FDIC Workplace Security

Introduction

Welcome

FDIC is committed to providing its employees and contractors with a safe and secure place of work.

In an effort to ensure the safety and security of its personnel, information, and facilities, FDIC has put in place programs, policies, and procedures FDIC personnel are required to follow.

In order to maintain a safe and secure workplace, everyone needs to become involved. The main objective of this Workplace Security course is to provide awareness about workplace security risks and steps that can be taken to prevent workplace security breaches.

Program Office

The Security Enterprise Programs Section (SEPS) is part of the Division of Administration and is responsible for the following areas:

- Physical Security
- Occupant Emergency Planning
- Personnel Security
- Intelligence and Threat Sharing Unit

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.

Visit the Security Enterprise Programs Section Intranet page at https://fdicnet.fdic.gov/content/doa/home/workplace/security.html

Overview

This Workplace Security Training consists of three 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: Occupant Emergency Planning

The occupant emergency planning module will introduce you to emergency preparedness and security practices you can follow to ensure you are prepared and know how to appropriately respond during an emergency. This module also provides resources available to FDIC employees to ensure you receive information prior to and during a building emergency.

Module 3: Operations Security (OPSEC)

This module defines OPSEC and explains why it is important. Following the OPSEC Cycle helps the FDIC analyze and assess risks and vulnerabilities and apply countermeasures. This module touches on the ways OPSEC can affect you at work and home.

Module 1: Physical Security

How often do you think about your safety and security while at work?

Appropriate security measures in the workplace help prevent crimes, accidents, and injuries. They also provide peace of mind so you can focus on your work.

It's not only employers who are responsible for workplace safety and security. As FDIC staff, you have an important role to play too.

By following safe practices and making sure you know how to respond in the event of an emergency or security situation, you can protect yourself and others.

This module will introduce you to FDIC workplace security practices and procedures.

Objectives

Upon completion of this Physical Security module, you should be able to do 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

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!

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

Read each description:

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.

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.

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.

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.

Reducing Physical Security Risks

Employees are expected to comply with FDIC Circular 1610.01, FDIC Physical Security Program. This describes procedures for:

- Gaining entry
- Securing your work area
- Responding to emergencies

Washington, DC and Virginia Square office employees can learn how to enter through the garage by viewing the garage entry security video.

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

Garage Video and Transcript

The FDIC has installed new vehicle barriers and high-speed roll up doors at all garage entrances at the Virginia Square Campus, 550 Main Building, and 1776 F Street owned Headquarter buildings. This short video will show how the barriers and high-speed roll up doors operate. When a vehicle approaches the garage entrance, the driver is required to show their FDIC badge to the officer.

Once the officer has manually verified the badge, the driver shall present their badge at the reader. Upon a valid badge read, the vehicle barrier will lower, the gate arm will raise, the traffic light will change from red to flashing amber and the high-speed roll up doors will raise. The flashing amber light is the drivers signal to slowly proceed over the barrier and through the garage door. Upon exiting the garage, the high-speed roll up door will raise when the vehicle crosses over the ground sensor located near the door. Once the high-speed exit door raises, pull forward slowly until you are directly in front of the barrier. When in front of the barrier, another ground sensor will trigger the barrier to lower, gate arm to raise, and light to change from red to flashing amber. When the light flashes amber, it is safe to exit. Please remember to only proceed if the light is flashing amber. Failure to do so may result in damage to your vehicle. When entering FDIC Headquarters building garages only one vehicle may enter per valid badge read and corresponding flashing amber light. When exiting, although the driver is not required to badge at a reader, only one vehicle may exit per amber light. Remember, for safety and security reasons there is no "piggy backing" or "tailgating" for those who have not swiped their PIV cards at the readers. There is a slightly different procedure for bicycles and motorcycles entering and exiting the FDIC garages. As the bicyclist or motorcyclist approaches the garage entrance, they will need to stop and provide their badge to the officer for visual verification. The officer will hold on to the badge while they manually open the barriers and garage door. After the officer returns the badge, the bicycle or motorcycle rider may cross over the barrier and though the garage door. Bicyclist may choose to ride or walk down ramps. When exiting, do not tailgate a car, even if the door or barrier is open. Instead, press the "garage exit" button to safely reset the garage door prior to exiting. If this step is skipped, the garage door will close with the exit of the car possibly injuring the cyclist. The officer will manually open the barrier to exit. Be patient at the garage gates and follow the processes in place for the safety of all.

