Fraud and Counterintelligence Concerns

Student Guide

August 2025

Center for Development of Security Excellence

Contents

Lesson 1: Course Introduction

Welcome

Introduction

A federal contractor is hit by a ransomware attack. A trusted contact infects a federal employee's phone with malware. A contracting officer is compromised by promises of lavish compensation, and one company loses millions when a partner sabotages their products, while another has files stolen by a newly purchased subsidiary. These are just some of the consequences that happen every year when federal employees and contractors fall victim to fraud operations, putting our national security at risk.

In this *Fraud and Counterintelligence (CI) Concerns* course, you will investigate each of these fictional scenarios, as well as several real-life case studies, to learn about the risks of fraud from Foreign Intelligence Entities (FIEs) and other adversaries.

Course Objectives:

- Describe fraud and recognize fraud operations.
- Understand how to mitigate the risk of fraud from FIEs.

Lesson 2: Overview of Fraud and CI

Lesson Introduction

Introduction

The United States government is under continual threat from adversaries that operate globally, including here at home. Many national governments and other organizations actively engage in espionage to steal American intelligence and subvert American goals. Fraud provides them several tools to do so. This lesson will introduce you to essential concepts in fraud and counterintelligence, or CI.

Lesson Objectives:

- Explain the threat of fraud by Foreign Intelligence Entities (FIEs).
- Describe common fraud schemes.

CI and Fraud

Defining Counterintelligence

The threat to United States intelligence comes from Foreign Intelligence Entities (FIEs). FIEs are any known or suspected foreign organizations, persons, or groups that conduct intelligence activities against the United States. These groups could be public, private or governmental. They could include foreign intelligence, security services, or international terrorist organizations.

Every year, these entities engage in espionage operations against the United States, acquiring American information, interfering with American intelligence collection, influencing American policy, and disrupting American systems and programs.

To meet the danger from international espionage, federal employees and contractors must engage in counterintelligence. *CI* involves gathering information and conducting activities to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, counterfeiting, sabotage, or assassinations by or on behalf of these foreign adversaries.

Defining Fraud

Many of the ways FIEs attack the United States fall under the umbrella of fraud. Fraud is any activity that relies on deception to achieve a gain. It becomes a crime when the fraudster knowingly misrepresents the truth or conceals material facts to

induce someone else to act to their own detriment. There are many different kinds of fraud. This course will discuss three in particular.

According to 18 United States Code (USC) 1341, the general crime of *fraud* involves devising any scheme to obtain money or property by means of false pretenses, or making and distributing counterfeit money or other items of value. *18 USC 1031: Fraud against the United States* involves schemes to obtain money or property through fraud, in any grant, contract, or other form of federal assistance. This includes actions as a government employee, contractor, vendor, or beneficiary. *18 USC 1343: Wire fraud* involves schemes to obtain money or property using telecommunications, including telephone and the internet.

Schemes and Operations

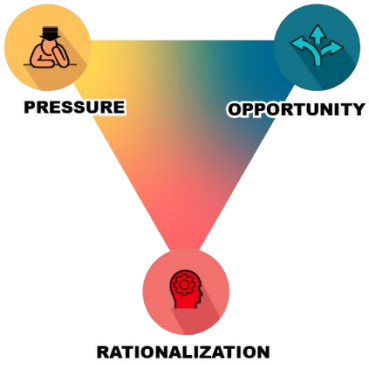
Fraud is carried out using a variety of specific *schemes*, each with their own tactics and goals, and enabled by *operations*.

A fraud scheme is any one of the many kinds of deceptions that can be engineered to obtain something of value. It is the specific deception being used to further the fraudster's goals. For example, an FIE who wants to breach a target's network and take the information they find there could use a *hacking* scheme to do so.

A fraud operation is a specific activity performed in furtherance of a fraud scheme. For example, our hypothetical hacker could use any number of operations to accomplish his goal, including cyber espionage tools like malware or spear phishing tactics.

The Fraud Triangle

Because the threat of fraud can come from individuals or organizations you may trust, an essential part of understanding fraud is learning the motivations people have for deceiving you. The Fraud Triangle is a model that describes the factors that could make someone more likely to commit fraud.



Fraudsters tend to commit fraud when they have *pressure* to do it—like financial pressures or pressures from leaders—*opportunities*—which could be anything from ineffective or poorly enforced laws and policies to poor controls to the availability of suitable targets—and the ability to *rationalize* the rightness of their behavior. Rationalizations are easy to find, like blaming or dehumanizing the victim, denying the existence of the injury, appealing to higher loyalties, posturing as a victim of circumstance, making advantageous comparisons, normalizing the deviance, or diffusing responsibility.

Looking at fraud through the lens of the Fraud Triangle helps us to see that, in the context of CI, fraud is an international organized crime. Using the fraud triangle, we can describe the influences on individuals or groups to commit this crime against our employees, agencies, and companies.

The Emerging Threat Landscape

Many of the fraud operations you will encounter in this course did not exist twenty or thirty years ago. Advancing technologies have provided adversaries with many new techniques to manipulate insiders and reach their objectives. Many of these new tactics involve gaining access to targets' information and using it to carry out more targeted and damaging operations. This course will introduce you to many of these schemes and operations.

Some of the newest emerging threats include deepfakes, poisoning attacks on Artificial Intelligence (AI) programs, and botnets. Adversaries' techniques will continue to evolve so it's important to understand the sources of these emerging threats and their targets, goals, and techniques.

Threat Actors

The threat actors working to commit fraud against the United States include criminal groups, foreign intelligence services, industrial competitors, and activist groups. East Asia and the Pacific and the Near East Regions are the most significant intelligence risks using these new techniques, collectively accounting for 62% of suspicious contacts reported to DCSA in 2023.

Targets

Because global connectivity provides adversaries with almost limitless reach, anyone connected to federal operations could be a target, including government employees, contractors and subcontractors, cleared academics, and associated businesses.

Objectives

Many kinds of information can be valuable for adversaries, not just classified or sensitive information. The objectives of these fraud schemes often involve proprietary information, customer data, or employee data. Other objectives could include ransomware, business email compromise, sabotage, and damage to the target's reputation.

Operations

Many of the most damaging emerging operations involve different forms of *phishing*, as well as face-to-face interaction. Phishing involves using email to impersonate someone the target would trust, while *smishing* involves SMS or text messages and *vishing* involves voice calls.

Learning Activity

Knowledge Check 1

QuikWerks, a company with several federal contracts, is considering using Savva, a foreign-owned company, as a vendor for certain important equipment. Which of the following are potential risks of fraud in this situation?

Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

- ☐ Savva could acquire information about government projects
- ☐ Savva could sabotage QuikWerks' networked systems
- ☐ Savva could acquire information about QuikWerks personnel for future operations
- ☐ Savva could gain access to QuikWerks facilities

Fraud Schemes

Overview of Fraud Schemes

While there are many different fraud schemes FIEs can use, they tend to focus on a handful of specific schemes to maximize their goals of stealing information or causing damage to the United States. This topic will introduce you to a few of the most common fraud schemes, including:

- Identity theft
- Hacking
- Infiltrating organizations

- Manipulating individuals
- Influencing political situations

Each of these schemes can be carried out using any number of fraud operations.

Identity Theft

Identity Theft is any crime in which someone wrongfully obtains and uses a person's personal data in some way that uses fraud and deception. Because identity theft can be committed from anywhere in the world, it's a flourishing criminal industry.

Americans are often familiar with the ways identity theft can happen to an individual, like how credit card information and personal data can allow a fraudster to make large purchases in your name. In the context of CI, identity theft can be used toward other objectives, such as harvesting information or credentials to steal sensitive information, stealing money or other assets from an individual or organization, or infiltrating locations or organizations under an assumed identity to commit crimes or acts of terror.

Hacking

Hacking refers to gaining unauthorized access to digital devices, computer systems, or computer networks. It's one of the most prolific schemes used by adversaries, and the techniques are becoming more sophisticated every year.

In the context of CI, there could be several common objectives. Adversaries can harvest information from their target, directly copying data from a hacked system or network to another location. They could infect the target with viruses or malware by tricking them into installing a prepackaged program that carries out the scheme. They can use ransomware, where opening a seemingly harmless file can lock down a network and hold its information for ransom. Adversaries can also exploit system vulnerabilities to execute code. By finding a way to gain direct access to a networked system, they can enter commands directly to achieve their goals.

Infiltrating Organizations

FIEs and other adversaries can use infiltration to gain access to organizations and their members and resources. They can take on any number of roles to do so, including employees, customers, partners, and students.

In the context of CI, these adversaries can manipulate organizations into giving them direct access to government systems, information, and insiders. It may be difficult to believe that a secure organization could give direct access to FIEs, but it is a

constant risk, and advancing technology gives adversaries more tools than ever to accomplish it.

Consider the following real case of infiltration:

Case Study: KnowBe4

In May 2024, the State Department announced charges against Christina Chapman, who was accused of helping facilitate employment for North Korean nationals. From about October 2020 through October 2023, four agents from North Korea's Munitions Industry Department—Jiho Han, Chunji Jin, Haoran Xu, and their manager Zhonghua—infiltrated a range of sectors and industries and attempted to access positions in U.S. government agencies. They used stolen identities from more than 60 U.S. citizens to obtain the positions – stolen identities that were allegedly provided by Chapman.

The agents were caught when they attempted to infiltrate KnowBe4, a company that provides anti-phishing and security awareness training. The FIE passed the interview and background check processes, and upon receiving their new laptop, they began to install malware.

Fortunately, the malware was detected by the company's security software. When KnowBe4 tried to reach the employee, he claimed to be troubleshooting an issue with his router. In actuality, he had begun trying to install and execute unauthorized software to bypass security and install malware. It sounds like a plot point from a Hollywood movie, but FIEs can and do use fraud to infiltrate U.S. industry.

Manipulating Individuals

Adversaries can use fraud to manipulate organizations or individuals into providing information or taking action against their own organization, often using tactics like spear phishing and other forms of social engineering. In these cases, adversaries are often successful in getting witting or unwitting insiders to take actions the adversaries cannot take themselves, or in building relationships with government insiders, they can later exploit. FIEs manipulate insiders using elicitation tactics.

Elicitation

Elicitation is a structured method of communication used to extract information from people without making them aware they are a collection target. Elicitation can sound like common conversation. The adversary will continually elicit small details over a period of time, piecing them together to form a larger picture.

Elicitation tactics work because people exhibit the same tendencies regardless of the context, allowing adversaries to exploit human nature. That includes using peoples' tendency to complain or willingness to respond to questionnaires and surveys. Adversaries can feign ignorance, lie, flatter, offer quid pro quos, or request paper review. They can use bracketing techniques to infer important details, or goad their target into talking by making oblique references or criticizing the target or their organization.

Influencing Political Situations

FIEs can engage in Foreign Malign Influence (FMI) to influence how Americans think, act, and make decisions using manipulative or criminal means. Some foreign malign actors gather personal information so they can target, influence, and coerce specific individuals or groups. Malign influence agents could be foreign government officials or criminal actors, but they can hide their true affiliations to appear like U.S. citizens, trustworthy news sources, or benevolent participants in America's institutions and processes.

Some foreign governments commit election influence, undertaking efforts to influence the outcome of elections, including Presidential and Congressional races, and voters' opinions. Others try to exacerbate social divisions, while still others question the legitimacy of American institutions or electoral processes as a means of undermining democracy. They have several ways of accomplishing this including influence campaigns, manipulating information, or using authentic American voices, commercial firms, or Artificial Intelligence.

Influence Campaigns

Influence campaigns are long-term efforts by foreign governments to achieve a strategic objective.

Information Manipulation

Malign actors can deploy tactics to alter, modify, or mischaracterize information to shape public views, undermine trust in the authenticity of information, or disrupt democratic decision-making.

Authentic American Voices

Foreign actors often use real Americans to launder their manipulated information. They rely on witting and unwitting Americans to seed, promote, and add credibility to narratives that serve the foreign actors' interests.

Commercial Firms

Malign actors can use marketing and public relations companies, leveraging these firms' expertise in communications and technical sophistication and complicating attribution.

Artificial Intelligence (AI)

AI is being used to quickly and convincingly tailor synthetic content, including audio and video. While individuals are more likely to encounter content purposefully altered by a human, this trend will change as AI technologies continue to advance.

Learning Activities

Knowledge Check 2

Which of the following would be an example of a scheme to *manipulate* a federal employee?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ The adversary exploits a vulnerability in the agency's security software to gain access to encrypted files.
- ○ The adversary impersonates an expert in the employee's field and asks technical questions about a particular federal system.
- ○ The adversary spreads online misinformation about a federal assistance program, leading the public to distrust it.
- ○ The adversary harvests personal data about several employees to use in later operations.

Knowledge Check 3

Which of the following would be an example of a scheme to *infiltrate* an organization?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ The adversary uses malware to gain access to employees' personally identifiable information.
- ○ The adversary impersonates a law enforcement officer to extort a federal contractor with threats of imprisonment.

- ○ The adversary gets a job as a graduate assistant with a cleared academic to work on technical projects.
- ○ The adversary runs a popular vlog giving deceptive commentary about current events.

