Insider Threat and Counterintelligence Program (ITCIP)

Introduction

How much do you know about your work environment?

ITCIP Introduction Video Transcript

"I always knew that guy was off. he complained a lot. His schedule was odd. He came in at odd hours. and he asked a lot of questions… maybe too many questions. He just wasn't like the rest of us, just trying to do our jobs."

"But there wasn't really "that one thing that really tipped me off that he was doing something wrong, and it wasn't my place to say anything. It's like a code. We're a team. you don't rat out your team."

"I never thought anything like this could happen here. We're FDIC. We don't have access to anything that could hurt someone, do we?"

If you see something, say something.

If You See Something, Say Something

The FDIC Insider Threat and Counterintelligence Program (ITCIP) is a defensive program focused on preventing and mitigating internal and external threats and risks posed to FDIC personnel, facilities, assets, resources, and both national security and sensitive information by insider threats and foreign intelligence entities.

Information about the program, along with helpful employee resources, are at the ITCIP website on the FDIC intranet. You can navigate to the site by selecting DOA under Divisions & Offices, then selecting Insider Threat & Counterintelligence under Workplace Services.

Objectives

Completing this training will enable you to:

- Describe the risks to the FDIC from insider threats.
- Identify methods adversaries may use to recruit insiders.
- Recognize indicators associated with possible insider threats.
- Describe reporting procedures when insider threat activity is suspected or detected.
- Describe ways in which you can protect yourself and others from insider threats.

Who is an Insider Threat?

An insider threat is anyone with authorized access to the information or things an organization values most, and who uses that access — either wittingly or unwittingly — to inflict harm to the organization or national security. When an insider becomes a threat, it can have far-reaching consequences on both an organization and national security.

As an FDIC employee, you play an important role in protecting against insider threats.

What Does an Insider Threat Look Like?

First, it helps to understand an insider risk. Everyone with access to FDIC facilities, personnel, systems, assets, or other resources carries a certain level of risk.

There is a small possibility that any one of us could cause harm, whether from having a bad day, not sleeping enough, encountering bad traffic on the way to work, or from something more nefarious — actually wanting to expose sensitive information improperly, being purposefully destructive, or acting against the FDIC at another party's request.

By allowing us the legitimate insider access we have, the Federal Government and the Office of Personnel Management have determined that we are not "trusted insiders" but rather simply less of a risk than someone in the public who may have been denied that same level of access.

Read Kim's Statement below.

"I was looking for a bad guy. I never thought it could be my friend. I never thought he'd hurt our organization."

What do insider threats look like?

They look like you and me. They look like your friends and neighbors. They could be the friendly foreign nationals you're hosting at an FDIC conference. They can be anyone and they can target anything. Sometimes insider threats are unwitting employees who simply create vulnerabilities for others to exploit. Classified information, proprietary information, personnel security, and physical security may be threatened as a result.

What are their motivations?

Malicious insiders go after anything they can use to inflict harm. They have many motivations. Some do it for money, while others do it for ego. Others do it for an ideological cause or to support another country's interests. Others do it simply because they can. There are many cases of insiders betraying the trust of their organizations and their nation. Perhaps the best known of these is the WikiLeaks case. But the FDIC has had its share.

Recent Cases from the FDIC

Case File #1

John Doe was an employee assigned to a temporary satellite office. During the course of his employment with the FDIC, Doe was detailed to a headquarters division in Washington, DC. Between January 2011 and September 2012, he emailed over 900 FDIC documents to his personal email account including sensitive, confidential, and strictly private information.

The FDIC-OIG conducted an investigation. The case was prosecuted by a United States Attorney's Office. On January 27, 2017, John Doe was sentenced to serve two years' probation in connection with his prior plea of guilty to a misdemeanor charge of intentionally exceeding authorized access to a FDIC computer to obtain information.

Case File #2

A former FDIC employee downloaded to her personal computer the private, highly sensitive documents from three financial firms in 2015, allegedly to leverage her job

prospects in the private section. After law enforcement agents found evidence of the theft at her home, she was arraigned on theft of government property charges and released on $5,000 bond. If convicted, she faces up to 10 years' incarceration.