Making Your Work Environment Safer

You can help make your work environment safer by:

- Always following security rules and procedures, as noted on the SEPS intranet page
- Always asking questions about any safety or security procedure from your Supervisor, Administrative Officer, or SEPS Staff
- Being familiar with the five categories of prohibited items in all FDIC Facilities

To view a complete list of prohibited items, review FDIC Circular 1610.01 Appendix C

Visit the Security Enterprise Programs Section Intranet page at https://fdicnet.fdic.gov/content/doa/home/workplace/security.html

Access and Security Control Threats Overview

The following common threats describe measures you can take in each area to promote a secure workplace:

- **Access and Security Control Threats**
- Criminal and Terrorist Threats
- Workplace Violence Threats

Access Control Procedures – ID Badges 1

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.

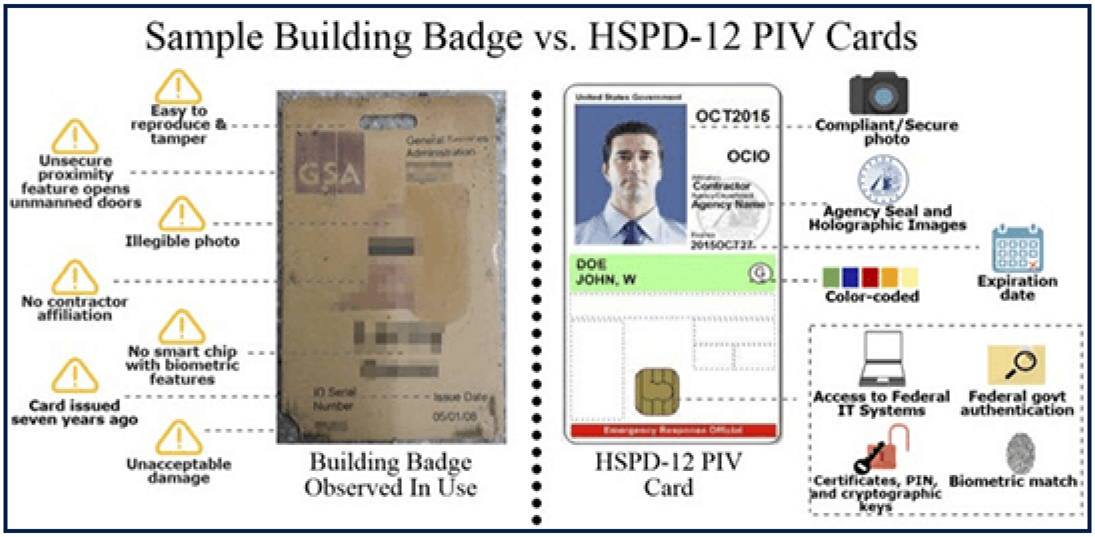
Sample Building Badge vs. HSPD-12 PIV Cards
Easy to reproduce & tamper
Unsecure proximity feature opens unmanned doors
Illegible photo
No contractor affiliation
No smart chip with biometric features
Card issued seven years ago
Unacceptable damage
GSA
Building Badge Observed In Use
OCT2015
OCIO
Contractor
DOE JOHN, W
HSPD-12 PIV Card
Compliant/Secure photo
Agency Seal and Holographic Images
Color-coded
Expiration date
Access to Federal IT Systems
Federal govt authentication
Certificates, PIN, and cryptographic keys
Biometric match

Image Description

Older building badge has the following problems: Easy to reproduce and tamper, Unsecure proximity feature opens unmanned doors, Illegible photo, No contractor affiliation, No smart chip with biometric features, Card issued seven years ago, and Unacceptable damage.