Knowledge Check 4

Which of the following would be an example of a scheme to commit *identity theft*?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ The adversary elicits information about a sensitive project from a federal employee at a conference.
- ○ The adversary exploits a system vulnerability to sabotage government-owned servers.
- ○ The adversary operates a company that wins a contract to service military equipment overseas.
- ○ The adversary plants malware on an employee's cell phone that collects their login credentials.

Lesson Conclusion

Conclusion

As you just learned, fraud operations can be combined to accomplish any of the fraud schemes we just reviewed. Over the next few lessons, you will review some of the most common types of fraud operations, including cyber espionage, social engineering, bribery and corruption, international law violations, and acquisition fraud.

You have completed the *Overview of Fraud and CI* lesson.

Lesson 3: Cyber Espionage

Lesson Introduction

Introduction

Imagine this scenario: an employee at Navigro, a government contractor, opened a document they thought was an invoice from a vendor. Instead, it contained malware that locked down the company's internal networks. Navigro has fallen victim to a hacking scheme.

As you learned in the previous lesson, these schemes are carried out using *operations*, specific plans that accomplish the scheme's objective. In this lesson, you will learn about cyber espionage operations.

Lesson Objectives:

- Describe common fraud operations.
- Describe best practices for mitigating the risk of fraud.
- Given a scenario and several possible mitigation strategies, select the best practice to mitigate the risk of fraud.

About Cyber Espionage

How Cyber Espionage Works

The internet provides adversaries with tools to commit a wide range of cyber espionage operations. It can be difficult to tell if any email you receive or post you see online is genuine, or if it was generated by a criminal or Foreign Intelligence Entity (FIE).

In 2023, the most recent data year available, cyber actors affiliated with foreign governments were observed scanning networks, spear phishing employees, exfiltrating data, and compromising credentials to target sensitive information. Hacktivist groups have used distributed denial-of-service (DDoS) campaigns to attack industry's unclassified networks, often for financial motives, targeting government and critical infrastructure organizations. Adversaries also frequently use ransomware, where a machine or network is infected with malware that locks information away from the victim until a ransom is paid via wire transfer or digital currency.

Publicly available information on the internet increases the risks. America's adversaries actively exploit social media to monitor accounts, request connections with insiders, elicit information, and recruit assets.

Case Study: Murali Venkata

Now, consider the following case study, which shows the risk cyber operations pose to government information.

Murali Venkata, a former Acting Branch Chief of the Information Technology Division of the Department of Homeland Security (DHS) conspired to steal proprietary U.S. software and databases. His goal was to provide the stolen software and information to software developers in India to develop a commercial version of a case management system to sell to government agencies. A trusted insider, Venkata exfiltrated proprietary source codes and databases from DHS facilities to three servers he set up, providing remote access to his software developers. He and his co-conspirators filled these servers with sensitive law enforcement information and personally identifiable information (PII) of over two-hundred thousand federal employees from the DHS Office of Inspector General and United States Postal Service Office of Inspector General.

When Venkata learned of the investigation, he attempted to obstruct it by deleting incriminating text messages and other communications. In using their access to steal sensitive government information and use it to defraud the United States, Venkata and his co-conspirators put American data where FIEs could access it.

Learning Activity

Which of the following is an example of a cyber espionage operation?

Select all that apply.

- ☐ A DOD employee inserts a USB device into their workstation that plants malware on their computer.
- ☐ A federal contractor's public-facing website is disabled by a distributed denial-of-service attack.
- ☐ An adversary exploits a vulnerability in cybersecurity software to hack directly into a secure network.
- ☐ An adversary calls a DOD employee on their cell phone and pretends to be a journalist.

Mitigating the Risks of Cyber Espionage

Which of the following is an example of a cyber espionage operation?

- ☑ A DOD employee inserts a USB device into their workstation that plants malware on their computer. (correct answer)
- ☑ A federal contractor's public-facing website is disabled by a distributed denial-of-service attack. (correct answer)
- ☑ An adversary exploits a vulnerability in cybersecurity software to hack directly into a secure network. (correct answer)
- ☐ An adversary calls a DOD employee on their cell phone and pretends to be a journalist.

Malware on a USB drive, attacks on websites, and exploiting software vulnerabilities are all common types of cyber operations.

A single mistake or oversight on your part could put your organization's sensitive information at risk. For Navigro, the damage was done as soon as the employee opened the malicious file.

It is vital for organizations to focus on prevention against cyberattacks. Conduct frequent computer audits to monitor for suspicious activity. At minimum, these must be conducted weekly, but ideally they should be done daily. If you detect any intrusion attempts, report them immediately. Don't rely solely on firewalls to protect against attacks. Many of the best defenses are behaviors, not technology. Avoid responding to unknown requests for information. These requests must be reported. In the event of a severe cyberattack, disconnect your computer systems temporarily to limit the damage. Document policies and procedures for protecting sensitive information in a Technology Control Plan (TCP).

Learning Activities

Knowledge Check 1

Consider the ransomware scenario. Which of the following mitigation tactics would be useful for Navigro in avoiding the risk of attacks like this one?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Do not use the internet to send and receive documents like invoices.
- ☐ Avoid responding to unknown requests for information, and report them instead.

- ☐ In the event of a severe cyberattack, disconnect your computer systems temporarily to limit the damage.
- ☐ Do not rely solely on firewalls to protect against attacks. Many of the best defenses are behaviors, not technology.

Knowledge Check 2

Which of the following would be good examples of effective counterespionage mitigation tactics?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ A new federal contractor develops a Technology Control Plan to describe how to control access to secured information systems.
- ☐ After receiving a suspicious email, a DOD employee forwards it to the designated information security personnel.
- ☐ A federal agency conducts audits of their computers and networks once per month.
- ☐ A federal employee downloads a new productivity app to their government mobile device that they heard about on social media.

Lesson Conclusion

Conclusion

Cyber espionage is one of the most common counterintelligence concerns, and the potential risks only increase with time.

You have completed the *Cyber Espionage* lesson.

Lesson 4: Social Engineering

Lesson Introduction

Introduction

Consider Grant, a policy analyst within the Department of Defense (DOD). Grant was recently contacted by someone purporting to be a political adviser in an allied nation. They began exchanging emails, and Grant was happy to provide context for DOD policy requirements.

This scenario is just one of countless ways Foreign Intelligence Entities (FIEs) and other adversaries can manipulate insiders into assisting them. In this lesson, you will learn about social engineering operations.

Lesson Objectives:

- Describe common fraud operations.
- Describe best practices for mitigating the risk of fraud.
- Given a scenario and several possible mitigation strategies, select the best practice to mitigate the risk of fraud.