Other Examples

- An employee departing the FDIC emailed eight documents he wrote containing sensitive FDIC business information to a personal email account. The FDIC Office of Inspector General sent two investigators to his home to retrieve the information and identify his reasons for wanting the information past his separation date.
- Here is something many of us do frequently: send a file to a shared printer, then forget about it.

But what if that information is what we refer to as high value asset information, such as sensitive information from a database, or other information such as encrypted emails, building blueprints, system schematics, or IT systems logs? Such information in the wrong hands can potentially be used to cause the FDIC and its personnel harm.

Lesson One: Risks to the FDIC

Using FDIC Information

Much of the information we handle on a daily basis may seem innocuous by itself. But casual updates on your social media pages or simple lunchtime conversation about work that is overheard can potentially be combined with other information leading to loss of public confidence.

Information that you create on behalf of the FDIC is always owned by the FDIC. Regardless of the pride you take in your work, you do not own the data rights to your work product. Take care when posting information about your work online and when applying to positions outside of the FDIC.

Below are examples of improper use of FDIC work products.

- Writing samples that have not had sensitive information or FDIC-affiliation redacted.
- Resumes including specific bank names, valuation, composite ratings, and outcomes of your work like “cease and desist orders.” Employment application

websites such as USAJOBS are NOT FDIC owned or operated.

- Sending a list of usernames and passwords, including FDIC system passwords, to a personal account for use at home.
- Bringing work home without keeping it in a secure, locked cabinet or room away from other occupants.
- Posting non-public information about the FDIC on social media.

Information Gathering Methods

An adversary who wants information can often get it just by listening to talkative employees or observing what we do outside the office.

Below are some of the more common methods they may use.

- Hanging out in nearby locations, like frequent lunch or after-hours spots, to overhear casual conversations to acquire information not openly available.
- Various cyber techniques, including but not limited to spear-phishing and whaling, against U.S. personnel or computer systems.
- Unexpectedly trying to enter U.S. facilities to test physical security measures and identify weaknesses for later use.
- Scheduled foreign visitors who may be operating under false pretenses to exploit a legitimate visit for information gathering purposes.
- Electronic monitoring, tampering, and penetrations to exploit U.S. official and personal travelers during overseas visits.
- Authorized access, as an insider, to harm the security of the U.S. through espionage, terrorism, self-harm, or disclosure of sensitive or classified information.

Hostile Insiders

You probably never think much about active shooter scenarios. However, such hostile physical actions can result from an insider threat. It is important to be able to recognize that active physical security situations can happen. See what action to take

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 web sites and the Headquarters OEP can be found on the Security & Emergency Preparedness Section (SEPS) web page.

Lesson Two: How Adversaries Recruit Insiders

Why Insider Threats Occur: Privileged Access

While some insiders volunteer, others are targeted and recruited by adversary groups. Certain risky behaviors may enable insider threat activities.

Choose the behavior that best matches the following description.

When personnel intentionally abuse their privileged access to cause damage to the FDIC.

A. Ignorance
B. Malicious Intent
C. Complacency

Feedback:

Correct answer is b. Malicious Intent - When personnel intentionally abuse their privileged access to cause damage to the FDIC.

Why Threats Occur: Approach to Policies and Information Security

While some insiders volunteer, others are targeted and recruited by adversary groups. Certain risky behaviors may enable insider threat activities.

Choose the behavior that best matches the following description.

When personnel expose the FDIC to external risks due to a lax approach to policies, procedures, and information security.

A. Ignorance
B. Malicious Intent
C. Complacency

Feedback:

Correct answer is C. Complacency - When personnel expose the FDIC to external risks due to a lax approach to policies, procedures and information security.

Why Insider Threats Occur: Lack of Awareness

While some insiders volunteer, others are targeted and recruited by adversary groups. Certain risky behaviors may enable insider threat activities.

Choose the behavior that best matches the following description.

When personnel expose the FDIC to external risks due to a lack of awareness of security policies, procedures, and protocols.