HPSD-12 PIV Card has the following features: Compliant/Secure photo, Agency Seal and Holographic Images, Color Coded, Expiration date, Access Federal IT Systems, Federal govt. authentication, Certificates, PIN, and cryptographic keys, and Biometric match.

Access Control Procedures – ID Badges 2

- Wear your badge on the outermost garment, above the waist, 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.

Link to FDIC Security Points of Contact (https://fdicnet.fdic.gov/content/doa/home/workplace/security/security-contacts.html)

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.

Link to Security Enterprise Programs Section Security Policies (https://fdicnet.fdic.gov/content/doa/home/workplace/security.html)

Link to SEPS's Electronic Visitor Management System (EVMS) (https://fdicnet.fdic.gov/content/doa/home/workplace/security/visitor-system.html)

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.

Scenario Access Control 1 Video and Transcript

Male speaker: Excuse me. Can you hold that door?

Female speaker: Wow, looks like you have your hands full.

Male Speaker: Yeah, all the dollies were checked out. Thanks, you're a life saver.

Female Speaker: Glad to help.

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.

Scenario Access Control 2 Video and Transcript

Male speaker: Excuse me. Can you hold that door?

Female speaker: I'm sorry. I can't let you in.

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.")
- Ask direct 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.

Link to FDIC Security Points of Contact

(https://fdicnet.fdic.gov/content/doa/home/workplace/security/security-contacts.html)

Knowledge Check 1:

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?

Select your answer

a. Borrow your coworker's badge to get into the restroom.
b. Ask around the office to find the person who took your badge.
c. Follow someone else who is heading to the restroom.
d. Report the missing badge to the appropriate security personnel.

Feedback

The correct answer is D.

You should report the missing badge to the appropriate security personnel.

Knowledge Check 2

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?

Select your answer

a. Continue to your manager's office; the report is due!
b. Report what you saw to the appropriate supervisor or security personnel.
c. Block the man and demand to see his badge.
d. Report the missing badge to the appropriate security personnel.

Feedback

The correct answer is B.

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.

Summary – Access Control Procedures

- You are responsible for your badge.
- Wear your PIV above the waist and visible.
- 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.
- Your safety and the safety of your co-workers comes first.

Criminal and Terrorist Threats Overview

The next threats relate to potential criminal and terrorist activities.

- Access and Security Control Threats
- **Criminal and Terrorist Threats**
- Workplace Violence Threats

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.

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 from 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)

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.

Link to FDIC Security Points of Contact (https://fdicnet.fdic.gov/content/doa/home/workplace/security/security-contacts.html)

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.

Read the 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)

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.

Read the FDIC Guidance on Handling Suspicious Mail or Packages below.

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

Summary – Criminal and Terrorist Threats

The greatest deterrent to Criminal and Terrorist Threats is you!

Report:

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

Workplace Violence Threats Overview

In this section of the course, we'll cover workplace violence threats

- Access and Security Control Threats
- Criminal and Terrorist Threats
- **Workplace Violence Threats**

Workplace Violence

Incidents of violence in the workplace, including domestic violence, have caused federal agencies to assess their vulnerabilities and risk factors while implementing 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

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.

Management Response Teams (MRT)

Management Response Teams work with the Security Management Section to:

- Identify and correct any physical security weaknesses at FDIC facilities
- Establish local procedures for dealing with incidents of harmful acts involving FDIC
- Assess any potential threat to an FDIC employee and recommend an appropriate course of action

You may refer to the FDIC Circular 1600.2, Workplace Violence Prevention Policy, for additional information.

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. The Department of Homeland Security (DHS) has created a video that shows what actions to take in an active shooter situation.

The video contains discussions of violence and graphic imagery. Sensitive audiences may choose to skip this 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.

