Instructor Guide

FDIC Workplace Security

CU.
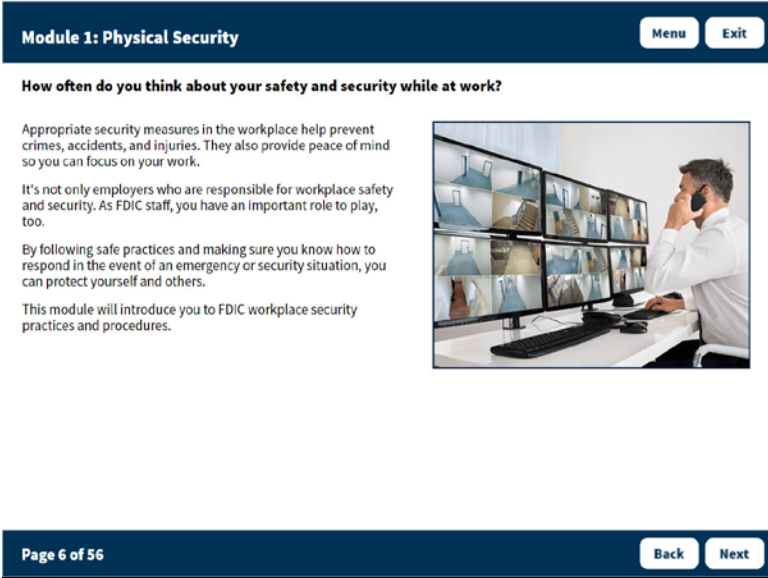
FDIC Workplace Security

	Instructor
Slide 1	
Slide 2	

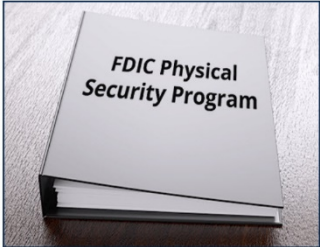| Instructor	
Slide 3	**Introduction** Menu Exit **Program Office** The Security and Emergency Preparedness Section (SEPS) is part of the Division of Administration and is responsible for the following areas: • Physical Security • Emergency Preparedness • Personnel Security • Continuity of Operations (COOP) • Transportation The goal of SEPS is to provide a safe and secure work environment for all FDIC employees, contractors, and visitors. SEPS staff work with regional Corporate Services Branch (CSB) personnel to ensure safety and security measures are in place for regional and field office personnel. **SEPS** Security and Emergency Preparedness Section **Visit the SEPS Intranet Page** Page 3 of 56 Back Next
Slide 4	**Introduction** Menu Exit **Overview** This Workplace Security Training consists of two modules. **Module 1: Physical Security** We will discuss physical security, which is defined as "the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution." This includes protection from fire, flood, natural disasters, burglary, theft, violence, vandalism and terrorism. **Module 2: Emergency Preparedness** The emergency preparedness module will introduce you to emergency preparedness practices you can follow to ensure you are prepared and know how to appropriately respond during an emergency. This module provides resources available to FDIC employees to ensure you receive information prior to and during a building emergency. Page 4 of 56 Back Next

	Instructor
Slide 5	
Slide 6	

	Instructor
Slide 7	**Module 1: Physical Security** Menu Exit **Objectives** In this physical security module, you'll learn the following. • Identify the components of physical security. • Recognize potential risks to physical security. • Describe measures for reducing physical security risks. • Determine the actions to take in response to a security situation. Page 7 of 56 Back Next
Slide 8	**Module 1: Physical Security** Menu Exit **Security Begins with You** We live in a world of ever-increasing risk. Risks threaten worker safety, employee morale, and FDIC operations. Some threats are intentional acts, such as sabotage and violence. Others are caused by natural disasters or man-made accidents. No matter the threat, all employees have a responsibility to help the FDIC protect its personnel, information, data, and facilities. Employees are often the target of these threats as well as the organization's first line of defense against them. As an employee, you are an integral part of your organization's security solution. Security is a shared responsibility, and it begins with you! Page 8 of 56 Back Next

	Instructor
Slide 9	**Module 1: Physical Security** Menu Exit **FDIC Physical Security Overview** FDIC is comprised of various types of facilities including HQ's buildings, Regional offices, Area offices, and Field offices secured through Access Control, Intrusion detection systems, and CCTV as well as other protective measures. Depending on the security rating level for your specific FDIC office, you may experience varying levels of security protocols when visiting other FDIC locations across the United States. The security level for a facility is determined by the following: **RISK = ASSET x THREAT x VULNERABILITY** **Instructions: Select each circle to view descriptions.** THREAT ASSET RISK VULNERABILITY Page 9 of 56 Back Next
	Asset People, property, and information. People may include employees and customers along with other invited persons such as contractors or guests. Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records, and many other intangible items. An asset is what we're trying to protect. **Close**

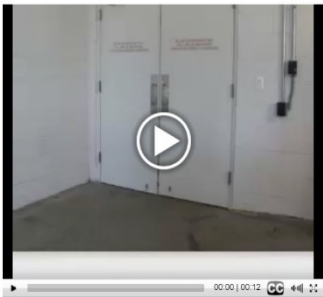| Instructor |
| --- |
| **Threat**

Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. A threat is what we're trying to protect against.