A. Ignorance
B. Malicious Intent
C. Complacency

Feedback:

Correct answer is A. Ignorance - When personnel expose the FDIC to external risks due to a lack of awareness of security policies, procedures and protocols.

Who are the FDIC's adversaries?

Those we consider adversaries include anyone who is trying to obtain information about the FDIC or its personnel that could be used against individuals or the organization. Examples include:

- Foreign Intelligence Entities and Foreign Security Services
- Terrorist organizations
- International criminal organizations
- Global competitors
- Hackers
- Witting insiders who are planning to do harm

Recruitment Methods

While not all insiders are recruited, those who are often recruited slowly over time. Recruitment frequently involves contacts with individuals or organizations from foreign countries. However, an already committed U.S. spy may attempt to recruit colleagues, possibly without the colleagues' knowledge of the malicious intent.

Read Eugenio's statement below.

"I did wonder how he supported his lifestyle, but I didn't think it was my place to say anything."

Phases of Recruitment

Classic recruitment by adversaries is a four-phased process. First, intelligence officers spot and assess individuals for potential recruitment. Adversaries are not necessarily looking for someone with a high level of access. Frequently the potential for future access or the ability of the recruit to lead to other high value targets is enough to generate adversary interest.

Many foreign intelligence agencies are vying for long-term advantage against the United States. Their interest in a recruit may not be obvious until years later.

Below are explanations of each phase

Spot and Assess Phase

Spotting and assessing potential recruits can take place anywhere, but is always approached in a non-threatening and seemingly natural manner. Put yourself in the place of an intelligence officer. How would you recruit a computer scientist? Perhaps at a trade show or through a business contact or perhaps at a computer store or other social event.

FDIC employees could be easily targeted at training, public venues, or conferences where attendees let their guard down among people like themselves. Even online venues — such as chat rooms, social media platforms, and interactive or role-player games — are used for this process.

During the Spot and Assess phase, the Foreign Intelligence Entity (FIE) will often explore potential exploitable weaknesses that may be used as leverage against the recruit. These could include: drugs or alcohol, gambling, adultery, financial problems,

excessive foreign family or financial interests, strong ideological sympathies, work underperformance, general naïveté, or other weaknesses.

Develop Phase

Once a potential recruit has been identified, adversaries begin to cultivate a seemingly benign relationship with that individual. At first, the recruit may or may not know that he or she has been targeted for development. Meetings are casual, social, and meant to develop general affinity between the intelligence officer and recruit.

Gradually, in the Develop phase, meetings with the recruit will become more private – and less likely to be observable or reportable. The recruit will begin to trust in the confidence felt from the relationship with the FIE.

Recruit Phase

Actual recruitment may involve appeals to ideological leanings, financial gain, blackmail or coercion, or any other of a number of motivators unique to that recruit. Some of these may manifest as observable and reportable behaviors.

The Recruit phase provides the targeted individual with a "pitch" to assist in the FIE's information gathering efforts. That pitch could include various other motivations the FIE learned during the Develop phase. Does the recruit need money to cooperate? Does the recruit need to feel like James Bond? Does the recruit require the threat of embarrassment through coercion or blackmail? FIEs have already thought through multiple strategies to get whatever they want out of their target.

Handle Phase

By the time the Handle phase is initiated, the recruited individual is emotionally tied to the adversary, either through the bonds of affinity or through fear of exposure. The targeted person is providing sensitive information to the handler.

The handler may be "tasking" the recruit with delivering specific information to which the recruit has access or going beyond access permissions to find information that will require overreaching in a potentially observable way.

Lesson Three: Indicators of Possible Insider Threats

Insider Threat Indicators

While some insider threats act on their own, others are targeted and recruited by adversary groups. For this reason, you should be aware of common signs someone is being recruited. Once an insider turns on his or her organization, that person will start collecting information. You need to be aware that this might be happening.

Once they have information, insiders must then transmit it. If you know the signs of information transmittal, you will be better prepared to detect it. And insiders often exhibit other common suspicious behaviors you need to know about.