Link to Security Enterprise Programs Section (https://fdicnet.fdic.gov/content/doa/home/workplace/security.html)

Link to RUN. HIDE. FIGHT.® Surviving an Active Shooter Event - English (https://www.youtube.com/watch?v=5VcSwejU2D0.)

Run. Hide. Fight.

In this fictional video, a man wearing light tactical gear and dark sunglasses enters an office area and begins firing a gun. Frightened office workers hide, prepare to defend themselves, evacuate the building, and warn others of the situation.

This video was produced by the City of Houston Mayor's Office of Public Safety and the Department of Homeland Security.

Statistics and Tips from the Video

Run when an active shooter is in your vicinity.

- If there is an escape path, attempt to evacuate.
- Evacuate whether others agree to or not.
- Leave your belongings behind.

- Help others escape if possible.
- Prevent others from entering the area.
- Call 911 when you are safe.

Hide if evacuation is not possible; find a place to hide.

- Lock and/or blockade the door.
- Silence your cell phone.
- Hide behind large objects.
- Remain very quiet.
- Your hiding place should:
    - Be out of the shooter's view.
    - Provide protection if shots are fired in your direction.
    - Not trap or restrict your options for movement.

Fight as a last resort and only if your life is in danger.

- Attempt to incapacitate the shooter.
- Act with physical aggression.
- Improvise weapons.
- Commit to your actions.

911- When law enforcement arrives:

- Remain calm and follow instructions.
- Keep your hands visible at all times.
- Avoid pointing or yelling.
- Know that help for the injured is on its way.

Active shooter statistics:

- 21 killed, 19 wounded eating at a fast food restaurant
- 32 killed, 25 wounded while attending classes
- 6 killed, 13 wounded at a shopping center
- 13 killed, 29 wounded while at work

For more information: www.readyhoustontx.gov

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.

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.

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.

Link to FDIC Security Points of Contact (https://fdicnet.fdic.gov/content/doa/home/workplace/security/security-contacts.html)

Module Two: Occupant Emergency Planning

Are you prepared for an emergency?

Preparing for a crisis is more than just knowing how or when to call 911 or waiting for first responders to direct you to safety. Emergency preparedness is about ensuring that you are ready before an emergency and are prepared to react appropriately to any emergency in a calm and thoughtful fashion.

It is not only the responsibility of the FDIC to ensure you are safe in the workplace. You too have responsibilities in ensuring you can respond appropriately in the unlikely event an emergency occurs in the workplace.

By understanding the steps of preparing for an emergency and making sure you know how to respond, you will be able to protect your own life and assist those around you if the time comes.

Objectives

Upon completion of this Occupant Emergency Planning module, you should be able to do the following:

- Describe occupant emergency 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

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.

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 cover.

Being Prepared

Responding During an Emergency

Requesting Assistance

Staying Informed

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 security information can be found on the SEPS web page for Headquarters employees and the respective regional offices web pages for regional office-specific plans.

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 in SEPS Physical Security Unit and Facilities Operations Section (FOS). They are supported by Federal supervisory employees 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 may communicate response activities to the Supervisors / Floor Marshals. All building occupants are to follow the direction of the OET, Supervisors / Floor Marshals, and Security Officers to ensure appropriate response to an emergency event.

When an emergency occurs, the safety of occupants is most important. Depending on the nature of the emergency, occupants may need to evacuate the building, shelter-in-place, or be prepared for a complete lockdown of the building. Additionally, in the event of an active shooter situation, personnel must quickly react and respond based on their own instincts, unless directed by law enforcement or other emergency personnel, and "run, hide, or fight".

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, Supervisors / 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.

Responding During an Emergency Situation: Evacuation 2

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, Supervisors / 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.

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.

Partial or Zoned Building 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.

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, Supervisors / Floor Marshals, or first responders.

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 outside entry into the building or mobility inside the building.

- If a lockdown is communicated, occupants will be instructed to remain inside the building and await further information. Building occupants should not attempt to leave the building until “All Clear" has been given via the PA System or first responders.

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.

