization*
  - *E-mail traffic with attachments or large file transfers to nongovernment or nonmilitary addresses*
- Ask participants the following discussion question: **What do you think are some of the personal motivations of an insider?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Greed or financial need: a belief that money can fix anything, excessive debt or overwhelming expenses make the employee vulnerable to approach by terrorists or organized crime organizations*
  - *Anger or revenge: dissatisfaction to the point of wanting to retaliate against the organization*
  - *Problems at work: a lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, a pending layoff*
  - *Ideology or identification: a desire to help a struggling or particular cause*
  - *Divided loyalty: allegiance to another person or company, or to a country besides the nation in which the agency or organization is located*
  - *Adventure or thrill: want to add excitement to their life, intrigued by the clandestine activity, a desire to be an aspiring espionage agent*
  - *Vulnerability to blackmail: does not want to risk the exposure of extra-marital affairs, gambling, or fraud*
  - *Ego or self-image: an attitude that the rules do not apply to him or her, a desire to repair wounded self-esteem, vulnerability to flattery or the promise of a better job; may be combined with anger, revenge, adventure, or thrill*
  - *Seeking favor: a desire to please or win the approval of someone who could benefit from insider information with the expectation of returned favors or monetary gain*
  - *Addictive or destructive behaviors: alcohol or drug addiction or other addictive or self-harmful behaviors that increase vulnerability to approach by terrorists or organized crime organizations*
  - *Family problems: marital conflicts or separation from loved ones that increases vulnerability to approach by terrorists or organized crime organizations*
- Ask participants the following discussion question: **What could an agency or organization do to reduce the possibility of insider threats?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Conduct thorough background investigations on all employees and network users at hire and at random intervals during employment or contract, especially those individuals with the greatest access to the information system and related cybersecurity protocols.*
  - *Provide continuous monitoring of network systems to ensure users do not request or gain inappropriate access.*
  - *Provide on-going cybersecurity training to employees to discuss the ways to not become an unintentional insider and the associated penalties of the intentional insider.*

Topic: Cybersecurity Policies and Procedures — 30 Minutes

Enabling Learning Objective:
- Explain cybersecurity policies and procedures.

Slide 24 Cybersecurity Policies and Procedures (1 of 3)

- Specific to cybersecurity of agency information systems
- Protocols to select and work with community partners
- Collaboration with community partners to write policies and procedures
- Limitations of information sharing

Graphic Description: No Graphic

- Explain that agencies should develop cybersecurity policies and procedures using the following guidelines:
  - Ensure that the policies and procedures specifically address the security controls that will specifically apply to the information system in your agency
  - Include protocols that address how to select community partners and also how your agency will work together with those partners during crisis or natural disaster events
  - Collaborate with your community partners in the process of writing your policies and procedures to ensure that all other organizations agree, understand requirements, and have approval rights to the documents that will also become part of their organization's policies and procedures
  - Determine the extent and limits of information sharing that will take place with other agencies, organizations, or community partners; legal guidelines that should be in place for every organization to follow should include policies, processes, and procedures for:
    - Notifying and reporting of incident occurrences
    - Monitoring to detect incidents
    - Implementing security measures to prevent and detect incidents
    - Maintaining security documentation to keep security measures updated

Slide 25 Cybersecurity Policies and Procedures (2 of 3)

- Policies to address three elements of resilience planning:
  - Robustness
  - Resourcefulness
  - Rapid recovery

Graphic Description: Security guard standing outside looking at a city skyline

- Address the three elements of resilience planning in your cybersecurity policies and procedures for both internal and external partners:
  - **Robustness:** the ability to maintain critical operations and functions in the face of crisis

- **Resourcefulness:** the ability to skillfully prepare for, respond to, and manage a crisis or disruption as it unfolds
- **Rapid recovery:** the ability to return to or reconstitute normal operations as quickly and efficiently as possible after a disruption

Slide 26 Cybersecurity Policies and Procedures (3 of 3)

- Policies and procedures for incident reporting:
  - Internal incidents
  - **Cross-border infrastructure** incidents
  - Reporting points-of-contact
  - Personnel training

Graphic Description: A cybercriminal stealing information from a computer

- Explain that policies and procedures must be in place for reporting incidents of system intrusion.
  - Internal incidents
  - Cross-border infrastructure incidents:
    - Define **cross-border infrastructure:** critical services such as banking or telecommunications that are located in another country or have a crucial dependency on information systems outside of a given country's jurisdiction
    - These dependencies create additional vulnerabilities and are a potential source of instability even in countries that have strong internal cybersecurity measures in place
  - Points-of-contact information for incident reporting
  - Policies that establish personnel training about reporting procedures

Slide 27 Discussion Questions

- What cybersecurity reporting requirements are already in place in your agency or nation?
- What cybersecurity reporting requirements would you consider adding?