About Social Engineering

How Social Engineering Works

Social engineering is a form of online manipulation where an adversary impersonates another person to obtain something fraudulently, including information or access. Common assumed identities used in social engineering include journalists, academic scholars, think tank researchers, government officials, law enforcement, and web administrators.

Social engineering often preys on individuals' ignorance. Targets like Grant often discount the threat posed by social engineering campaigns, either because they don't see their research and communications as being sensitive, or because they're not aware of how these efforts fuel broader cyber espionage efforts. However, FIEs rely heavily on the intelligence they gain from compromising policy analysts. Adversaries also create and prey on a sense of urgency by posing as authorities, including law enforcement officials or prosecutors, threatening victims with arrest or violence. They may show victims fraudulent documents as proof of their accusations, like realistic arrest warrants or intricate details about alleged criminal schemes. They

may also display basic knowledge of the victim to appear more legitimate. Using these operations as tools for extortion, adversaries can use social engineering to fund other fraud activities.

Focus: Spear Phishing

Spear phishing is a type of social engineering where an attacker impersonates other individuals or entities to influence a specific target. Grant in our scenario was a victim of spear phishing, because the adversary crafted a particular persona to influence Grant specifically. When adversaries use publicly available information to craft a persona, this can be a sophisticated tactic.

In 2023, state-sponsored cyber actors in Europe and Eurasia used phishing techniques and government network protocol vulnerabilities to conduct a large-scale phishing campaign, gaining access to user email accounts and cleared industry information. They sent a phishing email to cleared industry employees that, when clicked, enabled access to vulnerable employees' email. Due to a lack of strict network protocols, any employee not enrolled in multi-factor authentication was vulnerable.

Case Study: Kimusky Operations

Now, consider the following case study, which shows the risk social engineering poses to government information.

The government of the Democratic Peoples' Republic of Korea (DPRK) is a major social engineering risk. Cyber actors from the DPRK like Kimsuky engage in large-scale social engineering campaigns. Kimsuky is a state-backed hacker group. Kimsuky actors use spear phishing as one of their primary tactics for compromising a target's devices and networks.

The spear phishing campaign begins with broad research and preparation, using open-source information to identify potential targets of value and tailor online personas to appear more realistic and appealing to their victims. The actors then create email addresses that resemble the addresses of real individuals they intend to impersonate. They generate domains to host the malicious content the message directs to, often using domains that resemble common internet services and media sites. The cyber actors commonly impersonate well-known news outlets and journalists or other real people to gain trust and establish rapport with their digital targets. A single actor can use multiple personas. Once the cyber actors have engaged with their target, they attempt to compromise the account, device, or network by pushing malicious content in the form of a macro embedded in a text

document. These macros, when enabled, quietly establish connections with Kimsuky command and control infrastructure and provide access to the target's device.

Learning Activity

Which of the following could be an example of a social engineering operation?

Select all that apply.

- ☐ A federal contractor receives an urgent messages from someone identifying themselves as an IRS auditor, instructing them to immediately submit financial documentation.
- ☐ A DOD employee receives a social media message from a college acquaintance inviting them to follow a link to apply to a position at their company.
- ☐ A federal employee receives an email from an investigative journalist asking them to provide information about the agency's finances.
- ☐ An agency director receives an email from an ex-colleague asking them to consider the attached resumes of several potential job candidates.

Mitigating the Risks of Social Engineering

Which of the following could be an example of a social engineering operation?

- ☑ A federal contractor receives an urgent messages from someone identifying themselves as an IRS auditor, instructing them to immediately submit financial documentation. (correct answer)
- ☑ A DOD employee receives a social media message from a college acquaintance inviting them to follow a link to apply to a position at their company. (correct answer)
- ☑ A federal employee receives an email from an investigative journalist asking them to provide information about the agency's finances. (correct answer)
- ☑ An agency director receives an email from an ex-colleague asking them to consider the attached resumes of several potential job candidates. (correct answer)

The IRS auditor, the college acquaintance, the investigative journalist, and the resumés could easily all be social engineering operations, whether they seem plausible or not.

In Grant's case, once his contact had built trust with him, they sent Grant a link to review a white paper. The link instead downloaded malware to Grant's device and began siphoning away sensitive government data. Depending on the data exposed, the damage could be catastrophic.

Because of the risks of social engineering, it is vital that all efforts be taken to verify the identity of anyone attempting to contact federal employees. All personnel should be trained and prepared to take the following steps:

- Be wary of unsolicited messages, regardless of the sender.
- Do not provide information to an unknown person with unusual or heightened interest, specifically a person without a need to know.
- Do not click or download anything without first verifying the source.
- Limit what you post on social media.
- Use the strongest possible privacy settings on social media.
- Report suspicious contacts immediately, every time.

Learning Activities

Knowledge Check 1

Consider the spear phishing scenario. Which of the following mitigation tactics would be useful for Grant in avoiding the risk of attacks like this one?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Be wary of unsolicited messages.
- ☐ Forward the email to colleagues to get their opinion.
- ☐ Do not click or download anything without first verifying the source.
- ☐ Do not provide information to any individual with an unusual or heightened interest.

Knowledge Check 2

Which of the following would be good examples of effective counterespionage mitigation tactics?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ A federal employee on a trip overseas provides daily social media updates with images.
- ☐ A federal employee includes only vague position responsibilities on their LinkedIn profile.

- ☐ A DOD employee responds to a suspicious email, accusing the sender of being a Foreign Intelligence Entity.
- ☐ A contractor receives a suspicious request for proposal from a potential customer and forwards it to their Facility Security Officer (FSO).

Lesson Conclusion

Conclusion

Social engineering preys on our trust, our ignorance, and our urgency. You must always be vigilant.

You have completed the *Social Engineering* lesson.

Lesson 5: Bribery and Corruption

Lesson Introduction

Introduction

Consider Beth. Beth is a contracting officer with a federal agency. Her office is investigating billing issues with Sklodowska Limited, a foreign-owned contracting company. On a call with the company, the chief financial officer explains several innocent errors that led to the discrepancies, at the same time that he casually mentions a few well-paid positions opening at the company for people with Beth's skillset.

Bribery and corruption are useful tools for adversaries to support and protect their fraud schemes, manipulating federal employees and contractors with offers of cash, jobs, expensive trips, and other items of value. In this lesson you'll learn about bribery and corruption, and how to mitigate the risks.

Lesson Objectives:

- Describe common fraud operations.
- Describe best practices for mitigating the risk of fraud.
- Given a scenario and several possible mitigation strategies, select the best practice to mitigate the risk of fraud.

