Insider Threat Records Checks

Student Guide

June 2024

Center for Development of Security Excellence

Lesson 1: Course Introduction

Introduction

Welcome

Financial debt. Past due mortgage. An unsolicited LinkedIn message. Connections with a scientist working for a Chinese "think tank." An insider threat.

Reporter:
"The man standing on the right in the yellow shirt is Kevin Mallory, who once held the top-secret security clearance while working for the CIA and the Defense Intelligence Agency. Footage from a surveillance camera at a Virginia FedEx store in April last year caught him as he prepared to hand a clerk stacks of classified documents to be scanned onto an SD card."

Welcome to the Insider Threat Records Checks course! This course describes how records checks support the identification of anomalous behavior associated with insider threats like Kevin Mallory and allow Insider Threat Programs the opportunity to mitigate the risks these threats pose.

Objectives

Here are the course objectives. Take a moment to review them.

- Explain how records checks support the identification of anomalous behavior associated with potential insider threats
- Summarize legal and other requirements to consider when accessing, handling, and reporting records and data
- Demonstrate how to locate information about potential insider threats
- Assess the veracity of the information found in records
- Determine potential risk indicators in records, databases, and other electronic forms of information
- Assess circumstances to determine which information may be shared within an Insider Threat Program or referred outside of the program

Lesson 2: Records Checks Overview

Introduction

Objectives

In this lesson, we'll explore why we conduct records checks, discuss considerations for performing records checks, and review the types of information to seek in these records checks.

Here are the lesson objectives. Take a moment to review them.

- Explain how records checks support the identification of anomalous behavior associated with potential insider threats
- Summarize legal and other requirements to consider when accessing and handling records and data
- Identify the types of information and records to locate when performing an insider threat records check

Welcome

Colleague 1: "I don't know where she gets her money, but Ivanka is always wearing new, high-end clothes and shoes. She has quite a collection of designer bags and luxury watches, too."

Colleague 2: "She's always poking around on the network, saying how weak our security is. She says her grandmother could get through it."

Colleague 3: "A couple of us were talking about a documentary we'd seen about the USSR. She got pretty heated. She said Americans don't understand real strength or unity."

Records Checks

Purpose

Insider Threat Programs use techniques like workforce awareness campaigns and user activity monitoring to prevent, deter, detect, and mitigate future potential insider threats. Where prevention and determent fail, detection provides the critical opportunity to intervene with mitigation strategies. The records checks you conduct on a potential insider threat allow your Program to develop additional information about the individual that may corroborate or refute any indicators identified through monitoring or through referrals of information. The information developed through records and database checks enables the analysis your

Program will perform to evaluate the threat an individual insider poses and to recommend mitigation response actions.

Considerations

When a potential threat is identified, a common initial action taken by an Insider Threat Program is to perform a records check. At this stage, the records check is an administrative function used to gather additional information rather than a formal inquiry or investigation. Your goal is to gather as much information about the individual as possible while respecting privacy and civil liberties and preserving the viability of future response actions. You must report any possible loss or compromise of classified information, and this may require you to halt your activities. You should also have a plan in place should you discover an imminent threat of physical harm. Your Insider Threat Program may have additional considerations and guidance for conducting records checks. Consult your organization's General Counsel and security office.

Respect Privacy and Civil Liberties

Always act in accordance with applicable regulations and policy regarding privacy and civil liberties. Policy and regulations vary depending on whether you belong to the Department of Defense (DOD), another federal agency, or industry. In most cases, you must provide Privacy Act advisements to any records custodians from whom you obtain records and protect personally identifiable information (PII), and Health Insurance Portability and Accountability Act (HIPAA) data. In all cases, consult your General Counsel for additional guidance or with any questions that arise during the records check process.

Depending on your organization, guidance may include:

- Component or organizational privacy guidelines
- Privacy Act of 1974
- Health Insurance Portability and Accountability Act (HIPAA)
- Executive Order 12333
- DODD 5240.01, DOD Intelligence Activities

Preserve Viability

The individual should remain unaware of Insider Threat Program activities, including records checks, until your program develops a mitigation response. If the individual is alerted prematurely, this may escalate the threat behavior and limit your program's mitigation response options. Keeping the individual unaware may limit information gathering since some records custodians require a release, subpoena, National Security Letter, or Preservation Letter to provide information, or otherwise limit the amount of information provided to outside parties.

To avoid alerting the individual, do not request additional releases unless you have

coordinated with your General Counsel and developed a specific response plan for the matter. Consider referring insider threat matters that require additional records checks to law enforcement or counterintelligence. Subpoenas, National Security Letters, and Preservation Letters can only be issued as part of legal proceedings, which occurs outside of the scope of the Insider Threat Program.

Types of Records and Information

Your research should cover a variety of records and other information to create a holistic view of the individual. The information you seek should include the individual's current and past employment (including security records), military service, physical and mental health, law enforcement records, civil court activity, finances, residences, education, foreign travel, and birth and citizenship.

Employment & Personnel Records

Personnel records provide more than just dates and types of employment. They often include a wealth of information that can help corroborate what you find in other records. For example, consider the information a standard employment application contains. It may reveal:

- Residence
- Known associates
- Education history
- Military service
- Current and previous employers
- Positions held
- Dates of employment
- Reason for leaving a position
- Certifications
- Criminal history
- Hobbies, memberships, and associations

When aggregated, this information may reveal some biographical data, such as where the individual is from, and some of the individual's professional and personal interests.

The personnel file may also include attendance records, performance evaluations, rehire eligibility, and security files. Security files may provide information about the individual's compliance history, violations, levels of access, and more.

Military Records

Within an individual's military records, look for:

- Judicial or non-judicial punishments

- Unusually long periods between promotions
- Demotions
- Reclassifications and reasons why
- Awards and decorations
- Foreign travel, whether personal or professional
- Any variances in dates of service or types of discharge
- Foreign military service and types of duties

Medical Records

Review any medical information available to you. Some medical information may have been provided to the government with a signed release by the individual as a condition of employment. Note that industry Insider Threat Programs are unlikely to have access to an individual's medical information. This information may consist of a health professional's determination of any potential national security issues rather than the actual records, depending on the type of release used. Do not pursue additional medical information unless directed to do so by your Insider Threat Program's leadership.

If you do have access to medical information, you may be able to glean information from the individual's medical, dental, mental health, and alcohol and drug abuse treatment records. Your organization's behavioral science subject matter expert may be able to help you decipher and effectively evaluate these records.

Exercise caution when accessing, storing, retaining, and disseminating medical records. Consult your General Counsel when handling potential Health Insurance Portability and Accountability Act (HIPAA) information.

Law Enforcement Records

Review the individual's law enforcement records, such as:

- Criminal records, including non-convictions
- Traffic violations
- Uniform Code of Military Justice (UCMJ) violations
- Campus security records

These records may indicate patterns, associations with bad actors, and other suitability issues. For example, reviewing the individual's traffic violations may reveal a driving under the influence (DUI) offense, which presents a suitability issue.

Civil Court Records

Review civil court records such as:

- Liens, judgments, and filings
- Bankruptcies

- Divorce proceedings
- Probate records

These records may reveal a wide variety of information about the individual, like verification of affluence, and suitability issues such as financial problems.

Financial Information

Where possible, review the individual's financial information, such as credit reports and military finance records.

Credit reports may reveal:

- Delinquent accounts
- Loans and mortgages
- Consumer credit counseling
- Bankruptcies
- Suspicious transactions

Military finance records may contain:

- Leave periods and places
- Locations of financial institutions
- Direct deposit information
- Savings and loan allotments

There may be restrictions on acquiring additional commercial records about the individual. Consult with your General Counsel before attempting to acquire this information from outside sources.

