# *Insider Threat Records Checks*

## Student Guide

August 2020

*Center for Development of Security Excellence*

# Lesson 1: Course Introduction

## Introduction

### Welcome

A prominent scientist with a Ph.D. from the Massachusetts Institute of Technology. A contributor to our nation’s sensitive nuclear and satellite programs. A developer of cutting-edge defense and space technology. A long-trusted contractor granted access to Top Secret information. An insider threat.

> *Stewart Nozette:*
>
> *“Okay, so I gave you, even in this first run, some of the most classified information that there is. And so—I need a—I’ve sort of crossed the Rubicon in the sense that I can’t go back and take a CI polygraph now.”*

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 Stewart David Nozette 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
- Identify 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

### *Welcome*

*Colleague 1: "I don't know where he gets his money, but it seems like Carl is always driving a new car—and they are NICE cars."*

*Colleague 2: "That guy is always poking around on the network, saying how weak our security is. He says a child could hack it."*

*Colleague 3: "A couple of us were talking about a documentary we'd seen about the Vietnam War. Carl got pretty angry. He said he could never support a government that handled the war so badly."*

### *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

## 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. Note that 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, but 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 check out. A few people have noticed some possible indicators for Carl, the IT guy. Can you look into his records and let me know what you find?”*

### *Review Activity 1*

How will performing a records check on Carl 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 Carl’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 Carl’s employment.

### *Review Activity 2*

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

*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 Carl's personnel file. It contains personal information, including his 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 Carl.
○ 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 Carl's university to confirm his 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 Carl.
○ 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 Carl.
○ 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 Stewart Nozette, 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.

Nozette's scientific expertise opened the door for his access to highly classified—and highly valuable—information. For more than 15 years, he performed work for U.S. Government agencies, including the White House's National Space Council and the Department of Energy's Lawrence Livermore National Laboratory. In support of his work, he held security clearances as high as Top Secret and had regular, frequent access to classified information. During his work with the Government, he formed a non-profit organization called the Alliance for Competitive Technology (ACT) for which he served as president, treasurer, and director. Over a period of six years, Nozette entered into agreements through ACT with the U.S. Naval Research Laboratory (NRL), the Defense Advanced Research Projects Agency (DARPA), and the National Aeronautics and Space Administration (NASA).

# Lesson 3: Locating Information

## Introduction

### Welcome

Analyst: “That’s odd—why was Carl here at 1 a.m.?”

### 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

## 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.

DoD Component Insider Threat Programs may be able to access additional Department or Component 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<br>• Provides a centralized capability within the DoD to consolidate and analyze specified DoD reporting of potentially adverse information<br>• 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 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. Reinvestigations occur every five years, so the PSI file may not be up to date. Continue to review other sources and assess whether any changes have occurred since the last investigation.

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

| Term | Definition |
|---|---|
| DBIDS | Defense Biometric Identification System<br>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<br>• 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.

### *Federal Information Sources*

Sources of Federal information include:

- Human resources
- The National Personnel Records Center (NPRC)
- 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.

### National Personnel Records Center (NPRC)

The NPRC is an organization within the National Archives in St. Louis, Missouri. It holds individual Federal civilian and military personnel records dating back to the 19th century. The NPRC may be able to provide personnel and military files for your individual. Visit the Course Resources page to access the NPRC 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 United States 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. Seek guidance from your General Counsel before attempting to review or access these records.

**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 Carl'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)
- □ National Personnel Records Center (NPRC)
- □ National Crime Information Center (NCIC)

Question 2 of 4. Which data source(s) contain military service 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)
- □ National Personnel Records Center (NPRC)
- □ National Crime Information Center (NCIC)

Question 3 of 4. Which data source(s) contain employment history 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)
- □ National Personnel Records Center (NPRC)
- □ National Crime Information Center (NCIC)

Question 4 of 4. Which data source(s) contain criminal history 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)

□ National Personnel Records Center (NPRC)

□ National Crime Information Center (NCIC)

# 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 Stewart Nozette came about due to allegations that he submitted fraudulent expense claims to the National Aeronautics and Space Administration (NASA). NASA's Office of the Inspector General (OIG) began looking into Nozette and the Alliance for Competitive Technology (ACT) through general records checks. The records revealed irregular expenses in ACT's reports to the Internal Revenue Service (IRS) and a suspicious contract. The NASA OIG referred the case to the FBI.

# *Lesson 4: Verifying and Corroborating Information*

## Introduction

### *Welcome*

***Anytown Daily News***

*Police Blotter*

*Carl Nguyen was cited for public intoxication on Hilldale Avenue at 6:00 pm.*

*Analyst: “I haven’t found this mentioned anywhere else. This should have been reported.”*

### *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

### *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.

| 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

*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 Carl?