Requesting Assistance: Emergency Assistance Requests

The FDIC is committed to ensuring the safety of FDIC personnel and visitors in the event of a localized building emergency affecting its facilities. Emergency Preparedness Program staff in the Crisis Readiness and Response Section (CRRS) support SEPS and FDIC personnel by coordinating emergency assistance requests.

If you require additional assistance in the event of an emergency, either temporarily or for the long-term, simply email EmergencyPreparedness@FDIC.gov, and a member of the team will work with you to ensure your 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 reasonableaccommodationrequests@fdic.gov for assistance.*

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. Crisis Readiness and Response Section (CRRS) staff 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 ensure Security

Officers are 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.

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.

CRRS staff are 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.

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.

Staying Informed: The FDIC Emergency Notification System

- CRRS maintains the FDIC Emergency Notification System (ENS) that allows HQ and regional ENS dispatchers to rapidly notify personnel by text, email, or voicemail 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.

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.

Staying Informed: Sign Up to Receive Federal and Local Area Information

OPM Alert Mobile App

OPM Alert is the official operating status app of the US Office of Personnel Management (OPM). This free app provides a real-time look at the current operating status for Federal Government offices in the Washington, DC area. This app allows you to instantly view the current and active operating status and sign up for optional push notifications when status changes occur. You can also review previous status updates and take a look at OPM's Dismissal and Closure procedures for the Washington, DC area.

Download the OPM Alert Mobile App at https://www.opm.gov/policy-data-oversight/snow-dismissal-procedures/mobile-app/

Accuweather.com Alert

Local weather alerts inform you of any potential dangerous developing weather patterns.

Download the OPM Alert Mobile App at https://www.opm.gov/policy-data-oversight/snow-dismissal-procedures/mobile-app/

Register with AccuWeather for customizable weather alerts at https://afb.accuweather.com/snow-alerts

CapitalAlert.gov

Sign up for your local government alerts. Local governments in the National Capital Region have their own alerting systems which are not tied to the FDIC ENS.

To sign up for local government alert and warning system at visit http://www.capitalert.gov/

Module Three: Operations Security

Objectives

Upon completion of this Operations Security module, you should be able to do the following:

- Define Operations Security (OPSEC)
- Recognize the importance of OPSEC
- Identify the OPSEC Cycle
- Identify critical information and assets
- Recognize OPSEC-related threats and vulnerabilities
- Determine the necessary countermeasures to employ to protect and safeguard information at your workplace and home

Introduction

This module provides fundamental OPSEC awareness for the FDIC workforce to protect critical and sensitive information that is essential to protecting FDIC's mission and workforce.

The OPSEC program is designed to prevent the exploitation of any information that might harm the FDIC. This is achieved through continual assessments that identify and analyze critical information, vulnerabilities, risks, and external threats.

OPSEC Governance and FDIC Directive 1610.05

As indicated in the National Security Presidential Memorandum (NSPM)-28, the National Operations Security Program (NOP) requires all agencies to establish an OPSEC Program to identify and protect critical and sensitive information.

FDIC Directive 1610.05, Operations Security Program, fulfills the NSPM requirement and establishes policy, roles, and responsibilities to ensure national-level OPSEC compliance.

What Is Operations Security?

OPSEC is a systematic process that helps deny potential adversaries information about our capabilities and intentions. This is accomplished by identifying, controlling, and protecting information associated with the planning and execution of sensitive activities.

America's adversaries collect information pertaining to U.S. Government activities in order to harm and gain advantage. Small pieces of information can be of great value to an adversary.

By putting together enough small details and indicators, an adversary may piece together enough information to cause harm to the FDIC.

OPSEC serves as a complement to traditional security measures already in place to protect against exploitation of critical information. There is some overlap with Physical Security, Information Security, and Personnel Security, though OPSEC is a distinct discipline.

Importance of OPSEC

Understanding how an adversary could potentially exploit vulnerabilities to compromise your personal information and learning the different countermeasures to prevent it are key to ensuring that critical information does not land in the adversary's hands.