Residential Information

Verify any residences listed on other records, such as employment applications, for the individual and note any additional residences not previously disclosed. Look for any unexplained periods of time with no residence indicated, and review associations and references such as roommates, co-owners, neighbors, landlords, and listed references on rental applications. Also consider whether the residences are within the individual's reported financial means.

Education Information

Verify the individual's educational background and review:

- Locations and dates of attendance
- Achievements
- Extracurricular activities

- Disciplinary actions
- Job placement office and Reserve Officers' Training Corps (ROTC) files
- On-campus residence information

Foreign Travel Information

For foreign travel information, try to identify:

- Places visited
- Duration of travel
- Stated purpose of travel
- Foreign national contacts
- Mode of transportation
- Declared goods

Birth & Citizenship Records

Verify the individual's date and place of birth and citizenship.

If the individual is a United States citizen, confirm whether the citizenship is by birth, derivative, or naturalized. For derivative citizenships, review the details of the parents' citizenship to determine the basis of derivative citizenship status. For naturalized citizens, review the naturalization certificate number and the date, place, and court of issue.

If the individual is an alien, immigrant alien, or foreign national, review the individual's status documentation, such as the alien registration number, the work visa number, and information on foreign passports to ensure it is valid.

For naturalized citizens and non-citizens, try to determine the relationship the individual has with the country of birth. For example, was foreign citizenship renounced? Does the country accept the renunciation? Does the individual have any material participation in the country? Does the individual still hold a foreign passport? Has the individual served in a foreign military? Does the individual owe anything to the foreign country? Does the individual have foreign relatives still residing in the foreign country?

Term	Definition
By Birth	Born within U.S. states or territories recognized by law
Derivative	Born outside the U.S. to parents who are U.S. citizens ***or*** brought to the U.S. by parents who obtained citizenship prior to the child's 18th birthday
Naturalized	Granted citizenship by a court as an alien authorized by law to obtain citizenship

Review Activities

Supervisor: "Hey, do you have a minute? I've got a new case for you to triage. A few people have noticed some possible indicators for Ivanka, our chemical engineer. Can you look into her records and let me know if there's anything significant to report?"

Review Activity 1

How will performing a records check on Ivanka support your Insider Threat Program's goals?

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

- ☐ It will help the program to corroborate or mitigate what Ivanka's colleagues reported.
- ☐ The additional information will allow the Program to develop an appropriate mitigation strategy.
- ☐ It will build a case for your program to automatically terminate Ivanka's employment.

Review Activity 2

What types of information should you attempt to gather about Ivanka?

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

- ○ Birth and citizenship
- ○ Education
- ○ Finances
- ○ Law enforcement
- ○ Military
- ○ Foreign travel
- ○ Residence
- ○ Civil court
- ○ Medical
- ○ Employment and personnel
- ○ All of the above

Review Activity 3

Question 1 of 3. You've received a copy of Ivanka's personnel file. It contains personal information, including her social security number and birth date. What should you do?

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

- ○ Request a release from Ivanka.
- ○ Thank the records custodians for their time.
- ○ Provide a Privacy Act advisement.
- ○ Take special precautions to protect personally identifiable information (PII).
- ○ Destroy the record.

Question 2 of 3. You call the registrar's office at Ivanka's university to confirm her graduation date. What should you do?

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

- ○ Request a release from Ivanka.
- ○ Thank the records custodians for their time.
- ○ Provide a Privacy Act advisement.
- ○ Take special precautions to protect personally identifiable information (PII).
- ○ Destroy the record.

Question 3 of 3. The registrar asks you to provide a signed release in order to give you the information. What should you do?

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

- ○ Request a release from Ivanka.
- ○ Thank the records custodians for their time.
- ○ Provide a Privacy Act advisement.
- ○ Take special precautions to protect personally identifiable information (PII).
- ○ Destroy the record.

Conclusion

Case Study: Background

Earlier you were introduced to Kevin Mallory, a real-life insider threat who was brought down in part due to records checks. Throughout this course, we'll examine his case to learn how he became an insider threat, how he was stopped, and the damage he caused.

Mallory had served in the U.S. military for five years and continued as an Army reservist. He had worked as a CIA officer, and was stationed in Iraq, China, and Taiwan. During that time, Mallory held a Top Secret security clearance. His clearance was terminated when he left government service in October 2012. Mallory, a U.S. citizen, speaks fluent Mandarin Chinese. Mallory was over $230,000 in debt and months behind in mortgage payments.

Lesson 3: Locating Information

Introduction

Objectives

In this lesson, we'll discuss potential sources of information.

Here is the lesson objective. Take a moment to review it.

- Identify data sources available to DOD and other Insider Threat Programs

Welcome

Analyst: "That's odd—why was Ivanka here at 1 a.m.?"

Data Sources

Introduction

Where can you lawfully find records and information without requesting a release and alerting the individual? The sources available to you may vary based on whether you belong to a DOD, Federal Agency, or industry Insider Threat Program.

In general, you should be able to access your organization's records and any open sources of data. Open sources of data are available to the public.

DOD Component Insider Threat Programs may be able to access additional department or c o mponent records and some federal records. DOD source information is generally limited to DOD Component Insider Threat Programs. DOD Components may contact the DOD Insider Threat Management and Analysis Center (DITMAC) for assistance as well.

Federal Agency Insider Threat Programs may be able to access additional federal records.

Whether you belong to a DOD, Federal, or industry Program, consult your Insider Threat Program's Standard Operating Procedures (SOP). Your organization may have Memoranda of Agreement, policies, or other procedures in place to facilitate lawful access to additional sources.

Term	Definition
DITMAC	DOD Insider Threat Management and Analysis Center • Provides a centralized capability within the DOD to consolidate and analyze specified DOD reporting of potentially adverse information • Assesses cases, recommends intervention/mitigation, and tracks case action of threats insiders may pose

DOD Sources

Several DOD resources may be available to DOD Component Insider Threat Programs only. These include:

- The individual's Personnel Security Investigation (PSI) file
- The Defense Manpower Data Center (DMDC)
- The DITMAC System of Systems (DSOS)
- The Defense Central Index of Investigations (DCII)
- The Defense Information System for Security (DISS)

Personnel Security Investigation (PSI) File

The individual's PSI file contains the individual's completed Standard Form (SF)-86, Questionnaire for National Security Positions, and the background investigator's findings.

With continuous vetting, cleared individuals are regularly reviewed to ensure security clearance requirements are met and the appropriate individuals continue to hold positions of trust.

Automated record checks pull data from criminal, terrorism, and financial databases, as well as public records, at any time during an individual's period of eligibility. If potential threat information is discovered, investigators and adjudicators then gather facts and make clearance determinations. This information will be placed in the PSI file.

PSI files are only available to DOD components. If you belong to a DOD Insider Threat Program, consult your program's SOP to determine your component's access protocol for PSI files.

The PSI file will likely be the most comprehensive source of information about the individual.

Term	Definition
SF-86	Standard Form 86, Questionnaire for National Security Positions Includes self-reported information on the individual's citizenship, residence, education, employment, military history, references, marital status, family, foreign contact, foreign activity, foreign travel, psychological and emotional health, police record, drug and alcohol use, clearance, finances, information technology use, civil court cases, and associations
Background investigator's findings	Includes law enforcement checks, credit reports, and medical records

Defense Manpower Data Center (DMDC)

DMDC is the central repository for current and historical DOD human resources information, both civilian and military. Its Person Data Repository (PDR) collects data from the personnel master files provided periodically from the Services and other DOD activities, and from operational programs that include:

- The Defense Enrollment Eligibility Reporting System (DEERS)
- The Common Access Card (CAC)
- The Real-Time Automated Personnel Identification System (RAPIDS)
- The Defense Biometric Identification System (DBIDS)

DMDC contains personnel files for active duty, guard, and reserve members; civilians, retirees, and contractors; financial and contract files; and military records.