Not all of these indicators will be evident in every insider threat and not everyone who exhibits these behaviors is doing something wrong. However, most of the insider threats we have discovered displayed at least some of these indicators. It is important for you to be aware of these behaviors so you can combat the insider threat and protect the FDIC and the country.

General Suspicious Behaviors

Once an insider threat is revealed, coworkers often recall signs that something wasn't right. An active insider threat may exhibit a number of suspicious behaviors, including working outside of regular duty hours, repeatedly failing to follow processes and policies which result in security violations, or displaying a general lack of respect for the U.S. and the FDIC.

Special attention should be paid to disgruntled employees. Disgruntlement is a major motivating factor in insider threat cases.

For more specifics on behavioral indicators, check out the job aids and training supplements on the ITCIP web site

Read Regena's statement below.

"I always knew that guy was off. his schedule was odd. He would come in after hours when no one else was around."

Suspicious Behaviors - Recruitment

Indicators of insider threats fall under three major categories, each with its own set of indicators.

Examples of **recruitment** include, but are not limited to:

- Unreported request for critical assets outside official channels
- Unreported or frequent foreign travel
- Suspicious foreign contacts
- Contact with an individual who is known to be, or is suspected of being, associated with foreign intelligence, security, or terrorism
- Unreported offer of financial assistance, gifts, or favors by a foreign national or stranger: Beware of those bearing gifts
- Suspected recruitment by foreign or domestic competitive companies to convince employee to work for another company

Suspicious Behaviors - Information Collection

Before insiders can steal information, they must first **collect the information**. It can be intentionally stolen by a malicious insider or a person may have it already, and then inadvertently or purposefully leak it.

Insiders may physically remove files; they may steal or leak information electronically; or they may use elicitation as a technique to subtly extract information about you, your work, and your colleagues.

When done well, elicitation can seem like simple small talk. In reality, we each use elicitation every day, whenever we ask a question to learn from someone else. Elicitation is how people on a first date decide they want to have a second date…or not.

The same concept that we use to conduct facets of our business and personal lives are used against us by nefarious actors. We may think we have a new friend. In reality, we may have just been unwittingly recruited.

Read Mary's statement below

"He asked a lot of questions…maybe too many questions."

Information Collection Methods

There are a number of collection methodologies, but the most common foreign collection methods, used in over 80% of targeting cases, include:

- Unsolicited and direct requests for information
- Suspicious Internet activity
- Targeting at conferences, conventions, and trade shows
- Solicitation
- Employment
- Foreign visits
- Cyber intrusions

Cyber intrusions are quickly becoming the greatest method of collection. Adversaries can penetrate systems and gather information with little effort or cost and often without knowledge of the owner.

Regardless of the method used, any time a person attempts to access or record information without authorization, regardless of intent, it should be of concern.

Information Collection Indicators

Examples of improper information collection include, but are not limited to:

- Unauthorized downloads or copying of files, especially for employees who have given notice of termination of employment
- Keeping critical assets at home or any other unauthorized place
- Acquiring access to automated information systems without authorization
- Operating unauthorized cameras, recording devices, computers, or modems in areas where sensitive assets are stored, discussed, or processed

- Asking you or anyone else to obtain sensitive assets to which the person does not have authorized access
- Seeking to obtain access to sensitive assets inconsistent with present job requirements

Suspicious Behaviors – Information Transmittal

Examples of improper **information transmittal** include, but are not limited to:

- Removing critical assets from the work area without appropriate authorization
- Extensive use of copy, facsimile, or computer equipment to reproduce or transmit sensitive asset-related information that may exceed job requirements
- Discussing sensitive asset-related information in public or on a personal cell phone
- Actions/behaviors specific to national security:
- Using an unauthorized fax or computer to transmit classified information
- Attempting to conceal any work-related foreign travel and any personal foreign travel while having a national security clearance or access to covered sensitive information, or being a contractor with a similar reporting requirement
- Improperly removing the classification markings from documents.

Read Jenise's statement below.

"Looking back, there were signs. He'd talk about anything...even classified or sensitive information, like a bank closing...anywhere. He didn't care who was around."