OPSEC is not just a set of rules that tells you what you should or should not do. Rather, it helps us understand threats and vulnerabilities by using a cyclical approach to deny critical information to adversaries.

What Are Threats?

A threat is anything that can exploit a vulnerability intentionally or unintentionally and obtain, damage, or destroy an asset. A threat is what we are trying to protect against. It is necessary to understand relevant threats so you can develop appropriate countermeasures.

Threat assessments identify:

- Potential adversaries and their capabilities
- Adversaries' intentions to collect, analyze, and exploit critical information

Collaboration and support between security, intelligence, and counterintelligence experts are key in this process.

What Are Adversaries?

An adversary is a bad actor and can be an individual, group, organization, or government that threatens to compromise the FDIC's interests, mission, or sensitive information. An adversary is any entity with goals counter to our own.

Adversaries can be:

- Criminal organizations
- Nation states
- Economic competitors
- Terrorist organizations
- Hackers
- Insiders

These entities can blend. For example, hackers can act on the behalf of nation states, and criminal organizations can conduct cyber activities as hackers.

The OPSEC Cycle

The OPSEC methodology operates by a never-ending analytical and objective process cycle.

Understanding the Cycle and the benefits of the process is the first step to using OPSEC to help determine the necessary countermeasures to employ, to protect, and safeguard information in your workplace and home.

Read each step to learn more.

Step 1: Identify Critical Information

Critical information is classified or unclassified information that is important to the achievement of U.S. objectives and missions. It requires safeguarding or controls over its dissemination. The unauthorized access to or modification of critical information could adversely affect the national interest or national security, the conduct of Federal programs or operations, or individual privacy and identity management. It may be of use to an adversary of the U.S.

Information or activities identified in this step are captured in the FDIC Critical Information List (CIL) available to personnel to help them understand what must be safeguarded.

FDIC critical information examples include:

- Personally Identifiable Information (PII)
- Documentum (the repository of insured institutions' resolution plans, also referred to as living wills)
- Technical evaluations of contracts
- Background investigation documentation
- Continuity of Operations Plans

Here are some questions to help you identify critical information:

- Is the FDIC involved in activities that include access to sensitive information?

- Does an adversary gain advantage from access to this information?
- Is the information transmitted, disseminated, or disposed of properly to prevent unauthorized disclosure or loss?

Step 2: Analyze Threats

An OPSEC threat is an adversary whose activities indicate potential harm to life, information, operations, the environment, and property. Analyze threats by:

- Being objective
- Using reliable resources and sound judgment when determining threats
- Assessing an adversary's **capability**, **intent**, and **opportunity**

Step 3: Analyze Vulnerabilities

Vulnerabilities are:

- The susceptibility of information to exploitation by an adversary
- Weaknesses an adversary can exploit to get your critical information

Ensure you analyze any vulnerabilities that may be exploited by adversaries.

Step 4: Assess Risks

Risk assessment is evaluating risks to critical information, its susceptibility to adversarial collection, and anticipated impact of loss or compromise.

The probability of a determined adversary exploiting a vulnerability and compromising FDIC critical information can be HIGH without proper OPSEC applied.

Step 5: Apply Countermeasures

Countermeasures are actions, measures, or devices intended to reduce an identified risk, threat, or danger.

Countermeasures can be applied once risks are identified.

Step 6: Assess Effectiveness

The OPSEC Cycle never ends, and we must regularly review the FDIC's efforts to protect information from adversaries.

The effectiveness of the program and countermeasures we put in place will determine if FDIC's critical information is always safe.

Critical Information

What is Critical Information?

OPSEC views critical information from both the friendly and adversarial points of view to help determine the value and impact of the information if compromised.

Critical information is sensitive unclassified or classified information about the FDIC's activities, intentions, or capabilities an adversary can use to exploit, compromise, or interrupt our mission.