Term	Definition
DEERS	Defense Enrollment Eligibility Reporting System The DOD's Person Data Repository (PDR) of all personnel and certain medical data
CAC	Common Access Card • Provides an enterprise-wide credential for both physical and logical access to DOD facilities and networks • Uses the DEERS database for authentication and personnel information
RAPIDS	Real-Time Automated Personnel Identification System The infrastructure that: • Supports the Uniformed Services identification card • Provides online updates to DEERS • Issues the CAC to Service members, civilian employees, and eligible contractors

Term	Definition
DBIDS	Defense Biometric Identification System A personnel identity protection initiative that uses existing DOD-issued identification credentials to authorize approved cardholders' physical access on a scalable level
Personnel files	• May include pay, Social Security Administration (SSA), Veterans Affairs (VA), and Medicare information • For active duty personnel: May also include inventory, gains and losses, military units and addresses, and special purposes such as contingency operations

Defense Central Index of Investigations (DCII)

DCII is an automated index that catalogs DOD investigations and personnel security determinations. DCII may contain security information about your individual.

Defense Information System for Security (DISS)

DISS contains personnel security adjudicative actions and determinations. It replaced the Joint Personnel Adjudication System (JPAS). DISS may contain security information about your individual.

DITMAC System of Systems (DSOS)

DSOS is the enterprise level capability for managing and analyzing insider threat information. It is the primary tool for capturing, consolidating, storing, analyzing, and managing insider threat data and reporting to the DITMAC. DSOS may provide insider threat information about your individual.

Federal Information Sources

Sources of Federal information include:

- Human resources
- The Student and Exchange Visitor Information System (SEVIS)
- The Financial Crimes Enforcement Network (FinCEN)
- The National Crime Information Center (NCIC)
- TECS, which was formerly known as the Treasury Enforcement Communications System
- The Consolidated Screening List
- Direct contact with Federal Agencies

Human Resources

The human resources operations personnel within DOD and Federal Insider Threat

Hubs may be able to access and provide the individual's Federal employment file. This personnel file may contain pre-employment screening information and polygraph results for your individual.

Student and Exchange Visitor Information System (SEVIS)

SEVIS is part of U.S. Immigration and Customs Enforcement, or ICE. It is a web-based system for maintaining information on nonimmigrant students and exchange visitors in the U.S. It is the core technology for the Department of Homeland Security, or DHS, in this critical mission. SEVIS provides information about nonimmigrant students and exchange visitors to the U.S. Visit the Course Resources page to access the SEVIS website.

Financial Crimes Enforcement Network (FinCEN)

FinCEN is an organization within the United States Department of Treasury that combats financial crimes and money laundering operations. It gathers data on suspicious financial transactions, including banking, purchasing, or monetary transfers involving large sums of cash. FinCEN may have information about suspicious financial transactions associated with your individual. Visit the Course Resources page to access the FinCEN website.

National Crime Information Center (NCIC)

NCIC is a computerized index of criminal justice information provided by the Federal Bureau of Investigation (FBI). It contains criminal history records and information about fugitives, stolen properties, and missing persons. Visit the Course Resources page to access the NCIS website.

TECS (formerly Treasury Enforcement Communications System)

TECS is a Department of Homeland Security (DHS) system used by border officers to assist with screening and determinations regarding admissibility of arriving persons. It may contain foreign travel information about your individual.

Consolidated Screening List

The consolidated screening list is a joint product of the Departments of Commerce, State, and Treasury. It combines the denied persons list, debarment list, sanctions, specially designated nationals, and others and identifies individuals and organizations that are precluded from doing business with the U.S. Government. The presence of your individual or any known associates, whether individuals or organizations, on this list indicates a potential issue to research further.

Direct Contact with Federal Agencies

You may also consider contacting individual Service branches, the Internal Revenue Service (IRS), and Federal Agencies and Bureaus to ask if they would be willing to run name checks and provide additional information. Remember that you must provide Privacy Act advisements to all records custodians and that this direct contact may increase the risk of alerting the individual.

Other Sources

Sources outside the DOD and Federal Government may also provide valuable information. An Internet search may uncover blogs, publications, and social media sites that may reveal information such as employment, education, and residence. There are special requirements for access to social media accounts.

Check with your General Counsel in advance to ensure you remain in compliance with policy, such as the Security Executive Agent Directive 5, “Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications”. This directive includes details about what publicly available electronic information, or PAEI, may be collected and retained.

Additional Sources

Employment:

- Corporate employment verification and files

Residential:

- Property tax/recorder of deeds
- Police files
- Post office
- Telephone and utility companies
- Residence directories
- Local rental and real estate offices

Birth:

- Bureau of Vital Statistics
- Church records
- Hospital records
- Court records

Education:

- Public and private primary schools and universities
- Vocational schools
- Professional societies and courses
- Yearbooks
- Alumni associations
- Campus security

- Career office
- Reserve Officers' Training Corps (ROTC)

Foreign travel:

- Customs records
- Passport/visa applications
- Passenger manifests
- Currency exchange files
- Border police
- Private and Government travel agencies

Check your Insider Threat Program SOP before using these sources.

Review Activities

Supervisor: "Human resources gave me that personnel file you requested."

On reviewing Ivanka's personnel file, you've found a treasure trove of information. You note a few areas that you especially want to follow up on. Refer to the end of this Student Guide for a matrix of data types and sources that may aid your research.

Review Activity 1

Question 1 of 4. Which data source(s) contain education information?

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

- ☐ Personnel Security Investigation (PSI) File
- ☐ Defense Manpower Data Center (DMDC)
- ☐ Student and Exchange Visitor Information System (SEVIS)
- ☐ Financial Crimes Enforcement Network (FinCEN)
- ☐ TECS (formerly known as the Treasury Enforcement Communications System)

Question 2 of 4. Which data source(s) contain foreign travel information?

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

- ☐ Personnel Security Investigation (PSI) File
- ☐ Defense Manpower Data Center (DMDC)
- ☐ Student and Exchange Visitor Information System (SEVIS)
- ☐ Financial Crimes Enforcement Network (FinCEN)
- ☐ TECS (formerly known as the Treasury Enforcement Communications System)

Question 3 of 4. Which data source(s) contain residential information?

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

- ☐ Personnel Security Investigation (PSI) File
- ☐ Defense Manpower Data Center (DMDC)
- ☐ Student and Exchange Visitor Information System (SEVIS)
- ☐ Financial Crimes Enforcement Network (FinCEN)
- ☐ TECS (formerly known as the Treasury Enforcement Communications System)

Question 4 of 4. Which data source(s) contain financial information?

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

- ☐ Personnel Security Investigation (PSI) File
- ☐ Defense Manpower Data Center (DMDC)
- ☐ Student and Exchange Visitor Information System (SEVIS)
- ☐ Financial Crimes Enforcement Network (FinCEN)
- ☐ TECS (formerly known as the Treasury Enforcement Communications System)

Conclusion

Case Study: Initial Cause for Inquiry

Insider threats usually present some indication that something is not right before their actions cross the line. The initial inquiry into Kevin Mallory came about because Mallory had reached out to several former colleagues at the CIA, inquiring about current intelligence on China. Those colleagues reported the behavior to CIA security as suspicious.

Lesson 4: Verifying and Corroborating Information

Introduction

Objectives

In this lesson, we'll discuss how to verify and corroborate information.

Here are the lesson objectives. Take a moment to review them.

- Identify the purpose of verifying information
- Differentiate between primary and secondary sources of information
- Describe techniques to verify and corroborate information

Welcome

[Social media post]
Police Blotter

Ivanka Kuchinsky was cited for trespassing on Main Street at 6:00 pm.

Analyst: "I haven't found this mentioned anywhere else. This should have been reported."