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

□ The information could have a detrimental impact on Carl's career, even if it turns out to be untrue.

□ The Insider Threat Program could inaccurately assess the risk Carl poses as an insider threat.

□ The Insider Threat Program could employ an inappropriate or inadequate mitigation response.

### *Review Activity 2*

***Anytown Daily News***

*Police Blotter*

*Carl Nguyen was cited for public intoxication on Hilldale Avenue at 6:00 pm.*

Is this news item a primary source or a secondary source?

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

○ Primary source

○ Secondary source

### Review Activity 3

***Anytown Daily News***

*Police Blotter*

*Carl Nguyen was cited for public intoxication on Hilldale Avenue at 6:00 pm.*

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

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

○ Ask Carl's friends about it.

○ Get a copy of the police report.

○ Find it mentioned in another 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 Stewart Nozette, additional indicators of the threat he posed became evident. The FBI coordinated with the National Aeronautics and Space Administration (NASA), the Internal Revenue Service (IRS), and the Naval Criminal Investigative Service (NCIS) to interview people and check additional records, which revealed, through customs records, frequent foreign travel.

# Lesson 5: Identifying Indicators

## Introduction

### Welcome

*Analyst: "There's a lot of foreign travel. Is this a bad sign?"*

### 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.

- Identify 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

## Indicators

### Purpose and Qualities

Indicators provide a gauge to measure the state of a situation. We use them in everyday situations to get a feel for the situation and alter our behavior accordingly. For example, if you were trying to decide whether to bring an umbrella with you today, you'd look for indicators. What is the weather forecast? Are there clouds in the sky? With a sunny forecast and blue skies, you'd probably leave the umbrella at home, but you might decide to bring it when a chance of rain is forecast and the sky is overcast.

Similarly, indicators are valuable when assessing whether an insider poses a threat. 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 this a bad sign?"*

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

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

# APPLICATION FOR EMPLOYMENT

## GENERAL INFORMATION

**Name (Last, First, Middle):** Nguyen, Xuan (Carl) Ho
**Address (Mailing Address):** 124 Main St., Anytown, AK, 99501
**Home Telephone:** (800) 555-1212
**Other Telephone:** (888) 555-1212
**E-Mail Address:** JDoe@xyz.com
**Are you legally entitled to work in the U.S.?** Yes

## POSITION

**Position Or Type Of Employment Desired:** Data Entry Operator
**Are you able to perform the essential functions of the job you are applying for, with or without reasonable accommodation?** Yes
**Will Accept:** Part-Time, Full-Time, Temporary
**Shift:** Day, Swing, Graveyard, Rotating
**Salary Desired:** Negotiable
**Date Available:** Immediately
**How did you learn about our company?** Referred by Great Uncle
**Do you have any friends, relatives, or acquaintances working for us?** Yes
**If yes, state name, relationship, and address:** Pham Xuan Hoang An [Uncle] 6a De Tham St. Cau Ong Lanh Ward.1 Dist, Hochiminh, Saigon, Vietnam

## EDUCATION AND TRAINING

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

***College, Business School, Military (Most recent first)***

**Name and Location:** University of Texas
- **Dates Attended Month/Year:** From 08/2007 To 05/2011
- **Credits Earned | Quarterly or Semester Hours:** 120
- **Credits Earned | Other (Specify):**
- **Graduate:** Yes
- **Degree & Year:** M.S., 2011
- **Major or Subject:** Information Technology

**Name and Location:** University of Saigon
- **Dates Attended Month/Year:** From 08/1982 To 05/1987
- **Credits Earned | Quarterly or Semester Hours:** 120
- **Credits Earned | Other (Specify):**
- **Graduate:** Yes
- **Degree & Year:** B.S., 1987
- **Major or Subject:** History

**MILITARY SERVICE INFORMATION (Most recent)**

**Branch of Service:** Army of the Republic of Vietnam
**Date of Entry:** April 22, 1990
**Date of Discharge:** April 21, 1997

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

- Loyalty Medal (State of Vietnam)
- Military Merit Medal (State of Vietnam)

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

**Employer:** Generic Industries, Inc.

**Telephone Number:** (877) 555-1212
**Address:** 9876 South St., Anycity, OK 73101
**Job Title:** Network Administrator
**Number of Employees Supervised:** 12
**From (Month/Year):** 09/2008
**To (Month/Year):** 03/2012
**Hours Per Week:** 40
**Last Salary:** $53,500/year
**Supervisor:** David Manning
**Specific Duties:**

- Established network specifications and security requirements.
- Evaluated network performance issues including availability, utilization, throughput, goodput, and latency
- Defined network policies and procedures.
- Performed network monitoring and analysis, and performance tuning; troubleshooting network problems; escalating problems to vendor.
- Secures network by developing network access, monitoring, control, and evaluation; maintaining documentation.
- Design and conducted user training programs.
- Upgraded network by developing, testing, evaluating, and installing enhancements.