About Bribery and Corruption

How Corruption Works

Foreign Intelligence Entities (FIEs) may attempt to *corrupt* federal personnel, or influence them to use their positions dishonestly, to support their criminal enterprises They use forms of corruption such as bribery—offering items of value like expensive trips, dinners, or cash bonuses in exchange for official action—or embezzlement, where the insider takes government funds for themselves. Using these techniques, they can influence national and international authorities to ignore or assist in their activities. Corruption is prevalent, if not the norm, in certain societies, making any interaction with parties in those places risky.

Case Study: Robert Gilbeau

Consider the following case study, which shows the risk bribery and corruption pose to the government.

In May, 2017, U.S. Navy Rear Admiral Robert Gilbeau was sentenced to 18 months in prison for lying to investigators, concealing his 20-year relationship with Leonard Glenn Frances, or “Fat Leonard.” Frances was the owner of Glenn Defense Marine Asia (GDMA) a foreign defense contractor providing ship-husbanding services such as trash and sewage removal, food, water, security, and fuel to Navy ships making port calls in the Asia/Pacific region. Frances was at the center of the largest corruption scandal in the U.S. Navy in the 2000s and 2010s, involving bribery and conspiracy to commit bribery and defraud the United States.

In August, 2010, after he was promoted to admiral, Gilbeau assumed command of the Defense Contract Management Agency International, where he was responsible for the global administration of DOD’s most critical contracts performed outside the United States. In connection with his plea, Gilbeau admitted that he lied to agents from the Defense Criminal Investigative Service (DCIS) and the Naval Criminal Investigative Service (NCIS) when they asked if he had received any gifts from Frances. He claimed he had always paid for half of the dinners when he and Frances met about three times a year, but this was a lie.

In September, 2013, when Gilbeau became aware that Frances and others had been arrested in connection with fraud and bribery offenses, he destroyed documents and deleted computer files to obstruct the investigation.

Learning Activity

Which of the following could be an example of bribery and corruption?

Select all that apply.

- ☐ A federal employee investigating manufacturing issues at an aerospace company is invited to an all-expenses-paid fact-finding trip to the company’s headquarters.
- ☐ A contracting officer reviewing a company’s bid is invited to dinner by the company to discuss key details of the project.
- ☐ A federal employee attends a conference in an allied nation and all attendees are offered discounts on a sponsoring company’s products.
- ☐ A technical analyst with a federal contractor is offered a cash bonus to review details of another company’s project.

Mitigating the Risk of Bribery and Corruption

Which of the following could be an example of bribery and corruption?

- ☑ A federal employee investigating manufacturing issues at an aerospace company is invited to an all-expenses-paid fact-finding trip to the company's headquarters. (correct answer)
- ☑ A contracting officer reviewing a company's bid is invited to dinner by the company to discuss key details of the project. (correct answer)
- ☐ A federal employee attends a conference in an allied nation and all attendees are offered discounts on a sponsoring company's products.
- ☑ A technical analyst with a federal contractor is offered a cash bonus to review details of another company's project. (correct answer)

FIEs target specific individuals for bribery and corruption; expensive trips, dinners, and cash bonuses are common bribes that they offer.

Let's check in on Beth. Soon after she closes the investigation of Sklodowska Limited, she retires from her civil service position and accepts a highly compensated consulting role with the company. Her agency may or may not look into the circumstances of her departure and whether Sklodowska continues their suspicious practices.

Organizations have a better chance of preventing or addressing bribery and corruption if they use the Fraud Triangle to plan their policies and practices. Using the triangle, organizations can remove opportunities, minimize motivations and pressures, and remove rationalizations to participate in fraud.

Remove Opportunities

To stop fraud and prevent future fraud from occurring, organizations should commit to removing opportunities for fraud. They can do so by implementing preventive and detective internal controls, a fraud reporting system, anti-fraud education for employees, and employee background checks.

Minimize Motivations

To minimize the motivations and pressures employees have to commit fraud, organizations should establish an open-door policy with employees, measure employee attitudes about anti-fraud efforts, and establish a system of disciplinary measures for fraud.

Remove Rationalizations

To remove the rationalizations that employees use to justify fraud, organizations should communicate and adhere to clear, core ethical values, educate employees about the impacts of fraud, and make it easier for employees to act ethically.

Learning Activities

Knowledge Check 1

Consider the bribery scenario. Which of the following mitigation tactics would be useful for Beth's office in avoiding the risk of bribery and corruption?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Limiting open discussion of bribery and corruption in the office, since it could encourage the behavior
- ☐ Establishing an open-door policy between managers and employees to address ethical or behavioral concerns
- ☐ Ensuring personnel are current on anti-fraud and bribery training
- ☐ Clearly communicating the core ethical values of the organization

Knowledge Check 2

Which of the following describe the correct use of mitigation tactics against bribery and corruption?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ A team lead in a federal office schedules time during a meeting to discuss the risks of bribery.
- ☐ Federal contractors who communicate with foreign-owned companies are not provided with any training about bribery.
- ☐ A federal contracting company provides a clear reporting process for employees to address bribery concerns.
- ☐ A federal office posts a warning about bribery and corruption in a heavily trafficked area.

Lesson Conclusion

Conclusion

All organizations should have a clear understanding of the risks and consequences of bribery and corruption.

You have completed the *Bribery and Corruption* lesson.

Lesson 6: International Law Violations

Lesson Introduction

Introduction

Consider this scenario. Gravonics is a company with several contracts with the Department of Defense (DOD). Gravonics also does business with several other companies overseas. They recently started subcontracting with a company in Southeast Asia that provides electronic components. These components are integrated into communication equipment that Gravonics supplies to the U.S. military.

Working with foreign-owned companies comes with its share of risks. Foreign-owned companies can operate as fronts for fraud operations sponsored by foreign governments. In this lesson you'll learn about the fraud risks of international law violations, and how to mitigate those risks.

Lesson Objectives:

- Describe common fraud operations.
- Describe best practices for mitigating the risk of fraud.
- Given a scenario and several possible mitigation strategies, select the best practice to mitigate the risk of fraud.

About International Law Violations

How International Law Violations Work

Some governments engage directly in international fraud by producing fraudulent currency or products to help finance their operations and gain access to complex systems. FIEs use a range of fraudulent international operations to achieve their goals, including money laundering and the exploitation of supply chains.

Money Laundering

Money laundering is conducting or attempting to conduct a financial transaction, knowing that the property involved represents the proceeds of unlawful activity. Money laundering is an essential part of ongoing criminal enterprises and terrorist operations. It's used to disguise the nature, location, source, and ownership of the profits from the crime and to avoid transaction reporting requirements.