Purpose

Gathering information from many data sources means there is a possibility that you may come across conflicting or discrepant information as you perform your records checks. It's a best practice to verify all information through multiple sources, if possible. You must also include exculpatory information, if it exists, to paint as accurate a picture as possible. Incorrect or incomplete information should be further researched. Any allegation against an individual may have detrimental impacts on his or her career, so it is essential to gather all of the facts so the potential threat posed by the individual can be fully assessed before mitigation response options are determined.

Here's an actual example of what can happen when information is not corroborated.

[Newscaster]
"The man who was mistakenly *arrested has the same last name as the man who was supposed to be arrested. Due to a computer data entry error, an arrest warrant was issued for the wrong guy.*

Soon, Hector Acevedo-Rodriguez – the wrong guy – was taken into custody, on charges of felony battery and aggravated assault with a firearm. He would spend three nights *in jail, before authorities discovered the mistake."*

Term	Definition
Exculpatory information	Information that would tend to exonerate the individual

Verification and Corroboration Techniques

Use Multiple Sources

Using multiple data sources can help you corroborate information and determine the validity of discrepant information. Multiple data sources may also provide exculpatory information to mitigate potential risk indicators. For example, a credit report showing large amounts of debt or delinquent accounts may be explained by a police report filed by the individual claiming identity theft.

Use Primary Sources

When using multiple sources to corroborate and verify information, it is also important to consider the source. Primary sources provide direct or firsthand evidence about the individual—for example, a copy of probate court records detailing the individual's receipt of an inheritance. Secondary sources relay secondhand information about the individual—for example, a record of an interview with a co-worker alleging that the individual received an inheritance.

Primary sources are more likely to be valid than secondary sources, so attempt to use them whenever possible. If only secondary sources are available, it is a best practice to corroborate that information with multiple sources. For example, if you develop a residence using a telephone directory listing, you may be able to corroborate it with a copy of the rental agreement.

Review Activities

Check your answers in the Answer Key at the end of this Student Guide.

Analyst: "I haven't found this mentioned anywhere else."

Supervisor: "This is helpful information, but how do you know it's accurate?"

Review Activity 1

What are some possible consequences of not verifying the information uncovered about Ivanka? *Select all that apply.*

- ☐ The information could have a detrimental impact on Ivanka's career, even if it turns out to be untrue.
- ☐ The Insider Threat Program could inaccurately assess the risk Ivanka poses as an insider threat.
- ☐ The Insider Threat Program could employ an inappropriate or inadequate mitigation response.

Review Activity 2

[Social media post] Police Blotter

Ivanka Kuchinsky was cited for trespassing on Main Street at 6:00 pm.

Is this social media post a primary source or a secondary source? *Select the best response.*

- ○ Primary source
- ○ Secondary source

Review Activity 3

[Social media post] Police Blotter

Ivanka Kuchinsky was cited for trespassing on Main Street at 6:00 pm.

Which of the following would be the best way to verify and corroborate this news item? *Select the best response.*

- ○ Ask Ivanka's friends about it.
- ○ Get a copy of the police report.
- ○ Find it mentioned in a newspaper.
- ○ Ask the police beat reporter about it.

Conclusion

Case Study: Opening the Fraud Case

As the Federal Bureau of Investigation (FBI) took over looking into Kevin Mallory, additional indicators of the threat he posed became evident. The FBI coordinated with the Central Intelligence Agency (CIA), and Customs and Border Protection (CBP) to interview people and check additional records.

Customs records revealed that Mallory had taken multiple trips to China recently. On the return from one of those trips, CBP stopped Mallory. They discovered he had over $16,000 in cash – but he had stated he did not have more than $10,000 in his possession. They also discovered a cell phone he claimed was a gift from his wife – but was actually a covert communication device from Chinese Intelligence.

Lesson 5: Identifying Indicators

Introduction

Objectives

In this lesson, we'll explore indicators that you may find while conducting records checks.

Here are the lesson objectives. Take a moment to review them.

- Determine potential risk indicators (PRIs) in records, databases, and other electronic forms of information
  - Describe the purpose of indicators
  - Describe the qualities of an effective indicator
  - Identify DOD PRI categories and other resources for indicators

Welcome

Analyst: "There's a lot of foreign travel. Is this any of this travel anomalous or concerning?"

Indicators

Purpose and Qualities

Individuals at risk of becoming insider threats, and those who ultimately cause significant harm, often exhibit warning signs, or indicators. Potential risk indicators, or PRIs, include a wide range of individual predispositions, stressors, choices, actions, and behaviors. Some indicators suggest increased vulnerability to insider threat; others may be signs of an imminent and serious threat.

Indicators do not always have diagnostic value or reflect wrongdoing. Some indicators may involve activities that are constitutionally protected.

Reviewing an individual's records for known indicators can offer the Insider Threat Program early warning that an undesirable event may occur, giving the Program an opportunity to mitigate the risk. Keeping a record of indicators can also help you to monitor, detect, and evaluate change in the individual's records over time, such as sudden unexplained affluence.

To be effective, indicators must meet several criteria. First, they should be observable. The information must be able to be gathered from a reliable source in accordance with laws and regulations. Next, indicators should be valid. The information must be relevant to the risk of insider threat and considered in context with exculpatory information. Indicators should also be reliable. You and your colleagues must use consistent data collection methods and indicator definitions. In addition, indicators should be stable. When

monitoring an individual over time, be sure to use the same indicators throughout so you can track change. Finally, indicators should be unique. Each indicator should measure only one thing but may be combined with other indicators to identify risk.

DOD Potential Risk Indicators

The DOD Insider Threat Management and Analysis Center (DITMAC) sets the potential risk indicators (PRIs) used by DOD Component Insider Threat Programs. DITMAC bases the PRIs on the analysis of known insider threat cases and continues to improve them. In general, the DOD PRIs are categorized similarly to the adjudicative guidelines that are used to determine eligibility for access to classified information and that are used by industry Insider Threat Programs to determine reporting criteria. Federal Agency Insider Threat Programs may also use similar indicators.

DOD PRIs may belong to the categories listed here:

- Access attributes
- Professional lifecycle and performance
- Foreign considerations
- Security compliance and incidents
- Technical activity
- Criminal, violent, or abusive conduct
- Financial considerations
- Substance abuse and addictive behaviors
- Judgment, character, and psychological conditions

DOD Component Insider Threat Programs may contact the DITMAC for the most current PRIs and detailed explanations of each category. All Insider Threat Programs are encouraged to coordinate with their cognizant authorities to maintain current indicators.

Review Activity

Analyst: "There's a lot of foreign travel. Is any of this travel anomalous or concerning?"

Supervisor: "That's definitely a PRI. Are there any others?"

In this review activity, you will review Ivanka's employment application for PRIs. Remember that information on an employment application may reveal more than meets the eye when taken as a whole.

Review the full application and then identify each PRI in each section. Then go to the next page to check your answer.