Close |
| **Vulnerability**

Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. A vulnerability is a weakness or gap in our protection efforts.

Close |

Instructor	
	Risk The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability. Risk is the intersection of assets, threats, and vulnerabilities. **Close**
Slide 10	**Module 1: Physical Security** Menu Exit **Reducing Physical Security Risks** Employees are expected to comply with FDIC Circular 1610.01, FDIC Physical Security Program. This describes procedures for: • Gaining entry - Washington, DC and Virginia Square office employees can view the garage entry video on the SEPS website • Securing work area • Information on how to respond to emergencies ALL employees must be vigilant for anything unusual at their workplace that could threaten security. When observing a situation that may threaten security, you should: • Report the incident • Never confront the situation by yourself *FDIC Physical Security Program* Page 10 of 56 Back Next

Instructor	
Slide 11	
Slide 12	

Instructor	
Slide 13	**Module 1: Physical Security** Menu Exit **Access Control Procedures – ID Badges 1** Sample Building Badge vs. HSPD-12 PIV Cards SEPS's Badge and Fingerprinting Information FDIC employees and most contractors are issued personal identity verification (PIV) badges for FDIC network and facility access. FDIC short-term contractors and others who do not receive PIV badges are issued a proximity badge that provides physical access only. FDIC facilities have Physical Access Control Systems (PACS) that grant access to individuals based on their function at the workplace. PACS consist of card readers, panels, and other devices capable of electronically verifying an individual's identity and managing access rights. Page 13 of 56 Back Next
Slide 14	**Module 1: Physical Security** Menu Exit **Access Control Procedures – ID Badges 2** • Wear your badge on the outermost garment at all times while in the workplace. • Never allow individuals without appropriate identification into areas where card or key access is required. • Never allow "piggybacking" or "tailgating"—letting an individual follow you through secure access doors. • Never lend or borrow badges with employees, contractors, or visitors. • Report a lost badge to the appropriate security personnel immediately. • Conceal your badge when not at work to protect against compromise. **FDIC Security Points of Contact** Page 14 of 56 Back Next
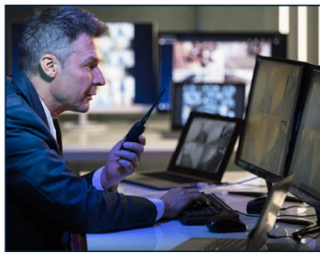
Instructor	
Slide 15	**Module 1: Physical Security** Menu Exit **Access Control Procedures – Visitors** Visitors should wear a visitor's badge and be escorted at all times. To learn more please refer to the following information. **SEPS Security Policies for Your Location** **SEPS's Electronic Visitor Management System (EVMS)** Page 15 of 56 Back Next
Slide 16	**Module 1: Physical Security** Menu Exit **Access Control – Visitor Video Scenario 1** It's just past lunchtime, and Kathy is returning to work. On her way in through the employee-only entrance, Kathy spots someone who has his hands full. Kathy is a helpful person, and she's always very courteous. Observe Kathy's actions. **Press the Play button to watch the video.** ▶ 00:00	00:17 CC ◀◀ ⛶ Page 16 of 56 Back Next
	Transcript *Excuse me.* *Can you hold that door?* Wow, looks like you have your hands full. *Yeah, all the dollies were checked out.* [Holds door] *Thanks, you're a life saver.* Glad to help.

Instructor	
Slide 17	**Module 1: Physical Security** Menu Exit **Access Control – Visitor Video Scenario 2** The person is not using his own pass and is attempting to get Kathy to let him in (to "piggyback"). She should apologize but pass through the secure employee-only door alone. **Press the Play button to watch the video.** Page 17 of 56 Back Next
	Transcript *Excuse me.* *Can you hold that door?* I'm sorry. I can't let you in. [Door closes]

Slide 18	**Module 1: Physical Security** Menu Exit
	
	Access Control – Approaching Unknown Individuals
	
	If you approach an unknown individual:
	• Maintain a safe distance of at least three steps (10 feet) between yourself and the person you intend to speak with.
	• Be persistent in your questioning (if appropriate).
	• Do not be easily dismissed. The unknown person may give you a brief explanation and just keep on going. (For example: "Sir, may I help you?" "No thanks, I'm fine.")
	• Use open-ended questions when addressing an unknown person:
	  ➢ "Who are you here to see?"
	  ➢ "What department are you visiting?"
	  ➢ "Are you lost, may I be of assistance?"
	• Notify security or your supervisor.
	• If possible, enlist the assistance of a coworker to notify security or your supervisor and assist in keeping an eye on the person of interest.
	• If the individual becomes threatening, abusive or violent, back off and wait for security and/or your supervisor to arrive.
	