Lesson Four: Reporting Procedures

If you suspect a possible insider threat, you must report it. You cannot assume someone else will do so. Every one of us is an owner of security — the security of information, the security of our surroundings, and the security of personnel. We are all responsible for keeping our workplace safe.

A major hurdle that deters people from reporting is the idea that they are wrongly reporting on a colleague. Yet reporting is a way of ensuring your security, the security of your colleagues, and the resources and capabilities of your organization.

Read Scott's statement below.

"I felt like something wasn't right. and I thought I should say something. I just didn't know who I should talk to."

Foreign Visitors

Any of the behaviors discussed throughout this course might be valid triggers prompting you to report them. Also be aware of foreign visitors. Possible threat indicators associated with foreign visitors may include:

- Asking inappropriate questions outside the scope of a visit.
- Attempting to gain access to unauthorized areas.
- Asking for extensive biographical or personal information about FDIC employees or contractors.
- Attempting to separate from the host or assigned escort.
- Providing electronic gifts to FDIC personnel.

Reporting Requirements for All FDIC Personnel

If you suspect insider threat activity, there are various ways you can report it. Which of these reporting methods make sense to you?

Select the appropriate answer(s)

- You can send an email describing your observations to: ITCIP-info@fdic.gov.

- You can speak directly to one of the contacts listed in the ‘Contacts’ section of the ITCIP web site

Feedback Reporting Requirements

Either of these options are correct. You should also tell your supervisor, if appropriate.

If you suspect insider threat activity, it is your responsibility to report it.

Even if you don't suspect insider threat activity, but see a coworker in extreme emotional distress, say something. Extreme stress can make coworkers more vulnerable to insider threat activity, either by being more vulnerable to malicious external influence, or as lone wolves with unpredictable destructive tendencies. Looking out for one another can help mitigate the risk and make the FDIC stronger. If a coworker appears to have serious emotional, financial, or other personal issues, letting ITCIP know can result in your coworker getting the help he or she needs.

Since the inception of the National Insider Threat Task Force through Executive Order 13587, Insider Threat programs have uncovered and stopped suicides as well as information breaches. You can help your colleagues come back from either end.

Failure to Report

Unfortunately, insider threats often go unreported until it is too late. In the majority of past cases, relevant information was available, yet went unreported. How different might things have been had someone said something?

When you fail to report:

- You risk both your physical security and the information security of the FDIC.
- You fail the person who needs help. When you don’t report, you lose the opportunity to help your coworker resolve problems before committing espionage or hurting themselves or others.

Read Regena’s statement below.

"I never thought anything like this could happen. Why didn't someone say something?"

But what if I'm wrong?

Reporting a person or incident does not make the person guilty.

ITCIP personnel are intelligence professionals – not law enforcement – who have access to information resources that you do not. Their job is to look at a potential insider threat situation relative to the whole person and determine the circumstances that may have led to the reportable issue.

Please let these experts use their resources to get to the bottom of a situation, help people who need it, and secure the FDIC.

You cannot underestimate the role you play in protecting against insider threats. You are the first line of defense. If you suspect a potential insider threat, you must report it.

How to Protect Yourself and the FDIC

Protecting Yourself and the FDIC

While you are the first line of defense against insider threats, the FDIC has additional means of protection in place, such as a secure firewall that isolates our network and controls the flow of information to and from the network.

As an authorized user of FDIC equipment and systems to accomplish your work, you are subject to monitoring. You have no reasonable expectation of privacy when using FDIC equipment. Communications using FDIC systems are always the property of the FDIC.

It is always your responsibility to be discreet with information associated with your work and to be aware of possible insider threat indicators.

How might you be targeted during official foreign travel?

During any travel, but especially while on official foreign travel, your host country will know you are coming and be prepared to greet you with maximum surveillance. There are no friendly nations in these situations, where the host country has the opportunity, through overt or clandestine intelligence collection against you, to gain an advantage against the U.S. government.

As FDIC personnel, you will be known to foreign countries as U.S. Government representatives. Your fellow travelers (family, friends, etc.), as a result of their affiliation with you, will also be affiliated with the Federal Government. U.S. Government representatives are always a target of nefarious actors, whether a foreign

intelligence entity or a private citizen with a grudge against our nation and the freedoms we represent.