APPLICATION FOR EMPLOYMENT

GENERAL INFORMATION

Name (Last)	(First)		(Middle Name)	Home Telephone
Kuchinsky	Ivanka		Polina	(800) 555 - 1212
Address (Mailing Address)	**(City)**	**(State)**	**(Zip)**	**Other Telephone**
124 White St.	Manhattan	NY	11240	N/A
E-Mail Address	Are you legally entitled to work in the U.S.? ☒ Yes ☐ No			
IvanK@xyz.com				

POSITION

Position Or Type of Employment Desired	Will Accept:	Shift:
Chemical Engineer	☒ Part-Time ☒ Full-Time ☒ Temporary	☒ Day ☒ Swing ☒ Graveyard ☒ Rotating
Are you able to perform the essential functions of the job you are applying for, with or without reasonable accommodation? ☒ Yes ☐ No		
Salary Desired Negotiable	**Date Available** Immediately	
How did you learn about our company? Referred by Cousin		
Do you have any friends, relatives, or acquaintances working for us? ☒ **Yes** ☐ No	**If yes, state name, relationship, and address:** Dale Greenglass Jr., Cousin, 543 Martin Luther King Blvd., New York, NY 10027	

EDUCATION AND TRAINING

High School Graduate Or General Education (GED) Test Passed? ☒ Yes ☐ No
If no, list the highest grade completed

College, Business School, Military (Most recent first)

Name and Location	Dates Attended Month/Year	Credits Earned: Quarterly or Semester Hours	Credits Earned: Other (Specify)	Graduate	Degee & Year	Major or Subject
Columbia University – New York	From 08/2018 To 05/2022	120		☒ Yes ☐ No	M.S., 2022	Nuclear Physics
Uzbekistan Institution of Chemical Engineers	From 08/2014 To 05/2018	120		☒ Yes ☐ No	B.S., 2018	Chemical Engineer

MILITARY SERVICE INFORMATION (Most recent)

Branch of Service	Date of Entry	Date of Discharge
Armed Forces of the Republic of Uzbekistan	April 22, 2010	April 21, 2014

MILITARY Awards and Recognitions (List all pertinent skills and equipment that you can operate)

(Maximum 1000 characters)

- Shon-Sharaf Order (Republic of Uzbekistan)
- Jasorat Medal (Republic of Uzbekistan)

WORK EXPERIENCE (Most Recent First) (Include voluntary work and military experience)

Employer Generic Industries, Inc. | **Telephone Number** (877) 555 - 1010 | **From (Month/Year)** 09/2021
Address 8765 South St., Anycity, NY 11235 | **To (Month/Year)** 03/2023
Job Title Chemical Engineer | **Number Employees Supervised** 5 | **Hours Per Week** 30-40
Last Salary $65,500/year
Supervisor Fred Davis

Specific Duties (Maximum 1000 characters)
- Established designs to convert raw materials into a variety of products.
- Performed calculations while conducting research and analysis.
- Collaborated with chemists, contractors, and other team members to ensure successful completion of projects.
- Tested high powered materials needed for aerospace, biomedical, and military applications.
- Process engineering for both areas of chemical reaction and separation process.
- Part of development team that invented and optimized methods for cleaner energy products such as efficient engines that produce fewer hazardous pollutants when burning fuel.

Reason For Leaving: Returned home to care for family member. | **May We Contact This Employer?** ☒ Yes ☐ No

---

Employer Generic Aeronautics, Inc. | **Telephone Number** (866) 555 - 1000 | **From (Month/Year)** 08/2019
Address 9871 Broadway, Mytown, VT 05009 | **To (Month/Year)** 08/2021
Job Title Aeronautic Engineer | **Number Employees Supervised** 0 | **Hours Per Week** 30
Last Salary $52,000/year
Supervisor Nancy Smith

Specific Duties (Maximum 1000 characters)
- Assisted in designing aircraft and missiles using aerodynamics in manufacturing parts, and developing structural design.
- Performed maintenance of aircrafts for commercial, government and military use.
- Resolved retrieval problems by altering design to meet requirements.
- Prepared reports by collecting, analyzing, and summarizing information.
- Wrote operating instructions.
- Maintained historical records by documenting system changes and revisions.
- Maintained client confidence and protects operations by keeping information confidential.
- Maintained professional and technical knowledge by attending educational workshops; reviewing professional publications; establishing personal networks; participating in professional societies.
- Development of aircraft parts and structural design was based in aeronautical engineering and astronautical engineering.
- Maintained database of all operations.

Reason For Leaving New opportunity | **May We Contact This Employer?** ☒ Yes ☐ No

---

Employer Johnson Temps, Inc. | **Telephone Number** (800) 555 - 2222 | **From (Month/Year)** 07/2019
Address 2456 Standard Road, Nowhere, MA 02115 | **To (Month/Year)** 08/2018
Job Title Chemist Assistant | **Number Employees Supervised** 0 | **Hours Per Week** 20
Last Salary $31,200
Supervisor George Walter

Specific Duties (Maximum 1000 characters)
- Ordering, stocking, and maintaining laboratory supplies.
- Prepared specimens for testing and performed basic lab tests.
- Resolved discrepancies by using standard procedures of informing the team leader for resolution.
- Assisted in setting up experiments, collected and analyzed data, and assisted with the development of new processes.
- Followed safety procedures and regulations and ensured all safety protocols were followed by team.
- Received certifications in chemistry, biochemistry, and related disciplines.

Reason For Leaving Position with more income | **May We Contact This Employer?** ☒ Yes ☐ No

Certifications and Licenses

Occupational License, Certificate or Registration	Number	Where Issued	Expiration Date
Fundamentals of Engineering (FE)	12345	NY	11/21/2026
Occupational License, Certificate or Registration	Number	Where Issued	Expiration Date
Certified Chemical Engineer (CCE)	54321	NY	07/15/2025

Criminal History

Have you ever been convicted of a criminal offense (felony or misdemeanor)? ☒ Yes ☐ No
If yes, please state nature of the crime(s), when and where convicted and disposition of the case. Trespassing

Hobbies and Activities List all memberships, associations, or other activities and pursuits.

Organization	Leadership positions held	Dates of membership
Russian American Social Club	President 2022 - 2023	2015 - Present
American Society of Civil Engineers	None	2018 - Present

I certify the information contained in this application is true, correct, and complete. I understand that, if employed, false statements reported on this application may be considered sufficient cause for dismissal.

Signature of Applicant_____ **Date**_____

Part 1

There are three PRIs in this section. Can you find them all?

POSITION

Position Or Type of Employment Desired Chemical Engineer	**Will Accept:** ☒ Part-Time ☒ Full-Time ☒ Temporary	**Shift:** ☒ Day ☒ Swing ☒ Graveyard ☒ Rotating
Are you able to perform the essential functions of the job you are applying for, with or without reasonable accommodation? ☒ Yes ☐ No		
Salary Desired Negotiable	**Date Available** Immediately	
How did you learn about our company? Referred by Cousin		
Do you have any friends, relatives, or acquaintances working for us? ☒ **Yes** ☐ No	**If yes, state name, relationship, and address:** Dale Greenglass Jr., Cousin, 543 Martin Luther King Blvd., New York, NY 10027	

EDUCATION AND TRAINING

High School Graduate Or General Education (GED) Test Passed? ☒ Yes ☐ No
If no, list the highest grade completed

College, Business School, Military (Most recent first)

Name and Location	**Dates Attended Month/Year**	**Credits Earned**		**Graduate**	**Degee & Year**	**Major or Subject**
		Quarterly or Semester Hours	Other (Specify)			
Columbia University – New York	From 08/2018 To 05/2022	120		☒ Yes ☐ No	M.S., 2022	Nuclear Physics
Uzbekistan Institution of Chemical Engineers	From 08/2014 To 05/2018	120		☒ Yes ☐ No	B.S., 2018	Chemical Engineer

Part 1 – Answer Key

There are three PRIs in this section. Can you find them all?