	FDIC Security Points of Contact
	
	Page 18 of 56 Back Next

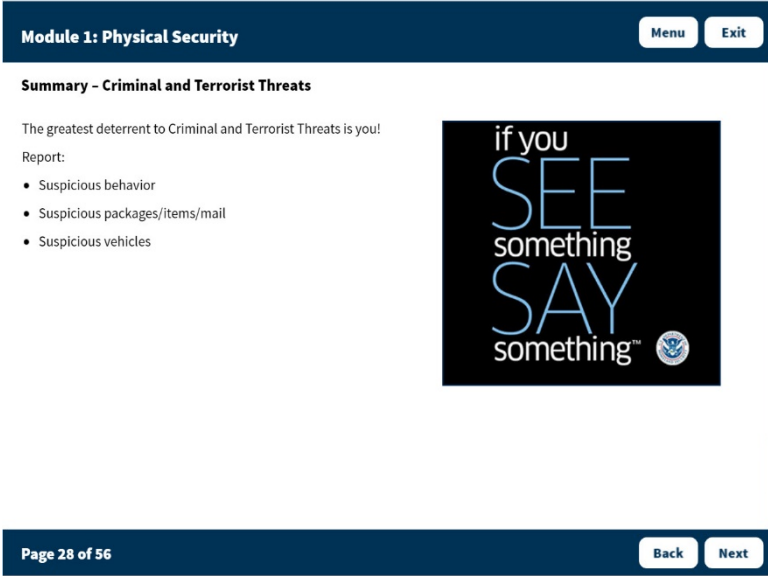| Instructor	
Slide 19	**Module 1: Physical Security** Menu Exit **Knowledge Check 1** Review the scenario and select the best course of action. Then select Submit. You decide to take a quick break from your work and go talk to a coworker next door. After a few minutes, you need to use the restroom. You realize you do not have your badge. When you return to your desk to retrieve it, it's not there. That's strange—you thought you left it on your desk. What should you do? ○ Borrow your coworker's badge to get into the restroom. ○ Ask around the office to find the person who took your badge. ○ Follow someone else who is heading to the restroom. ○ Report the missing badge to the appropriate security personnel. **Submit** Page 19 of 56 Back Next
	Knowledge Check Feedback Correct! You should report the missing badge to the appropriate security personnel. *When you are ready to proceed, select the Next button.* **Close**

	Instructor
Slide 20	**Module 1: Physical Security** Menu Exit **Knowledge Check 2** Review the scenario and select the best course of action. Then select Submit. You are rushing to deliver a report to your manager, who has an important meeting and needs the data from your report immediately. As you hurry down the hall, you see someone carrying boxes. As you pass him, he offers a smile and a quick nod. He does not appear to be wearing a badge, nor does he have an escort, as all visitors are required to. What should you do? ○ Continue to your manager's office; the report is due! ○ Report what you saw to the appropriate supervisor or security personnel. ○ Block the man and demand to see his badge. ○ Don't worry about it; he is probably a courier with a delivery. **Submit** Page 20 of 56 Back Next
	Knowledge Check Feedback Incorrect. You need to take the time to report the situation rather than proceeding or ignoring it. Because the individual did not have a badge in clear view and did not have an escort, you should report this matter to the appropriate supervisor or security personnel immediately. *When you are ready to proceed, select the Next button.* **Close**

Instructor	
Slide 21	**Module 1: Physical Security** [Menu] [Exit] **Summary – Access Control Procedures** • You are responsible for your badge. • Do not share or lend your badge. • Present your PIV card on entrance and exit from buildings and garages as warranted. • Do not let people "piggyback" through secure office doors or parking garage doors. • It is okay to approach people who do not have their badge and ask if you can be of assistance. • If you don't want to do this notify security or your supervisor. • Consider your safety and the safety of your co-workers comes first. **Resources:** FDIC Security Points of Contact Garage Barrier Safety Video Page 21 of 56 [Back] [Next]
Slide 22	**Module 1: Physical Security** [Menu] [Exit] **Criminal and Terrorist Threats Overview** The next threats relate to potential criminal and terrorist activities. **Access & Security Control Threats** **Criminal & Terrorist Threats** **Workplace Violence Threats** Page 22 of 56 [Back] [Next]

Instructor

| Slide 23 | |
| Slide 24 | |

Slide 23

Module 1: Physical Security   Menu   Exit

Criminal or Terrorist Threats

Be alert for people who behave suspiciously or engage in unusual actions. These could indicate behaviors of criminal or terrorist activity. Make sure that you:

- Promptly alert your security personnel, management, and appropriate authorities when you see suspicious behavior or items.
- Report something if it looks or feels wrong. Security is everyone's responsibility.