Hundreds of billions – maybe even trillions – of dollars are estimated to be laundered every year, and while there are global requirements to detect money laundering, as much as 91-99% of funds go undetected. Foreign Intelligence Entities (FIEs) and other adversaries can also use cryptocurrency and other digital assets to launder money and fund their operations, either directly, through crypto fraud, or indirectly, by providing unregulated destinations for money. Digital currencies play a large part in the cybercrime and fraud worlds and allow criminal organizations to fund operations, launder or transfer money, or hold information for ransom.

Exploiting Supply Chains

FIEs and other adversaries can exploit and compromise global supply chains by introducing counterfeit or malicious products into the supply chain to gain unauthorized access to protected data, alter data, disrupt operations, or interrupt communication.

Successful exploitation of supply chains enables foreign agents to manipulate DOD system components, degrade DOD capabilities and effectiveness during potential conflicts, or gain access to Controlled Unclassified Information (CUI). An FIE with insider access could introduce malicious changes or substitutions with a nonconforming part during any phase in the supply chain, making it more difficult to identify the fraud.

Case Study: Office 39

Now, consider the following case study, which shows the risk international fraud poses to government information.

The government of the Democratic Peoples' Republic of Korea (DPRK) is actively engaged in money laundering and other international crimes to supplement its national income, and often uses its struggling citizens as participants. The DPRK's Office 39 operates an organized crime network coordinating many schemes, including counterfeiting U.S. one-hundred-dollar bills. Other crimes include industrial espionage, cybercrime, extortion, theft, deception, and smuggling prohibited goods.

The regime's operatives often conduct covert activities under the guise of legitimate business operations, making it difficult to identify and disrupt their efforts. For example, they often launder money by trading high-value luxury goods. In this way individuals and organizations around the world can be part of their fraud schemes without even knowing it.

Learning Activity

Which of the following would be good examples of international law violations by foreign governments?

Select all that apply.

- ☐ A foreign-owned contracting company produces networked devices that surreptitiously collect information about the systems they are part of.
- ☐ A federal contracting company's foreign-owned subcontractor produces adulterated medications to sell cheaply in foreign markets.
- ☐ A foreign-owned company under consideration for a federal contract provides accurate financial documentation as part of the approval process.
- ☐ An organization receiving federal grants shifts uses crypto markets to hide the source of their income.

Mitigating the Risk of International Law Violations

Which of the following would be good examples of international law violations by foreign governments?

- ☑ A foreign-owned contracting company produces networked devices that surreptitiously collect information about the systems they are part of. (correct answer)
- ☑ A federal contracting company's foreign-owned subcontractor produces adulterated medications to sell cheaply in foreign markets. (correct answer)
- ☐ A foreign-owned company under consideration for a federal contract provides accurate financial documentation as part of the approval process.
- ☑ An organization receiving federal grants shifts uses crypto markets to hide the source of their income. (correct answer)

Frequent, unclear money transfers can be a good indicator of fraud, and money laundering and supply chain schemes can lead to severe consequences for careless companies.

Let's check in with Gravonics. Their product testing has revealed that their recent foreign subcontractor has tampered with new electronics components to reduce the effectiveness of Gravonics equipment. This resulted in a loss of millions of dollars for the company.

Any organization that interacts with foreign business operations runs the risk of participating in international fraud, wittingly or unwittingly. These organizations should perform fraud risk assessments guided by the behavioral factors outlined in the fraud triangle. Risk assessments are the starting point for determining a well-

designed compliance program. They demonstrate the organization's understanding of its risk and whether they have the appropriate tools, systems, and resources to mitigate those risks. Because state-sponsored fraud can often appear as legitimate business activity, per the Department of Justice's *Evaluation of Corporate Compliance Programs,* and the Securities and Exchange Commission's (SEC's) guidance on the Foreign Corrupt Practices Act, organizations with relationships to third-party organizations and vendors must understand:

- The types of conduct governed by the guiding regulations, pursuant to the organization's risk profile
- The theories of legal liability for third-party misconduct and/or levels of intent
- The types of red flags and risk indicators commonly associated with third-party risk
- How the strength of internal controls can serve to potentially mitigate liability for misconduct
- The importance of documenting third-party relationships from the business purpose through contract completion

Learning Activities

Knowledge Check 1

Think back on the Gravonics scenario. Which of the following mitigation tactics would help Gravonics avoid the risk of participating in international fraud?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Establishing a clear process for profiling the potential risk of a contract with a foreign-owned company
- ☐ Providing training for employees to recognize red flags associated with fraud
- ☐ Understanding the company's limitations in detecting and responding to potential fraud
- ☐ Refraining from interacting with any foreign-owned companies.

Knowledge Check 2

Which of the following describe the correct use of mitigation tactics against international law violations?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ The owner of a federal contracting company delegates risk assessment to a single unit so the other members of the company don't have to worry about it.
- ☐ A federal contracting company hires a trusted third-party agency to assess the risks of a partnership with a foreign-owned company.
- ☐ A federal contracting company signing a contract with a vendor includes a clause that the vendor must submit to regular financial reviews.
- ☐ A cleared academic developing equipment for satellites requires the foreign-owned vendor to disclose the sources of all parts and materials to be used.

Lesson Conclusion

Conclusion

Agencies and companies should carefully weigh the risks against the benefits of working with foreign-owned companies.

You have completed the *Bribery and Corruption* lesson.

Lesson 7: International Law Violations

Lesson Introduction

Introduction

Now, consider this scenario: Kronosale is a company with several active federal contracts. They have just purchased a foreign-owned company, Saela. After a regular audit, the Department of Defense (DOD) discovers that Saela has less value and does less business than they initially reported. It's unclear what else Kronosale doesn't know about Saela.

Because of the many risks of international fraud in foreign-owned businesses, companies that purchase businesses engaged in fraud are legally responsible for the behavior of their subsidiaries. In this lesson, you will learn about the risks of acquisition fraud.

Lesson Objectives:

- Describe common fraud operations.
- Describe best practices for mitigating the risk of fraud.
- Given a scenario and several possible mitigation strategies, select the best practice to mitigate the risk of fraud.

About Acquisition Fraud

How Acquisition Fraud Works

Business mergers and acquisitions are common throughout the world, and they can be used by fraudsters as tools for corruption and fraud, or to hide fraud. These acquisitions become a *counterintelligence* risk when the corruption and fraud are perpetrated by Foreign Intelligence Entities (FIEs) to accomplish a larger scheme.