POSITION

Position Or Type of Employment Desired Chemical Engineer	**Will Accept:** ☒ Part-Time ☒ Full-Time ☒ Temporary	**Shift:** ☒ Day ☒ Swing ☒ Graveyard ☒ Rotating
Are you able to perform the essential functions of the job you are applying for, with or without reasonable accommodation? ☒ Yes ☐ No		
Salary Desired Negotiable	**Date Available** Immediately	
How did you learn about our company? Referred by Cousin		
Do you have any friends, relatives, or acquaintances working for us? ☒ **Yes** ☐ No	**If yes, state name, relationship, and address:** Dale Greenglass Jr., Cousin, 543 Martin Luther King Blvd., New York, NY 10027	

EDUCATION AND TRAINING

High School Graduate Or General Education (GED) Test Passed? ☒ Yes ☐ No
If no, list the highest grade completed

College, Business School, Military (Most recent first)

Name and Location	**Dates Attended Month/Year**	**Credits Earned**		**Graduate**	**Degee & Year**	**Major or Subject**
		Quarterly or Semester Hours	Other (Specify)			
Columbia University – New York	From 08/2018 To 05/2022	120		☒ Yes ☐ No	M.S., 2022	Nuclear Physics
Uzbekistan Institution of Chemical Engineers	From 08/2014 To 05/2018	120		☒ Yes ☐ No	B.S., 2018	Chemical Engineer

Chemical Engineer and M.S., Nuclear Physics:

This applicant is applying for a job much below her skill level and experience. This may be an indicator that the individual is applying for a position for the access to information it provides rather than for personal, professional, or financial reasons that impel most job searches.

Uzbekistan Institution of Chemical Engineers: *The applicant was educated at a foreign school. Foreign influence or preference issues may be present based on obligations from scholarships or loans.*

Part 2

There are four PRIs in this section. Can you find them all?

MILITARY SERVICE INFORMATION (Most recent)

Branch of Service	Date of Entry	Date of Discharge
Armed Forces of the Republic of Uzbekistan	April 22, 2010	April 21, 2014

MILITARY Awards and Recognitions (List all pertinent skills and equipment that you can operate)

(Maximum 1000 characters)

- Shon-Sharaf Order (Republic of Uzbekistan)
- Jasorat Medal (Republic of Uzbekistan)

Criminal History

Have you ever been convicted of a criminal offense (felony or misdemeanor)? ☒ Yes ☐ No

If yes, please state nature of the crime(s), when and where convicted and disposition of the case.
Trespassing

Hobbies and Activities List all memberships, associations, or other activities and pursuits.

Organization	Leadership positions held	Dates of membership
Russian American Social Club	President 2022 - 2023	2015 - Present
American Society of Civil Engineers	None	2018 - Present

Part 2 – Answer Key

There are four PRIs in this section. Can you find them all?

MILITARY SERVICE INFORMATION (Most recent)

Branch of Service	Date of Entry	Date of Discharge
Armed Forces of the Republic of Uzbekistan	April 22, 2010	April 21, 2014

MILITARY Awards and Recognitions (List all pertinent skills and equipment that you can operate)

(Maximum 1000 characters)

- Shon-Sharaf Order (Republic of Uzbekistan)
- Jasorat Medal (Republic of Uzbekistan)

Criminal History

Have you ever been convicted of a criminal offense (felony or misdemeanor)? ☒ Yes ☐ No

If yes, please state nature of the crime(s), when and where convicted and disposition of the case.

Trespassing

Hobbies and Activities List all memberships, associations, or other activities and pursuits.

Organization	Leadership positions held	Dates of membership
Russian American Social Club	President 2022 - 2023	2015 - Present
American Society of Civil Engineers	None	2018 - Present

Military Service: *Foreign military service may be indicative of foreign influence, loyalty, or preference issues.*

Military Awards: *Awards and recognitions from foreign military service may indicate foreign influence, preference, or loyalty issues.*

Criminal History: *Criminal behavior is considered a PRI and is a factor under the adjudicative guidelines, both of which require reporting actions under Insider Threat policy.*

Russian American Social Club: *Be sure to review hobbies, outside employment, and activities. These can reveal groups, memberships, or associations that constitute potential risk indicators, reportable information under the adjudicative guidelines, or other information about the individual (including exculpatory information).*

Part 3

There is one PRI in this section. Can you find it?

WORK EXPERIENCE (Most Recent First) (Include voluntary work and military experience)

Employer Generic Industries, Inc.	**Telephone Number** (877) 555 - 1010	**From (Month/Year)** 09/2021
Address 8765 South St., Anycity, NY 11235		
Job Title Chemical Engineer	**Number Employees Supervised** 5	**To (Month/Year)** 03/2023
Specific Duties (Maximum 1000 characters) • Established designs to convert raw materials into a variety of products. • Performed calculations while conducting research and analysis. • Collaborated with chemists, contractors, and other team members to ensure successful completion of projects. • Tested high powered materials needed for aerospace, biomedical, and military applications. • Process engineering for both areas of chemical reaction and separation process. • Part of development team that invented and optimized methods for cleaner energy products such as efficient engines that produce fewer hazardous pollutants when burning fuel.		**Hours Per Week** 30-40 **Last Salary** $65,500/year **Supervisor** Fred Davis
Reason For Leaving: Returned home to care for family member.	**May We Contact This Employer?** ☒ Yes ☐ No	

Employer Generic Aeronautics, Inc.	**Telephone Number** (866) 555 - 1000	**From (Month/Year)** 08/2019
Address 9871 Broadway, Mytown, VT 05009		
Job Title Aeronautic Engineer	**Number Employees Supervised** 0	**To (Month/Year)** 08/2021
Specific Duties (Maximum 1000 characters) • Assisted in designing aircraft and missiles using aerodynamics in manufacturing parts, and developing structural design. • Performed maintenance of aircrafts for commercial, government and military use. • Resolved retrieval problems by altering design to meet requirements. • Prepared reports by collecting, analyzing, and summarizing information. • Wrote operating instructions. • Maintained historical records by documenting system changes and revisions. • Maintained client confidence and protects operations by keeping information confidential. • Maintained professional and technical knowledge by attending educational workshops; reviewing professional publications; establishing personal networks; participating in professional societies. • Development of aircraft parts and structural design was based in aeronautical engineering and astronautical engineering. • Maintained database of all operations.		Hours Per Week 30 Last Salary $52,000/year **Supervisor** Nancy Smith
Reason For Leaving New opportunity	**May We Contact This Employer?** ☒ Yes ☐ No	

Part 3 – Answer Key

There is one PRI in this section. Can you find it?

WORK EXPERIENCE **(Most Recent First) (Include voluntary work and military experience)**

Employer Generic Industries, Inc.	**Telephone Number** (877) 555 - 1010	**From (Month/Year)** 09/2021
Address 8765 South St., Anycity, NY 11235		
Job Title Chemical Engineer	**Number Employees Supervised** 5	**To (Month/Year)** 03/2023
Specific Duties (Maximum 1000 characters) • Established designs to convert raw materials into a variety of products. • Performed calculations while conducting research and analysis. • Collaborated with chemists, contractors, and other team members to ensure successful completion of projects. • Tested high powered materials needed for aerospace, biomedical, and military applications. • Process engineering for both areas of chemical reaction and separation process. • Part of development team that invented and optimized methods for cleaner energy products such as efficient engines that produce fewer hazardous pollutants when burning fuel.		**Hours Per Week** 30-40 **Last Salary** $65,500/year **Supervisor** Fred Davis
Reason For Leaving: Returned home to care for family member.	**May We Contact This Employer?** ☒ Yes ☐ No	

Employer Generic Aeronautics, Inc.	**Telephone Number** (866) 555 - 1000	**From (Month/Year)** 08/2019
Address 9871 Broadway, Mytown, VT 05009		
Job Title Aeronautic Engineer	**Number Employees Supervised** 0	**To (Month/Year)** 08/2021
Specific Duties (Maximum 1000 characters) • Assisted in designing aircraft and missiles using aerodynamics in manufacturing parts, and developing structural design. • Performed maintenance of aircrafts for commercial, government and military use. • Resolved retrieval problems by altering design to meet requirements. • Prepared reports by collecting, analyzing, and summarizing information. • Wrote operating instructions. • Maintained historical records by documenting system changes and revisions. • Maintained client confidence and protects operations by keeping information confidential. • Maintained professional and technical knowledge by attending educational workshops; reviewing professional publications; establishing personal networks; participating in professional societies. • Development of aircraft parts and structural design was based in aeronautical engineering and astronautical engineering. • Maintained database of all operations.		Hours Per Week 30 Last Salary $52,000/year **Supervisor** Nancy Smith
Reason For Leaving New opportunity	**May We Contact This Employer?** ☒ Yes ☐ No	

To 3/2023: *The individual's previously listed position ended over a year before this position began. Gaps in employment may represent a security concern if the individual does not account for the time unemployed and the means of support.*

Conclusion

Case Study: Opening the Espionage Case

As the investigation continued, the FBI uncovered further evidence that Kevin Mallory posed a risk to national security. When they executed a search warrant on his home, they found the smartphone that had been used as a covert communication device – hidden in the drawer in a closet and wrapped in aluminum foil. The investigation revealed text messages between Mallory and the Chinese contact, in which Mallory said he could bring the remainder of the documents on another trip.