Page 23 of 56   Back   Next

Slide 24

Module 1: Physical Security   Menu   Exit

Suspicious Behaviors and Observations

Be alert for:

- Nervous or evasive behavior
- Individuals loitering, taking notes, pictures or videos of the facility
- Suspicious packages or items (for example fumes, odors, or liquids coming form a package)
- Disassembled electrical components
- Plans, drawings, schematics, or maps
- Breach in perimeter security (for example, broken window or open door)
- Suspicious vehicles
  - Abandoned or idle vehicles
  - Circling vehicles (for example taxi circling numerous times)

Page 24 of 56   Back   Next

Instructor	
Slide 25	**Module 1: Physical Security** Menu Exit **How to Respond to Suspicious Behaviors and Observations** What to do: • Report observations to security personnel or an appropriate supervisor immediately. • Observe and, if possible, record suspicious vehicle's license plate number and description. • Do not take any other action except observe and report. **FDIC Security Points of Contact** Page 25 of 56 Back Next
Slide 26	**Module 1: Physical Security** Menu Exit **Bomb Threat Procedures** If you receive a bomb threat call or mail, take it seriously and use the following procedures: • Keep calm. • Keep the caller on the line. • Record every word. • Obtain information. • Pay attention to background noises and the caller's voice. • Notify your FDIC Security contact immediately. • Do not destroy written threats or envelopes in which they are received unless directed to do so by your management or security procedures. • Keep a copy of the "Bomb Threat Call Procedures" Checklist at your desk at all times. **FDIC's Emergency Action Guidance** Page 26 of 56 Back Next

Instructor

FDIC's Emergency Action Guidance

Bomb Threat Procedures

If you receive a bomb threat call, take it seriously and note the following information:

1. Time call received
2. Time call ended
3. Number call received at
4. Exact wording of the threat
5. Sex of caller
6. Accent of caller
7. Age of caller

Questions to Ask:

1. When is the bomb going to explode?
2. Where is it right now?
3. What does it look like?
4. What kind of bomb is it?
5. What will cause it to explode?
6. Did you place the bomb?
7. Why?
8. What is your name?
9. What is your address?
10. What is your location and/or number? (Check caller ID)

Close

Slide 27

Module 1: Physical Security   Menu   Exit

Suspicious Mail or Package

Immediately notify FDIC Security Personnel if you observe a suspicious package or item.

Do not go near the package, and do not attempt to open or inspect the package.

Immediately notify FDIC Security Personnel if you receive:

- Threatening letters.
- Letters or packages with:
  - ➤ Suspicious contents (white powder, photos of the workplace)
  - ➤ Oil or grease spots, an inaccurate address, or excessive postage or packaging.

Never handle, open or approach a suspicious letter or package.

Click on the button to learn more.

FDIC Guidance on Handling Suspicious Mail or Packages

Page 27 of 56   Back   Next
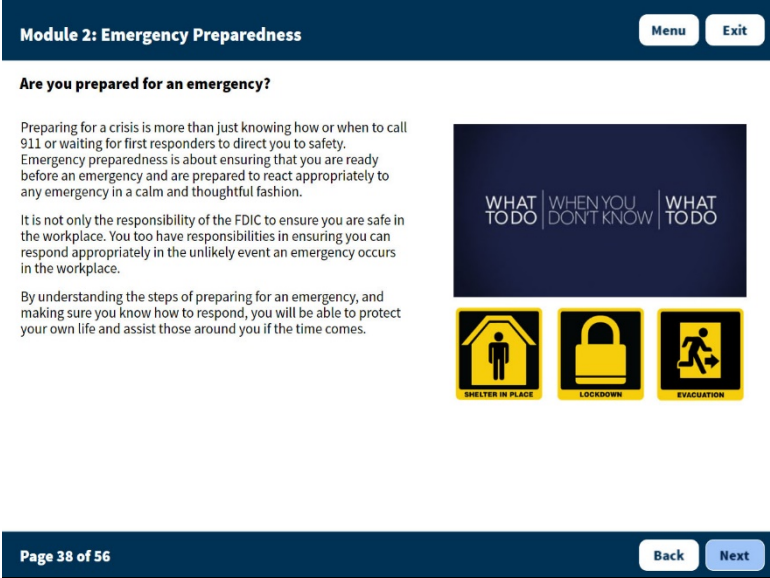
Instructor

FDIC Guidance on Handling Suspicious Mail or Packages

If you open a letter containing a suspicious substance, immediately wash your hands with soap and water.

Notify your FDIC Security contact immediately. Your security officer may isolate the damaged or suspicious piece of mail or package and cordon off the immediate area. As soon as practical, take a shower with soap and water.

Sources: U.S. Postal Inspection Service Guide to Mail Center Security and DHS Best Practices for Safe Mail Handling.

Close

Slide 28

Module 1: Physical Security   Menu   Exit

Summary – Criminal and Terrorist Threats

The greatest deterrent to Criminal and Terrorist Threats is you!