Depending on the business sector and nation of origin, corporations could be exposed to a high risk of corruption and fraud. FIEs can use many tactics to persuade witting or unwitting insiders into doing business. Often the selling company presents fraudulent information to the purchasing company, including inflated financial projections and doctored records showing the company has more assets or revenue than it really does. Selling companies may cover up evidence of pre-existing fraud or corruption. If FIEs have an inside contact, they may also offer

positions, compensation, or other payment in return for assistance in completing the acquisition or procurement process.

Case File: Chinese FDI

Now, consider the following case study, which shows the risks corporate acquisitions can pose to U.S. interests. Many fast-growing global markets, such as the Peoples' Republic of China (PRC) are targets for Foreign Direct Investment (FDI) where multinational corporations acquire local businesses to do business in that market. Because the government of the PRC exercises a high degree of control over Chinese companies, American corporations in the PRC are often forced to engage with government officials and intelligence entities without realizing it. The government of the PRC promotes direct investment in its economy. It also prioritizes the acquisition and theft of intellectual property from other nations to bolster its technological development, often forcing American companies to sign intellectual property sharing agreements. They are also known to punish companies that attempt to perform due diligence during the acquisition process. In this way, any direct investment in businesses in the PRC has the potential to create an intelligence risk, leading to the theft of American technologies.

Learning Activity

Consider a situation in which a foreign-owned company is in the process of being bought by an American company. Which of the following could be examples of acquisition fraud?

Select all that apply.

- ☐ The foreign-owned company offers several high-value gifts to American representatives during the acquisition process.
- ☐ The foreign-owned company reports revenues that aren't clearly accounted for by business operations.
- ☐ The American company finds discrepancies in the reported value of the foreign-owned company's assets.
- ☐ The American company is encouraged to reduce the time spent conducting due diligence to meet an urgent timeline.

Mitigating the Risk of Acquisition Fraud

Consider a situation in which a foreign-owned company is in the process of being bought by an American company. Which of the following could be examples of acquisition fraud?

- ☑ The foreign-owned company offers several high-value gifts to American representatives during the acquisition process. (correct answer)
- ☑ The foreign-owned company reports revenues that aren't clearly accounted for by business operations. v
- ☑ The American company finds discrepancies in the reported value of the foreign-owned company's assets. (correct answer)
- ☑ The American company is encouraged to reduce the time spent conducting due diligence to meet an urgent timeline. (correct answer)

High-value gifts, discrepancies in financial documentation, and resistance to due diligence are all important signs that a business acquisition may be fraudulent.

Let's check in on Kronosale. After an internal investigation, the company finds that Saela has been able to access files from several of Kronosale's federal projects.

Organizations engaged in acquisitions, contracts, or procurements with international corporations must perform due diligence in every step of the process. By including fraud examiners and analytical tools both before and after the transaction, organizations can be better positioned to detect fraud and intelligence risks.

Specifically, organizations should have internal control processes in place and supported by management to regularly monitor whether the company's reporting and compliance objectives are being met. These objectives and processes must be clearly communicated to the organization and enable management to identify and analyze risks both internal to the organization and from external parties with which the organization interacts.

Learning Activities

Knowledge Check 1

Consider the Kronosale scenario. Which of the following mitigation tactics would be useful for Kronosale in avoiding the risk of acquisition fraud?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Communicating with employees about the goals and processes of the acquisition

- ☐ Involving trained analysts in the due diligence process during and after the acquisition
- ☐ Identifying the most up-to-date analytical tools and integrating them into the process
- ☐ Implementing internal controls that involve continuous monitoring of Saela's finances

Knowledge Check 2

Which of the following describe the correct use of acquisition fraud mitigation tactics?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ A federal contracting company conducts frequent audits of a recently purchased company's supply chain.
- ☐ The owner of the American company involves personnel from several functional areas in assessing the risk of the company they are acquiring.
- ☐ A federal contracting company requests guidance from the DOD to properly assess risk in a business acquisition.
- ☐ The owner of the American company relies entirely on third-party analysis services so that internal personnel do not have to engage in the process.

Lesson Conclusion

Conclusion

Companies in the Defense Security Enterprise must take strong precautions against fraudsters that would abuse the business relationship.

You have completed the *Acquisition Fraud* lesson.

Lesson 8: Course Conclusion

Course Conclusion

Course Review

In this course, you learned about some of the ways Foreign Intelligence Entities, or FIEs, and other adversaries perpetrate fraud against American agencies and contractors. Fraud is any activity that relies on deception to achieve a gain, and our nation's information is under constant assault. The fraud triangle describes the motivations of adversaries and insiders to commit fraud, helping organizations to anticipate and avoid fraud schemes and operations. Cyber operations, social engineering, bribery and corruption, international criminal activity, and acquisition fraud are just some of the ways our adversaries gain access to systems, operations, information, and resources.

Course Summary

Congratulations! You have completed the *Fraud and Counterintelligence Concerns* course.

You should now be able to perform all of the listed activities.

- Describe fraud and recognize fraud operations.
- Understand how to mitigate the risk of fraud from FIEs.

To receive course credit, you must take the *Fraud and Counterintelligence Concerns* examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to access the online exam.

Appendix A: Answer Key

Lesson 2 Learning Activities

Knowledge Check 1

QuikWerks, a company with several federal contracts, is considering using Savva, a foreign-owned company, as a vendor for certain important equipment. Which of the following are potential risks of fraud in this situation?

- ☑ Savva could acquire information about government projects (correct answer)
- ☑ Savva could sabotage QuikWerks' networked systems (correct answer)
- ☑ Savva could acquire information about QuikWerks personnel for future operations (correct answer)
- ☑ Savva could gain access to QuikWerks facilities (correct answer)

***Feedback**: These are all potential risks of fraud from this business relationship.*

Knowledge Check 2

Which of the following would be an example of a scheme to *manipulate* a federal employee?

- ○ The adversary exploits a vulnerability in the agency's security software to gain access to encrypted files.
- ⊙ The adversary impersonates an expert in the employee's field and asks technical questions about a particular federal system. (correct answer)
- ○ The adversary spreads online misinformation about a federal assistance program, leading the public to distrust it.
- ○ The adversary harvests personal data about several employees to use in later operations.

***Feedback**: An adversary using fraud against a particular employee to gain information is an example of a manipulation scheme.*

Knowledge Check 3

Which of the following would be an example of a scheme to *infiltrate* an organization?

- ○ The adversary uses malware to gain access to employees' personally identifiable information.

- ○ The adversary impersonates a law enforcement officer to extort a federal contractor with threats of imprisonment.
- ⊙ The adversary gets a job as a graduate assistant with a cleared academic to work on technical projects. (correct answer)
- ○ The adversary runs a popular vlog giving deceptive commentary about current events.

***Feedback**: An adversary using fraud to gain direct access to facilities and information is an example of an infiltration scheme.*

Knowledge Check 4

Which of the following would be an example of a scheme to commit *identity theft*?