FBI forensic analysis of the device also revealed a handwritten index describing eight different documents, later determined to be classified. Four of the documents listed in the index were stored on the device, with three being confirmed as containing classified information. Two of those documents were classified as Secret – and one was classified *Top Secret*.

At this point in the case, a number of PRIs were apparent, including:

- Previous access to classified information
- Foreign connections
- Technical activity
- Security compliance
- Financial issues

Lesson 6: Sharing and Reporting Information

Introduction

Objectives

In this lesson, we'll discuss your responsibility to report certain kinds of information.

Here are the lesson objectives. Take a moment to review them.

- Assess circumstances to determine which information may be shared within an Insider Threat Program or referred outside of the Program
- Identify requirements to consider when reporting records and data
- Identify reportable potential risk indicators (PRIs)

Welcome

Analyst: "She has several indicators that may increase her risk of becoming a threat."

Sharing and Reporting

Internal Sharing

The information and indicators you gather about an individual are shared with your Insider Threat Program so the Program can make a risk determination and identify potential mitigation response options. Consult your organization's Insider Threat Program Standard Operating Procedures (SOP) for guidance on how information is shared within your program.

External Reporting

Certain types of information may meet thresholds for referral outside your Insider Threat Program.

Per Section 811 of the Intelligence Authorization Act, all DOD and Federal Insider Threat Programs must report the possible or probable loss or compromise of classified information to the Federal Bureau of Investigation (FBI) immediately. Under 32 CFR Part 117.8 of the National Industrial Security Program Operating Manual (NISPOM) Rule, Insider Threat Programs in cleared industry must report actual, probable, or possible espionage, sabotage, terrorism, or subversive activities to the FBI. Once referral to the FBI is made, your Program must halt activity related to the referred action until the appropriate authorities provide guidance to resume.

In addition to reporting to the FBI, DOD Insider Threat Programs may be required to notify their cognizant Military Department Counterintelligence Office in accordance with DOD Instruction (DODI) 5240.10, Counterintelligence in the Combatant Commands and Other DOD Components, and under the guidance of General Counsel. Industry Insider Threat Programs must notify the Defense Counterintelligence and Security Agency (DCSA) when there is a possible or probable loss of classified information.

The Intelligence Authorization Act contains FBI reporting requirements for all Government Insider Threat Programs, including the DOD's. Industry Insider Threat Programs should refer to the NISPOM for the applicable FBI reporting requirements. Visit the Course Resources page to access a job aid about Section 811 reporting requirements.

Term	Explanation
Report	If you find reportable information, escalate it for immediate review by supervisors or team members within your Insider Threat Program who are responsible for referral actions or act in accordance with your Insider Threat Program SOP.

Additional DOD Reporting Requirements

DOD Components must also report information related to:

- Imminent threats of harm or violence to self or others
- Destruction or compromise of resources, including facilities, personnel, and information
- Conduct of criminal activity
- Any information that meets a reporting threshold established by the DOD Insider Threat Management and Analysis Center (DITMAC)

DOD Insider Threat Programs should contact the DITMAC for the current thresholds. To learn more, refer to the DITMAC Short available on the CDSE website.

Term	Explanation
Report	If you find reportable information, escalate it for immediate review by supervisors or team members within your Insider Threat Program who are responsible for referral actions or act in accordance with your Insider Threat Program SOP.

Term	Explanation
DITMAC	DOD Insider Threat Management and Analysis Center • Provides a centralized capability within the DOD to consolidate and analyze specified DOD reporting of potentially adverse information • Assesses cases, recommends intervention/mitigation, and tracks case action on threats insiders may pose

Legal Considerations

Remember that you are still bound to protect the privacy and personal information of the individual in accordance with policy and regulation. Whether sharing information internally or reporting information outside your Insider Threat Program, you must:

- Transmit the information securely
- Protect the privacy of the individual
- Be cognizant of the presence of personally identifiable information (PII) or Health Insurance Portability and Accountability Act (HIPAA) information
- Consider the classification level of the information

Consult your General Counsel with questions about sharing and reporting protected information.

Review Activities

Analyst: "She has several indicators that may increase her risk of becoming a threat."

Supervisor: "What is the next course of action?"

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

Review Activity 1

Which types of information must be shared or reported?

- ☐ Unreported foreign travel
- ☐ Unexplained employment gaps
- ☐ Possible loss of classified information
- ☐ Inconsistent education history

Review Activity 2

Which types of information require special handling when sharing or reporting?

- ☐ Personally identifiable information (PII)
- ☐ Health Insurance Portability and Accountability Act (HIPAA) information
- ☐ Classified information

Conclusion

Case Study: Undercover Operation

Mallory reached out to former colleagues at the Central Intelligence Agency, or CIA, inquiring about current intelligence on China. They found this suspicious and reported him to CIA security.

Mallory worked with Chinese Intelligence and provided them with classified information. On his way back from a covert trip to China, Mallory was stopped by Customs Border Protection, or CBP. Mallory lied about the purpose of his trip, how much money he had with him, and the phone they discovered in his belongings. The phone was a covert communication device given to him by Chinese Intelligence.

Mallory started to get nervous that the CIA and FBI were onto him, so *he* reached out to the CIA. He had a cover story ready, in an attempt to control the narrative. The CIA called Mallory in for a voluntary interview. During the interview, Mallory said he believed he was being recruited by Chinese intelligence. He lied and said he had *not* sent them any information.

Two weeks later, Mallory arrived for a second meeting with the CIA. When he arrived, the FBI was waiting for him, with a computer forensic examiner. Mallory agreed to show them how the phone worked as a covert communication device. He thought he had deleted all transmitted information and was surprised when texts and documents were shown to him on the device. Four weeks later, the FBI arrested Kevin Mallory.

Lesson 7: Course Conclusion

Conclusion

Case Study: Outcome

Former CIA officer, Kevin Mallory, was sentenced to 20 years in prison for conspiring to transmit national defense information to the People's Republic of China.

Mallory was first approached by Chinese intelligence officers using a fake profile on a social networking platform. Mallory was convicted under the Espionage Act of:

- Conspiracy to transmit,
- Attempted delivery, and
- Delivery of defense information to an agent of the People's Republic of China.

He was also convicted of making false statements to the FBI. Mallory was sentenced to 20 years in prison to be followed by five years of supervised release. Refer to the Course Resources page for a summary of this case study.

Lesson Review

Here is a list of the lessons in the course.

- Lesson 1: Course Introduction
- Lesson 2: Records Checks Overview
- Lesson 3: Locating Information
- Lesson 4: Verifying and Corroborating Information
- Lesson 5: Identifying Indicators
- Lesson 6: Sharing and Reporting Information
- Lesson 7: Course Conclusion

Lesson Summary

Congratulations. You have completed the *Insider Threat Records Checks* course.