Graphic Description: No Graphic

- Ask participants the following discussion questions:
  - **What cybersecurity reporting requirements are already in place in your agency or nation?**
  - **What cybersecurity reporting requirements would you consider adding?**
- Acknowledge responses. *Responses will vary.*

Slide 28 ATA Terrorist Tactics and Trends Handbook

- Definition
- Growing threats and weapons
- Terrorist tactics and trends
- Terrorist use of the Internet
- Terrorist publications
- References to stay informed

Graphic Description: A laptop view screen displaying a person pointing a weapon

- Refer participants to **ATA Terrorist Tactics and Trends Handbook**.
- Briefly refer to the elements of terrorism as presented in the handbook:
  - Definition: premeditated, politically motivated violence against noncombatant targets (pages 2 and 3)
  - Growing threats and weapons: MANPADS, cyberthreats, weapons (page 4)
  - Terrorist tactics and trends: bombing is most common, lone-wolf attacks (page 5)
  - Terrorist use of the Internet: information technology and social media (page 6)
  - Terrorist publications (page 6)
  - References to stay informed (page 7)
- Encourage participants to read the entire handbook during their study time this week.

Slide 29 TeachBack Moment

- What is the definition of cybersecurity?
- How is cybersecurity used to respond to ongoing cyberthreats?
- What are examples of cybersecurity policies and procedures?

Graphic Description: No Graphic

- Conduct a TeachBack moment to assess how well the participants understand the content presented in this module.
- Ask participants: **What is the definition of cybersecurity?**
- Acknowledge responses. *If not provided by participants, add the following: cybersecurity is preventing damage to, unauthorized use of, or exploitation of electronic information and communication systems and databases and the information contained therein to ensure confidentiality, integrity, and availability; and restoring electronic information and communications systems in the event of a terrorist attack or natural disaster.*
- Ask participants: **How is cybersecurity used to respond to ongoing cyberthreats?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Using information technology*
  - *Checking backgrounds of all personnel and contractors*
  - *Involving the entire agency*
  - *Building community partnerships*
  - *Determining critical and cyberinfrastructure*
  - *Decentralizing critical and cyberinfrastructure*
  - *Incorporating technology to protect technology*
  - *Using intrusion detection and prevention system*

  - *Firewalls*
- Ask participants: **What are examples of cybersecurity policies and procedures?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Policies to address resilience planning*
  - *Policies and procedures for incident reporting*
- Ask participants whether they have any questions about anything covered thus far.

Topic: Module Summary	**10 Minutes**

Slide 30 Module Summary
▪ Cybersecurity overview ▪ Protecting against cyberthreats ▪ Cybersecurity policies and procedures
Graphic Description: No Graphic

- Summarize the module by reviewing the following points:
  - **Cybersecurity overview:**
    - Information system
    - Cyberspace
    - Cyberinfrastructure
    - Cyberthreat
    - Cyberattack
    - Cybersecurity
  - **Protecting against cyberthreats:**
    - Using information technology
    - Checking backgrounds of all personnel and contractors
    - Involving the entire agency
    - Building community partnerships
    - Determining critical and cyberinfrastructure
    - Decentralizing critical and cyberinfrastructure
    - Incorporating technology to protect technology
    - Using intrusion detection and prevention system
    - Firewalls
    - Cybercrime sources
    - Stop.Think.Connect campaign
    - Evaluating cybersecurity for resilience
  - **Cybersecurity policies and procedures:**
    - Policies to address resilience planning
    - Policies and procedures for incident reporting
  - Ask whether there are any questions about the contents of this module.
- Explain that *Module 8: Surveillance Awareness: What You Can Do* will explain the actions necessary to detect and report suspicious activities associated with hostile surveillance.