Report:

- Suspicious behavior
- Suspicious packages/items/mail
- Suspicious vehicles

if you SEE something SAY something™

Page 28 of 56   Back   Next

	Instructor
Slide 29	**Module 1: Physical Security**　　　　　　　　Menu　Exit **Workplace Violence Threats Overview** In this section of the course, we'll cover workplace violence threats. Access & Security Control Threats Criminal & Terrorist Threats Workplace Violence Threats Page 29 of 56　　　　　　　　　　　　　　Back　Next
Slide 30	**Module 1: Physical Security**　　　　　　　　Menu　Exit **Workplace Violence** Incidents of violence in the workplace, including domestic violence, have caused federal agencies to assess their vulnerabilities and risk factors and implement workplace violence awareness. The FDIC does not tolerate violent behaviors and takes reports of such behaviors seriously. Workplace Violence can be: • Carried out by current or former employees • Noticed by intuitive managers or coworkers Refer to the FDIC Circular 1600.2, Workplace Violence Prevention Policy, for additional information. Page 30 of 56　　　　　　　　　　　　　　Back　Next

	Instructor
Slide 31	**Module 1: Physical Security** Menu Exit **Indicators of Workplace Violence** Potentially violent employees typically do not just "snap," but display behavioral indicators over longer periods of time. If these behaviors are recognized, they can often be managed and treated. Indicators of potentially violent behavior may include: • Depression or withdrawal • Repeated violations of organizational policies • Explosive outbursts of anger or rage without provocation • Behavior that might indicate paranoia (Everybody is against me.) • Escalation of domestic problems into the workplace • Talk of severe financial problems • Talk of previous incidents of violence The Management Response Teams (MRT) was created to assist in these areas as part of the FDIC Security in the Workplace Program. Page 31 of 56 Back Next
Slide 32	**Module 1: Physical Security** Menu Exit **Hostile Insiders** You probably don't think often about a fellow co-worker hurting other employees or about armed belligerents invading the building. Such hostile physical actions can result from an insider threat. See what actions to take in physical security situations by watching the Department of Homeland Security (DHS) Active Shooter video. Information on how personnel should react in the event of an active shooter can be found in your facility's Occupant Emergency Plan (OEP). Occupant Emergency Plans can be found on Regional Office websites and the Headquarters OEP can be found on the SEPS webpage. Additional information on responding during an active shooter event will be discussed in Module 2. **Visit SEPS Intranet Page** Page 32 of 56 Back Next

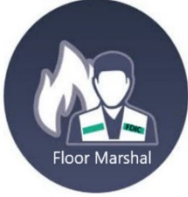| Instructor |
|---|

| Slide 33 | |
| Slide 34 | |

Slide 33

Module 1: Physical Security   Menu   Exit

Summary – Workplace Violence Threats

- Workplace violence refers to any harmful act or acts against an employee that create a hostile work environment and negatively affect the employee, either physically or psychologically.
- The FDIC's workplace violence policy states that violence will not be tolerated, including harassment, verbal abuse, and physical aggression.
- There is no profile of workplace violence that is limited to gender, type of act, or work location.
- People who commit workplace violence typically progress from anger resulting from recurring stress to loss of control when the issue continues unresolved.
- The Management Response Team (MRT) can help supervisors ensure that the workplace violence prevention program is properly implemented and supported.

Page 33 of 56   Back   Next

Slide 34

Module 1: Physical Security   Menu   Exit

Security Is Everyone's Business

You can contribute to your workplace security by:
- Identifying threats and vulnerabilities that affect workplace security
- Avoiding complacency
- Observing with all your senses
- Being aware of unusual changes in your surroundings
- Noticing unusual or suspicious behavior
- Knowing whom to call if something is not right
- Getting assistance. **Do NOT try to "handle it" yourself**
- Remember, security is everyone's job. Take it seriously

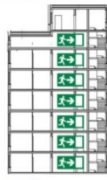Page 34 of 56   Back   Next

Instructor	
Slide 35	**Module 1: Physical Security** Menu Exit **Situational Awareness** To avoid being targeted by adversaries, remain aware of your surroundings. For example: • Remove your security badge after leaving your controlled area or office building. • Don't talk about work outside your workspace unless you are in a specifically designated meeting environment. • Even inside a closed work environment, be careful when discussing classified or sensitive information, such as Personal Identifying Information (PII) or Sensitive Information (SI), as people without a need-to-know may be present. • Be aware of people eavesdropping when retrieving messages from smartphones or other media. **PAY ATTENTION** Page 35 of 56 Back Next
Slide 36	**Module 1: Physical Security** Menu Exit **If You See Something, Say Something** The Department of Homeland Security has launched the "If You See Something, Say Something™" campaign as part of the national Suspicious Activity Reporting initiative. The campaign emphasizes that everyone should: • Be vigilant • Take notice of your surroundings • Report suspicious items or activities to local authorities immediately Click the link below for more information about how to report suspicious activity. **FDIC Security Points of Contact** if you SEE something SAY something* Page 36 of 56 Back Next