Examples of critical information include:

- Personally Identifiable Information (PII)
- Schedules and travel itineraries
- Usernames, passwords, network details
- Continuity of Operations Plans
- Security assessments
- Acquisitions
- Training materials
- Security clearance data
- Pre-decisional information

Collection of Information

Adversaries collect critical information through various ways, including:

Open-Source

Exploiting open-source information that is unclassified and publicly available.

Eavesdropping

Critical information can be inadvertently released during casual conversations, especially in public spaces. Have you been at a restaurant for lunch and overheard or engaged in work-related conversations?

Social Engineering

Tricking people into providing sensitive information or access, the most common of which is phishing.

Phishing

Phishing is using an email that looks legitimate to induce individuals to reveal critical information. Scammers can use phishing to trick people into installing malware or sending sensitive information.

Protecting and Safeguarding Information

To protect our critical information, we have to know what to protect.

What Information to Protect and Safeguard

The FDIC Critical Information List (CIL) is designed so everyone understands what information needs to be protected and is critical to our success and mission.

How to Protect and Safeguard Critical Information

Know

Know what is on the CIL. Is what you are typing or talking about on the CIL? If so, do not share it with those who do not have a need to know.

Think

Consult the CIL before you send an unencrypted email, have a discussion in a public place, or share information with family or friends.

Limit

If you have to share critical information, such as your travel itinerary, with family or close friends, ask them not to share this information. You would not share this information with your dry cleaner, neighbors, or people at the gym.

Always limit the details of what you share depending on the audience.

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is critical information that can be used to distinguish or trace an individual's identity. Some examples of PII are:

- Name
- Social Security Number
- Biometric records (e.g., finger or palm prints, DNA, voice or facial patterns)

PII can be used alone or combined with other personal or identifying information, such as date of birth, place of birth, or mother's maiden name, to be linked to a specific individual.

PII is a key component of our lives and online identity and can be exploited by adversaries, so it is essential to safeguard it.

How Vulnerabilities Are Observed by Adversaries

Vulnerabilities are weaknesses that an adversary uses to obtain critical information. They provide an opportunity to disrupt the FDIC's mission and activities. Vulnerabilities can be detected or observed in many ways, such as:

- Observing an activity we do, such as basic security procedures when entering an FDIC building
- Observing the physical environment of our work area
- Getting information from our policies and procedures or the Internet

In reality, the biggest vulnerability is ourselves. Adversaries observe what we say and do, so we have to be careful.

Common Vulnerabilities

Here are some common vulnerabilities:

- Use of email, social media, and the Internet
- Access to mail, trash, and recyclables
- Predictable patterns and procedures
- Lack of awareness of threats and vulnerabilities
- Increased connectivity on unsecured devices
- Aggregation of data (data compiled from multiple sources)

Be OPSEC-minded and think about:

- What we do or post on the Internet
- What we discard without sanitizing
- How we conduct ourselves and the connection between our devices and our lives

Vulnerability Indicators

Indicators are observable and detectable activities that signify the degree to which our critical information is vulnerable. They act as clues to an activity that adversaries can exploit to their advantage through analysis.

Indicators alone are not considered OPSEC vulnerabilities. However, a combination of indicators can potentially reveal critical information.

Here are some examples of signs which could serve as indicators:

- Sudden changes in procedures
- Staging of cargo or vehicles
- Presence of specialized equipment
- Increased security measures
- Personal behavior or actions

How Is Risk Related to OPSEC?

In the context of OPSEC, risk is the likelihood of an adversary getting hold of your critical information. In our home life, if we left our purse or wallet in plain sight in our car, there is a high risk that it would be taken.

Risks are created by vulnerabilities, and they can be mitigated by the use of protection and safeguarding measures outlined in the OPSEC Cycle and process.

Stolen Identity and Its Effects

Many companies collect personal information about their customers, including names, addresses, phone numbers, bank and credit card account numbers, income, and even Social Security Numbers.

Stories regarding fraud and telephone or Internet scams are becoming more widespread because of the span of information available from various sources.