- ○ The adversary elicits information about a sensitive project from a federal employee at a conference.
- ○ The adversary exploits a system vulnerability to sabotage government-owned servers.
- ○ The adversary operates a company that wins a contract to service military equipment overseas.
- ⊙ The adversary plants malware on an employee's cell phone that collects their login credentials. (correct answer)

***Feedback**: Collecting the employee's credentials to allow the adversary to impersonate the employee is an example of identity theft.*

Lesson 3 Learning Activities

Knowledge Check 1

Consider the ransomware scenario. Which of the following mitigation tactics would be useful for Navigro in avoiding the risk of attacks like this one?

- ☐ Do not use the internet to send and receive documents like invoices.
- ☑ Avoid responding to unknown requests for information, and report them instead. (correct answer)
- ☑ In the event of a severe cyberattack, disconnect your computer systems temporarily to limit the damage. (correct answer)
- ☑ Do not rely solely on firewalls to protect against attacks. Many of the best defenses are behaviors, not technology. (correct answer)

***Feedback**: Navigro should not rely solely on firewalls, should avoid responding, and disconnect their systems in the event of an attack.*

Knowledge Check 2

Which of the following would be good examples of effective counterespionage mitigation tactics?

- ☑ A new federal contractor develops a Technology Control Plan to describe how to control access to secured information systems. (correct answer)
- ☑ After receiving a suspicious email, a DOD employee forwards it to the designated information security personnel. (correct answer)
- ☐ A federal agency conducts audits of their computers and networks once per month.
- ☐ A federal employee downloads a new productivity app to their government mobile device that they heard about on social media.

Feedback*: Good information security includes using your TCP and reporting suspicious messages to appropriate personnel.*

Lesson 4 Learning Activities

Knowledge Check 1

Consider the spear phishing scenario. Which of the following mitigation tactics would be useful for Grant in avoiding the risk of attacks like this one?

- ☑ Be wary of unsolicited messages. (correct answer)
- ☐ Forward the email to colleagues to get their opinion.
- ☑ Do not click or download anything without first verifying the source. (correct answer)
- ☑ Do not provide information to any individual with an unusual or heightened interest. (correct answer)

Feedback*: It is important to be cautious with suspicious contacts and to report them immediately.*

Knowledge Check 2

Which of the following would be good examples of effective counterespionage mitigation tactics?

- ☐ A federal employee on a trip overseas provides daily social media updates with images.
- ☑ A federal employee includes only vague position responsibilities on their LinkedIn profile. (correct answer)

- ☐ A DOD employee responds to a suspicious email, accusing the sender of being a Foreign Intelligence Entity.
- ☑ A contractor receives a suspicious request for proposal from a potential customer and forwards it to their Facility Security Officer (FSO). (correct answer)

***Feedback**: Be cautious with the information you share online, and do not reply to suspicious contacts – report them instead.*

Lesson 5 Learning Activities

Knowledge Check 1

Consider the bribery scenario. Which of the following mitigation tactics would be useful for Beth's office in avoiding the risk of bribery and corruption?

- ☐ Limiting open discussion of bribery and corruption in the office, since it could encourage the behavior
- ☑ Establishing an open-door policy between managers and employees to address ethical or behavioral concerns (correct answer)
- ☑ Ensuring personnel are current on anti-fraud and bribery training (correct answer)
- ☑ Clearly communicating the core ethical values of the organization (correct answer)

***Feedback**: Establishing an open-door policy, ensuring personnel are current on training, and communicating the organization's values are all important measures.*

Knowledge Check 2

Which of the following describe the correct use of mitigation tactics against bribery and corruption?

- ☑ A team lead in a federal office schedules time during a meeting to discuss the risks of bribery. (correct answer)
- ☐ Federal contractors who communicate with foreign-owned companies are not provided with any training about bribery.
- ☑ A federal contracting company provides a clear reporting process for employees to address bribery concerns. (correct answer)
- ☑ A federal office posts a warning about bribery and corruption in a heavily trafficked area. (correct answer)

***Feedback**: Organizations should focus on clear communication, training, and processes to prevent corruption.*

Lesson 6 Learning Activities

Knowledge Check 1

Think back on the Gravonics scenario. Which of the following mitigation tactics would help Gravonics avoid the risk of participating in international fraud?

- ☑ Establishing a clear process for profiling the potential risk of a contract with a foreign-owned company (correct answer)
- ☑ Providing training for employees to recognize red flags associated with fraud (correct answer)
- ☑ Understanding the company's limitations in detecting and responding to potential fraud (correct answer)
- ☐ Refraining from interacting with any foreign-owned companies.

***Feedback**: Clear processes, training, and strategy can help companies to avoid international fraud.*

Knowledge Check 2

Which of the following describe the correct use of mitigation tactics against international law violations?

- ☐ The owner of a federal contracting company delegates risk assessment to a single unit so the other members of the company don't have to worry about it.
- ☑ A federal contracting company hires a trusted third-party agency to assess the risks of a partnership with a foreign-owned company. (correct answer)
- ☑ A federal contracting company signing a contract with a vendor includes a clause that the vendor must submit to regular financial reviews. (correct answer)
- ☑ A cleared academic developing equipment for satellites requires the foreign-owned vendor to disclose the sources of all parts and materials to be used. (correct answer)

***Feedback**: Third-party risk assessment and contractual requirements can be useful steps toward mitigating risk.*

Lesson 7 Learning Activities

Knowledge Check 1

Consider the Kronosale scenario. Which of the following mitigation tactics would be useful for Kronosale in avoiding the risk of acquisition fraud?

- ☑ Communicating with employees about the goals and processes of the acquisition (correct answer)
- ☑ Involving trained analysts in the due diligence process during and after the acquisition (correct answer)
- ☑ Identifying the most up-to-date analytical tools and integrating them into the process (correct answer)
- ☑ Implementing internal controls that involve continuous monitoring of Saela's finances (correct answer)

***Feedback**: All of these would be useful tactics to mitigate the risks.*

Knowledge Check 2

Which of the following describe the correct use of acquisition fraud mitigation tactics?

- ☑ A federal contracting company conducts frequent audits of a recently purchased company's supply chain. (correct answer)
- ☑ The owner of the American company involves personnel from several functional areas in assessing the risk of the company they are acquiring. (correct answer)
- ☑ A federal contracting company requests guidance from the DOD to properly assess risk in a business acquisition. (correct answer)
- ☐ The owner of the American company relies entirely on third-party analysis services so that internal personnel do not have to engage in the process.

***Feedback**: The organization should be actively engaged in due diligence in every stage.*