	Instructor
Slide 37	
Slide 38	

	Instructor
Slide 39	**Module 2: Emergency Preparedness** Menu Exit **Objectives** Upon completion of this Emergency Preparedness module, you should be able to do the following. • Describe emergency preparedness procedures. • Respond appropriately to specific emergency events. • Know how to appropriately request additional assistance in advance of an emergency event. • Ensure you are receiving Corporation-wide emergency notifications as well as local notifications for your specific area. Page 39 of 56 Back Next
Slide 40	**Module 2: Emergency Preparedness** Menu Exit **What is an Emergency?** Emergencies can happen anytime and anywhere without warning. It is important to be prepared for any type of emergency and know how to appropriately react and respond when an emergency occurs. Before getting into how to prepare, let's first define what an emergency is. An emergency is a serious, unexpected, and often dangerous situation requiring immediate action. **For this module, an emergency is defined as an event that disrupts the day-to-day operations of the FDIC and its employees and contractor staff.** Nobody knows when an emergency or disaster will affect them personally. Plain and simple, emergencies and disasters can strike anytime and anywhere, and may affect more than just your workplace. Page 40 of 56 Back Next

	Instructor
Slide 41	**Module 2: Emergency Preparedness** Menu Exit **Do You Know What To Do in an Emergency?** An important safety measure is knowing what to do if something goes wrong. Listed below are the topics we will be cover. Being Prepared Responding During an Emergency Requesting Assistance Staying Informed Page 41 of 56 Back Next
Slide 42	**Module 2: Emergency Preparedness** Menu Exit **Being Prepared: Occupant Emergency Plans** To ensure the safety of FDIC personnel, Occupant Emergency Plans (OEPs) and procedures have been developed for HQ and Regional Offices to provide information that will assist Federal employees, contractors, and visitors (also referred to as occupants) in the event of a building emergency. Simplified emergency procedures are also posted and available in FDIC Field Offices. It is important to learn the established emergency procedures for your building and your work area by reviewing the building-specific occupant emergency plans and procedures for your office location. Before an emergency occurs, make sure you: • Know the location of at least two exits (including emergency exits) and two shelter-in-place locations in your area. • Practice how to get to these exits and shelter-in-place locations from your office to ensure you know the best route to take. • Know where the fire alarm pull stations or glass break fire alarms are located closest to you. **Plans, procedures, and other preparedness information can be found on the SEPS web page for Headquarters employees and the respective regional offices web pages for regional office-specific plans. Links to these web pages can be found in the Downloadable PDF of Course Links at the end of the course.** Page 42 of 56 Back Next

	Instructor
Slide 43	**Module 2: Emergency Preparedness** Menu Exit **Being Prepared: What am I supposed to do in an Emergency?** The FDIC has established Occupant Emergency Teams (OETs) for HQ and Regional Offices to plan for and lead the response to a building emergency. OETs are led by DOA staff, to include Corporate Services Branch (CSB), SEPS and facilities personnel, and are supported by Federal employee volunteers who serve as Floor Marshals (also referred to as Fire Wardens or Fire Marshals in some regions) to assist occupants in the event of a building emergency. During an emergency, the OET will coordinate with first responders and communicate response activities to the Floor Marshals. All building occupants are to follow the direction of the OET, Floor Marshals, and Security Officers to ensure appropriate response to an emergency event. When an emergency occurs, the safety of building occupants is most important. Depending on the nature of the emergency, occupants may need to evacuate or shelter-in-place, or a lockdown of the building may be necessary. *Floor Marshal* Page 43 of 56 Back Next
Slide 44	**Module 2: Emergency Preparedness** Menu Exit **Responding During an Emergency Situation: Evacuation 1** A wide variety of emergencies, both man-made and natural, may require a building to be evacuated. An evacuation is implemented under conditions when it is no longer safe for building occupants to remain in a building or a specific area of a building. A building evacuation requires occupants to quickly leave the building and move at least 100 feet away or to a designated assembly point (refer to your specific building Occupant Emergency Plan for specific information). Building evacuation is most commonly implemented when the fire alarm is activated indicating a possible fire inside the building. Depending on the procedures in place for your building and the capabilities of the fire alarm or Public Address (PA) system, when the alarm sounds you may be advised via the OET, Floor Marshals, fire alarm, smoke detector, or PA System of a full or partial (also referred to as *zone*, *zoned*, or sometimes *staged*) building evacuation. **EVACUATION** Page 44 of 56 Back Next