Do your best to protect your information with the following tips:

- Shred documents instead of just throwing them away.
- Protect your personal computer networks.
- Randomize your passwords and change them often.
- Do not give your Social Security Number to anyone unless you are assured how it will be used, stored, and protected.
- Do not use web commerce without assurance that the website is secure.

Use of Countermeasures

Use of countermeasures helps reduce the likelihood of critical information being lost. You must understand threats and vulnerabilities, employ OPSEC measures, and follow policies to reduce risks.

You can reduce the probability of adversaries observing indicators and exploiting vulnerabilities by taking various countermeasures.

Examples of Countermeasures

- Encrypting files containing PII
- Encrypting all emails with sensitive information
- Ensuring all information is reviewed by Public Affairs for OPSEC concerns before it is released to the public
- Destroying any papers with sensitive information properly
- Not discussing sensitive information with unauthorized people
- Being cautious of having sensitive discussions in public (in person or online)

- Ensuring that your privacy settings are turned on for your smart devices and on social media
- Using unique passwords for all your personal accounts

When applied properly, OPSEC principles can promote safety, security, and success.

OPSEC at Work: Keeping Your Workspace Safe

Whether you are in the office, teleworking, or on travel, you must protect critical information.

Read below to learn more about how to protect your critical information.

At the Office

- Encrypt your emails
- Remove your PIV card when not using your device
- Shut your device down at the end of your day

Teleworking

Teleworking increases the chances of inadvertently exposing critical information to the wrong person.

Adversaries target teleworkers by using different methods and types of software to gain access to sensitive information. Most at-home cyberattacks occur when employees click on bad links and phishing emails.

Poor security configurations and practices allow adversaries to exploit security flaws in connected devices and potentially provide adversaries access to sensitive information.

Protecting Information While Teleworking

- Protect your router
- Guard against eavesdropping
- Protect sensitive and critical information
- Don't mix business with pleasure
- Remove your PIV Card
- Don't connect unauthorized devices
- Keep security updates current
- Keep devices apart
- Shut your device down at the end of your day

Work Travel

- Avoid unsecure public Wi-Fi
- Don't leave your laptop unattended
- Be conscious of public discussions relating to work

OPSEC at Home: Keeping Your Family and Home Safe

We usually think about applying OPSEC at work to protect our mission, but it is also important to practice it at home to protect yourself, your family, your information, and your property.

The average household contains at least ten different connected devices. All these devices can create vulnerabilities, which increase the probability of providing indicators to adversaries. Many family members inadvertently provide critical information without even realizing it.

When your critical information is exposed to the wrong person, it can endanger your family. It is important to understand the risk that an adversary could create with your critical information if you share it.

You should practice OPSEC at home to protect your family's information.

Read below to learn more about what measures you can take to protect your critical information at home.

Protect Your Network

- Install the latest router firmware
- Use strong passwords
- Encrypt and hide your network
- Change passwords regularly, especially for your Wi-Fi

Protect Your Social Media Account

- Refrain from posting a lot of personal information
- Use the highest privacy setting available
- Be selective with friend and connection requests
- Turn off location settings features
- Avoid clicking on suspicious messages or links

- Report any scam posts or messages

Summary: Operations Security

- Avoid risks by reducing vulnerabilities and taking correct countermeasures to keep you and your critical information safe at the office and at home.
- Remember, OPSEC is a proven risk analysis process that determines the value of unclassified information and helps you protect critical information. Awareness is key.
- The OPSEC Cycle uses an iterative process to identify and analyze threats and vulnerabilities to determine necessary countermeasures to employ to protect and safeguard information.
- OPSEC does not stop when you leave work.
- Share this guidance with your family and colleagues. Your inner circle becomes safer when everyone does the right thing.

For additional resources, go to the SEPS web page or email us at ITSU-Info@fdic.gov.

Visit the Security Enterprise Programs Section Intranet page at https://fdicnet.fdic.gov/content/doa/home/workplace/security.html

Course Completion

You have now completed the FDIC Workplace Security Training.