Common Monitoring Techniques

Common techniques used to monitor travelers include:

- Audio and video coverage of hotel rooms.
- Electronic and physical surveillance.
- Copying traveler's computer and cell phone hard drives.
- Monitoring and collecting all communications, regardless of encryption.
- Requesting sensitive or classified information during casual conversations.
- Breaking into in-room safes.

Protect Yourself and the FDIC During Foreign Travel

Protect yourself and the FDIC during foreign travel by:

- Securing information that is valuable to you and the FDIC. Bring as little with you as required for your meetings.
- Requesting a counterintelligence threat and travel brief from ITCIP before you travel to a foreign country.
- Knowing the contact information for the nearest Consulate or Embassy.
- Consider bringing FDIC loaner equipment only if work communications are absolutely necessary – otherwise, leave all of your devices at home.
- Remaining aware of your surroundings, trusting your instincts, and reporting anything suspicious.

You should NOT:

- Engage in illegal activity in a foreign country. Know the local customs and observe them accordingly (e.g., no gum chewing in Singapore).
- Leave your laptop computer or phone unattended.

- Look for electronic audio or video devices in foreign hotel rooms, restaurants, meeting rooms, or other areas.

This last item may seem counterintuitive, but the reason you should NOT look for surveillance devices is that if you were to find them, your actions or changes in behaviors could tip off your adversaries that you're wise to their ways. This could, in their eyes, increase your value as a possible target.

See "Know the Risk - Raise Your Shield: Travel Awareness" for more information

Before You Travel

When you're planning a vacation abroad, probably the last thing on your mind is identifying your vacation plans to ITCIP. One of the benefits of notification is that ITCIP can provide you with useful resources to help ensure you have a safe journey.

Visit the ITCIP web site before your trip for tips and tricks for staying safe and secure in your travels. Look under the section titled "Foreign Travel: Business and Personal."

Another routine part of your travel preparations should be to register with the State Department in their Smart Traveler Enrollment Program (STEP). STEP is a free service that allows U.S. citizens to enroll with the nearest U.S. embassy or consulate.

By registering with STEP, the State Department will know to look for you and your companions during uneasy times specifically because of your status with the U.S. government and consequently being a potential target.

Hosting Foreign Visitors

If you are responsible for hosting foreign visitors, there are precautions you can take to help keep the FDIC secure. These precautions involve the ethics of gifts as well as hosting, escorting, and briefing foreign visitors. See the brochure entitled: "Counterintelligence: Foreign Visitors at FDIC" for more information. You'll find it under 'Job Aids' at the ITCIP web site.

Applying for Employment Outside of the FDIC

An often forgotten element in the protection of FDIC information is your resume. In your enthusiasm to trumpet your accomplishments, you may inadvertently disclose proprietary information. Some examples include:

- A bank's condition in terms of its CAMELS (**C**apital adequacy, **A**ssets, **M**anagement Capability, **E**arnings, **L**iquidity, **S**ensitivity) ratings.
- Composite ratings.
- Bank asset valuations or sales records.
- Anything non-public regarding the bank regulatory process.
- Any specific information that details your work product. Remember, you do not own the data rights to any work performed on behalf of the FDIC.

Keep in mind that USAJOBS is a public web site, so the information in your resume will be available to a wide audience.

Conclusion

In Conclusion

While it may seem remote, the possibility always exists that a colleague may be an insider threat.

We never want to suspect that a trusted colleague may be the perpetrator of insider threat activities, but sometimes people, through financial hardship, personal distress, or simple naïve friendliness, may find themselves in a precarious position. By reporting your suspicions, you may be enabling a colleague to get help early rather than allowing the situation to escalate.

Look out for each other in a good way — be neighborly and care about the welfare of your colleagues. Care about the safety and security of the FDIC, its assets, its information, and especially its people.

ITCIP Website

Course Completion

Congratulations on completing Insider Threat and Counterintelligence Program (ITCIP).