	Instructor
Slide 45	**Module 2: Emergency Preparedness** [Menu] [Exit] **Responding During an Emergency Situation: Evacuation 2** **Full Building Evacuation** **Partial or Zoned Building Evacuation** **General Evacuation Response Actions** • Follow building-specific evacuation procedures for full or partial building evacuation. When instructed, evacuate immediately - do not wait. Use the closest exit and leave without delay. • Lock your computer and take your ID badge with you. • Take your coat and personal belongings, such as a purse, bag, keys, ONLY if they are readily available. Do not return to your office to retrieve these items if they are not nearby. • Follow direction of the OET, Floor Marshals, and Security Officers. • When exiting, do not congregate immediately outside of the doors, and move at least 100 feet or to a designated assembly point away from the building. **Click on the images to learn more.** **Page 45 of 56** [Back] [Next]
	Full Building Evacuation As the name implies, all building occupants, on all floors, immediately evacuate the building upon notification from the fire/alarm system, OET, Floor Marshals or PA System. [Close]

Instructor
Partial or Zoned Evacuation Only personnel on the floor where the fire/alarm system is activated and the floors immediately above and below are evacuated from the building. Evacuation instructions will be conveyed via the alarm and PA Systems. **Close**

| Slide 46 | **Module 2: Emergency Preparedness**   Menu   Exit

Responding During an Emergency Situation: Shelter-in-Place

In certain emergency situations, such as a severe weather event, you may be instructed to shelter-in-place.

The purpose of sheltering in place is to keep people safe while indoors; however, it does not mean stay where you are. When instructed via the Public Address (PA) System, promptly move to a designated Shelter-in-Place location. Warn others in the area and advise them to move to shelter-in-place.

Shelter-in-Place Response Actions

• Shelter in Place locations are typically interior rooms without windows. Once there, close the door and lock the door, if appropriate.

• Do not exit the room until the emergency has passed and you are instructed to do so via the Public Address (PA) system, Floor Marshals, or first responders.

SHELTER IN PLACE

Page 46 of 56   Back   Next |

Instructor	
Slide 47	**Module 2: Emergency Preparedness** Menu Exit **Responding During an Emergency Situation: Lockdown** A building lockdown is a procedure used to keep building occupants safely inside if an outside threat hinders evacuation. Lockdown is also used if an event occurs inside the building where moving within the building would put occupants in harm's way. **Lockdown Response Actions** • In the event of a lockdown, building doors will be locked to restrict access to the building or to restrict an intruder's mobility inside of the building. • If a lockdown is instructed, secure yourself in the room you are in, lock the door (if possible), turn off lights and conceal yourself from sight, remain quiet, silence your cell phone, and **do not** leave until it is deemed safe and the "All Clear" has been given via the PA system or first responders. • If you are in a public area or a cubicle, move to a room which can be secured. **LOCKDOWN** Page 47 of 56 Back Next
Slide 48	**Module 2: Emergency Preparedness** Menu Exit **Responding During an Emergency Situation: Active Shooter** In the event of active shooter violence: • **RUN** (Evacuate). If there is an accessible escape path, attempt to evacuate the premises regardless of whether others agree to follow. • **HIDE**. If you are close to the incident and exiting the building is not possible, hide in a secure location, keep quiet, await instruction. • **FIGHT** (Take Action). As a last resort, and only when life is in imminent danger, attempt to disrupt or incapacitate the active shooter by whatever means necessary. Fight to survive. If possible, have someone call 911 to report the incident and your location. Follow the instructions of Security Officers and first responders. Run Hide Fight Page 48 of 56 Back Next

	Instructor
Slide 49	**Module 2: Emergency Preparedness** [Menu] [Exit] **Requesting Assistance: Emergency Assistance Requests** SEPS is committed to ensuring the safety of FDIC personnel and visitors in the event of a localized building emergency affecting its facilities. If you require additional assistance in the event of an emergency, either temporarily or for the long-term, simply e-mail EmergencyPreparedness@FDIC.gov and a member of the team will work with you to ensure you needs are met. Information will be coordinated with regional points of contact for personnel located in a regional or field office. **It is important to remember that your personal information will not be shared without your consent.** Types of emergency assistance requests include mobility assistance for those who may need help evacuating the building as well as emergency email notifications for those who are Deaf or Hard of Hearing. *Note: If you are an individual with a disability or serious health condition and require a reasonable accommodation, please email DisabilityProgram@fdic.gov for assistance.* Page 49 of 56 [Back] [Next]
Slide 50	**Module 2: Emergency Preparedness** [Menu] [Exit] **Requesting Assistance: Mobility Assistance Requests** If you require assistance evacuating the building due to a disability or a physical need, either permanent or temporary, email EmergencyPreparedness@FDIC.gov. Your personal information will not be shared without your consent. SEPS will: • Prearrange appropriate evacuation procedures. • Build a specific, personal emergency plan to ensure your individual needs are met prior to an emergency. A member of the Emergency Preparedness Program will work with you to coordinate an assigned area of refuge, an evacuation assistant/buddy, and, if appropriate, ensure the Floor Marshal (also referred to as Fire Marshal or Fire Warden) for your area is aware of the needs in the area. If needed, first responders are able to override the elevator system and take individuals who need assistance evacuating down via the elevator. Page 50 of 56 [Back] [Next]