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

- Explain how records checks support the identification of anomalous behavior associated with potential insider threats
- Summarize legal and other requirements to consider when accessing, handling, and reporting records and data
- Demonstrate how to locate information about potential insider threats

- Assess the veracity of the information found in records
- Determine potential risk indicators in records, databases, and other electronic forms of information
- Assess circumstances to determine which information may be shared within an Insider Threat Program or referred outside of the Program

To receive course credit, you must take the *Insider Threat Records Checks* examination. Please use the STEPP system from the Center for Development of Security Excellence to access the online exam.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

How will performing a records check on Ivanka support your Insider Threat Program's goals?

- ❒ It will help the Program to corroborate or mitigate what Ivanka's colleagues reported. *(correct response)*
- ❒ The additional information will allow the Program to develop an appropriate mitigation strategy. *(correct response)*
- ☐ It will build a case for your Program to automatically terminate Ivanka's employment.

***Feedback**: Records checks allow Insider Threat Programs to develop additional information that may corroborate or mitigate existing insider threat indicators and to evaluate a potential insider threat with the goal of developing mitigation response actions. The response does not always necessarily result in termination of employment.*

Review Activity 2

What types of information should you attempt to gather about Ivanka?

- ○ Birth and citizenship
- ○ Education
- ○ Finances
- ○ Law enforcement
- ○ Military
- ○ Foreign travel
- ○ Residence
- ○ Civil court
- ○ Medical
- ○ Employment and personnel
- ⊙ All of the above *(correct response)*

***Feedback**: All of these are types of records and information to seek about an individual.*

Review Activity 3

Question 1 of 3. You've received a copy of Ivanka's personnel file. It contains personal information, including her social security number and birth date. What should you do?

- ○ Request a release from Ivanka.
- ○ Thank the records custodians for their time.
- ○ Provide a Privacy Act advisement.
- ◉ Take special precautions to protect personally identifiable information (PII). *(correct response)*
- ○ Destroy the record.

Feedback*: You should always protect personally identifiable information.*

Question 2 of 3. You call the registrar's office at Ivanka's university to confirm her graduation date. What should you do?

- ○ Request a release from Ivanka.
- ○ Thank the records custodians for their time.
- ◉ Provide a Privacy Act advisement. *(correct response)*
- ○ Take special precautions to protect personally identifiable information (PII).
- ○ Destroy the record.

Feedback*: You must provide Privacy Act advisements to records custodians.*

Question 3 of 3. The registrar asks you to provide a signed release in order to give you the information. What should you do?

- ○ Request a release from Ivanka.
- ◉ Thank the records custodians for their time. *(correct response)*
- ○ Provide a Privacy Act advisement.
- ○ Take special precautions to protect personally identifiable information (PII).
- ○ Destroy the record.

Feedback*: To protect the viability of future response options, you should NOT request a signed release or take any other actions that may alert the individual.*

Lesson 3 Review Activities

Review Activity 1

Question 1 of 4. Which data source(s) contain education information?

- ❒ Personnel Security Investigation (PSI) File *(correct response)*
- ☐ Defense Manpower Data Center (DMDC)
- ☐ Student and Exchange Visitor Information System (SEVIS) *(correct response)*
- ☐ Financial Crimes Enforcement Network (FinCEN)
- ☐ TECS (formerly known as the Treasury Enforcement Communications System)

***Feedback**: The PSI file (DOD only) is the most comprehensive source of information available about the individual and SEVIS provides information related to student exchange.*

Question 2 of 4. Which data source(s) contain foreign travel information?

- ❒ Personnel Security Investigation (PSI) File *(correct response)*
- ❒ Defense Manpower Data Center (DMDC) *(correct response)*
- ☐ Student and Exchange Visitor Information System (SEVIS) *(correct response)*
- ☐ Financial Crimes Enforcement Network (FinCEN)
- ☐ TECS (formerly known as the Treasury Enforcement Communications System) *(correct response)*

***Feedback**: The PSI file, DMDC, TECs, and SEVIS may contain foreign travel information.*

Question 3 of 4. Which data source(s) contain residential information?

- ❒ Personnel Security Investigation (PSI) File *(correct response)*
- ❒ Defense Manpower Data Center (DMDC) *(correct response)*
- ☐ Student and Exchange Visitor Information System (SEVIS) *(correct response)*
- ☐ Financial Crimes Enforcement Network (FinCEN)
- ☐ TECS (formerly known as the Treasury Enforcement Communications System)

***Feedback**: The PSI file, DMDC, and SEVIS may contain residential information.*

Question 4 of 4. Which data source(s) contain financial information?

- ❒ Personnel Security Investigation (PSI) File *(correct response)*
- ☐ Defense Manpower Data Center (DMDC)
- ☐ Student and Exchange Visitor Information System (SEVIS)
- ☐ Financial Crimes Enforcement Network (FinCEN) *(correct response)*
- ❒ TECS (formerly known as the Treasury Enforcement Communications System)

***Feedback**: The PSI file and FinCEN may contain financial information.*

Lesson 4 Review Activities

Review Activity 1

What are some possible consequences of not verifying the information uncovered about Ivanka?

- ❒ The information could have a detrimental impact on Ivanka's career, even if it turns out to be untrue. *(correct response)*
- ❒ The Insider Threat Program could inaccurately assess the risk Ivanka poses as an insider threat. *(correct response)*
- ❒ The Insider Threat Program could employ an inappropriate or inadequate mitigation response. *(correct response)*

***Feedback**: These are all reasons it is important to verify and corroborate information.*

Review Activity 2

Is this social media post a primary source or a secondary source?

- ○ Primary source
- ⦿ Secondary source *(correct response)*

***Feedback**: A social media post is an example of a secondary source.*

Review Activity 3

Which of the following would be the best way to verify and corroborate this news item?

- ○ Ask Ivanka's friends about it.
- ⦿ Get a copy of the police report. *(correct response)*
- ○ Find it mentioned in a newspaper.
- ○ Ask the police beat reporter about it.

***Feedback**: Cross-checking the information with a primary source like a police report is good technique.*

Lesson 6 Review Activities

Review Activity 1

Which types of information must be shared or reported?

- ☐ Unreported foreign travel *(correct response)*
- ☐ Unexplained employment gaps *(correct response)*
- ☐ Possible loss of classified information *(correct response)*
- ☐ Inconsistent education history *(correct response)*

***Feedback**: All of these types of information must be reported to your Insider Threat Program – and should be referred to the FBI or DCSA as appropriate.*

Review Activity 2

Which types of information require special handling when sharing or reporting?

- ❒ Personally identifiable information (PII) *(correct response)*
- ❒ Health Insurance Portability and Accountability Act (HIPAA) information *(correct response)*
- ❒ Classified information *(correct response)*

***Feedback:** PII, HIPAA information, and classified information require special handling.*

Data Types and Sources Matrix

Insider Threat Indicators in Records Checks

This table cross-references data sources used in records checks with the types of records and information they may contain.

	Employment Information	Military Records	Medical Records	Law Enforcement Records	Civil Court Records	Financial Records	Residential Information	Education Information	Foreign Travel Information	Birth & Citizenship Information	Other Information
Personnel Security Investigation (PSI) File	X	X	X	X	X	X	X	X	X	X	X
Defense Manpower Data Center (DMDC)	X	X				X					
Defense Central Index of Investigations (DCII)											X
Defense Information System for Security (DISS)											X
DITMAC System of Systems (DSOS)											X
Human Resources	X										
Student and Exchange Visitor Information System (SEVIS)							X	X	X	X	
Financial Crimes Enforcement Network (FinCEN)						X					
National Crime Information Center (NCIC)				X							
TECS (formerly Treasury Enforcement Communications System)									X		
Consolidated Screening List											X
Direct Contact with Federal Agencies											X
Internet / Open Source Search	X						X	X			X