	Instructor
Slide 51	**Module 2: Emergency Preparedness** Menu Exit **Requesting Assistance: Deaf and Hard of Hearing Requests** Individuals who are Deaf or Hard of Hearing in the National Capital Region can request to be added to a designated email distribution list to receive an email message when the fire alarm sounds. To sign up, simply send an email to EmergencyPreparedness@fdic.gov and request to be added to the **Emergency Assistance Group** distribution list. SEPS is also available to coordinate with regional emergency preparedness points of contact to ensure those who are located in the regions receive the messages they need. Page 51 of 56 Back Next
Slide 52	**Module 2: Emergency Preparedness** Menu Exit **Staying Informed: Signing Up for Warning Alerts** FDIC and public safety officials use timely and reliable systems to alert you in the event of natural or man-made disasters. This section describes different warning alerts you can sign up to receive. STAY INFORMED Page 52 of 56 Back Next

	Instructor
Slide 53	**Module 2: Emergency Preparedness** Menu Exit **Staying Informed: The FDIC Emergency Notification System** FDIC Emergency Notification System / Security & Emergency Preparedness Section / SIGN UP for EMERGENCY ALERTS • The FDIC maintains an Emergency Notification System (ENS) that allows SEPS and regional ENS points of contact to rapidly notify personnel by text, email, or voice mail of security situations, office closures, or weather events that could affect personnel safety or the workplace. • The ENS can also be used to conduct accountability of personnel during an emergency event (e.g., building evacuation, shelter in place, or office closure). • ENS is in use nationwide (Headquarters, Regional, Area, and all Field locations). All FDIC personnel will receive emergency notifications on FDIC-issued devices to include office telephones, email, and FDIC-issued iPhone, if applicable. Page 53 of 56 Back Next
Slide 54	**Module 2: Emergency Preparedness** Menu Exit **Staying Informed: Sign Up for the FDIC Emergency Notification System** Personnel have the option to voluntarily add their personal home and mobile telephone numbers and email addresses to the ENS, but providing personal contact information is not required. By adding personal contact information, messages can be received when away from the office and an FDIC-issued device. Personnel have the ability to designate the order in which they receive ENS announcements, including those sent to personal telephone numbers or email addresses by creating a user account. To add your personal contact information, send an email to EmergencyPreparedness@fdic.gov requesting an invitation to create a user account. You will receive a response email with instructions on how to create a user account, enter your personal contact information, and customize how and where you receive alerts. Page 54 of 56 Back Next

	Instructor
Slide 55	
Slide 56	

Instructor	
Slide 57	**Course Menu** **Introduction** Welcome Program Office Overview **Module 1: Physical Security** Module 1 Physical Security How often do you think about your safety and security while at work? Objectives Security Begins with You FDIC Physical Security Overview Reducing Physical Security Risks Making Your Work Environment Safer Access and Security Control Threats Overview Access Control Procedures - ID Badges 1 Access Control Procedures - ID Badges 2 Access Control Procedures - Visitors Access Control - Visitor Video Scenario 1 Access Control - Visitor Video Scenario 2 Access Control - Approaching Unknown Individuals Knowledge Check 1 Knowledge Check 2 Summary - Access Control Procedures Criminal and Terrorist Threats Overview Criminal or Terrorist Threats Suspicious Behaviors and Observations How to Respond to Behaviors and Observations Bomb Threat Procedures Suspicious Mail or Package Summary - Criminal and Terrorist Threats Workplace Violence Threats Overview **Module 1: Physical Security (cont.)** Workplace Violence Indicators of Workplace Violence Hostile Insiders Summary - Workplace Violence Threats Security is Everyone's Business Situational Awareness If You See Something, Say Something **Module 2: Emergency Preparedness** Module 2 Emergency Preparedness Are you prepared for an emergency? Objectives What is an Emergency? Do You Know What To Do in an Emergency? Being Prepared: Occupant Emergency Plans Being Prepared: What am I supposed to do in an Emergency? Responding During an Emergency Situation: Evacuation 1 Responding During an Emergency Situation: Evacuation 2 Responding During an Emergency Situation: Shelter-in-Place Responding During an Emergency Situation: Lockdown Responding During an Emergency Situation: Active Shooter Requesting Assistance: Emergency Assistance Requests Requesting Assistance: Mobility Assistance Requests Requesting Assistance: Deaf and Hard of Hearing Requests Staying Informed: Signing Up for Warning Alerts Staying Informed: The FDIC Emergency Notification System Staying Informed: Sign Up for the FDIC Emergency Notification System Staying Informed: Sign Up to Receive Federal and Local Area Information Course Completion **Return to Previous Page**