**Reason For Leaving:** Returned home to care for sick mother.
**May We Contact This Employer?** Yes

**Employer:** Smith Electronics, Inc.

**Telephone Number:** (866) 555-1212
**Address:** 7812 Broadway, Mytown, VT
**Job Title:** IT Specialist
**Number of Employees Supervised:** 0
**From (Month/Year):** 06/2000
**To (Month/Year):** 06/2004
**Hours Per Week:** 40

**Last Salary:** $48,000/year

**Supervisor:** Julius Jones

**Specific Duties:** Identifies client requirements by establishing personal rapport with potential and actual clients and other persons in a position to understand service requirements.

- Collected data by identifying sources of information and designing survey and collection methods.
- Organized information by studying, analyzing, interpreting, and classifying data.
- 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.
- Established and revised database by conferring with analysts and programmers to code and retrieve data.
- Maintained database by entering data.

**Reason For Leaving:** New opportunity

**May We Contact This Employer?** Yes

**Employer:** Johnson Temps, Inc.

**Telephone Number:** (800) 555-1212

**Address:** 1122 Standard Rd., Nowhere, MA 01004

**Job Title:** Data Entry Specialist

**Number of Employees Supervised:** 0

**From (Month/Year):** 07/1999

**To (Month/Year):** 03/2000

**Hours Per Week:** 28-32

**Last Salary:** $15/hour

**Supervisor:** Janet Hudson

**Specific Duties:**

- Prepared source data for computer entry by compiling and sorting information; establishing entry priorities.
- Processed customer and account source documents by reviewing data for deficiencies
- Resolved discrepancies by using standard procedures or returning incomplete documents to the team leader for resolution.
- Entered customer and account data by inputting alphabetic and numeric information on keyboard or optical scanner according to screen format.
- Maintained data entry requirements by following data program techniques and procedures.
- Verified entered data by reviewing, correcting, deleting, or reentering data
- Secured information by completing data base backups.

**Reason For Leaving:** Found full-time work
**May We Contact This Employer?** Yes

**CERTIFICATIONS AND LICENSES**

**Occupational License, Certificate or Registration:** Cisco Certified Network Professional (CCNP)
**Number:** 12345
**Where Issued:** Texas
**Expiration Date:** 11/21/2018

**Occupational License, Certificate or Registration:** CompTIA Network+
**Number:** 54321
**Where Issued:** Oklahoma
**Expiration Date:** 07/15/2017

**CRIMINAL HISTORY**

**Have you ever been convicted of a criminal offense (felony or misdemeanor)?** Yes
**If yes, please state the 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:** Oklahoma Lion's Club
**Leadership positions held:** President 2008 – 2009
**Dates of membership:** 2006 – Present

**Organization:** Vietnamese Social Club
**Leadership positions held:** None
**Dates of membership:** 1992 – 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 two PRIs in this section. Can you find them both?

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

**GENERAL INFORMATION**

**Name (Last, First, Middle):** Nguyen, Xuan (Carl) Ho
**Address (Mailing Address):** 124 Main St., Anytown, AK, 99501
**Home Telephone:** (800) 555-1212
**Other Telephone:** (888) 555-1212
**E-Mail Address:** JDoe@xyz.com
**Are you legally entitled to work in the U.S.?** Yes

**POSITION**

**Position Or Type Of Employment Desired:** Data Entry Operator
**Are you able to perform the essential functions of the job you are applying for, with or without reasonable accommodation?** Yes
**Will Accept:** Part-Time, Full-Time, Temporary
**Shift:** Day, Swing, Graveyard, Rotating
**Salary Desired:** Negotiable
**Date Available:** Immediately
**How did you learn about our company?** Referred by Great Uncle
**Do you have any friends, relatives, or acquaintances working for us?** Yes
**If yes, state name, relationship, and address:** Pham Xuan Hoang An [Uncle] 6a De Tham St. Cau Ong Lanh Ward.1 Dist, Hochiminh, Saigon, Vietnam

### *Part 1 – Answer Key*

There are two PRIs in this section. Can you find them both?

**GENERAL INFORMATION**

**Name (Last, First, Middle):** Nguyen, Xuan (Carl) Ho

**Address (Mailing Address):** 124 Main St., Anytown, AK, 99501

**Home Telephone:** (800) 555-1212

**Other Telephone:** (888) 555-1212

**E-Mail Address:** JDoe@xyz.com

**Are you legally entitled to work in the U.S.?** Yes

**POSITION**

**Position Or Type Of Employment Desired:** Data Entry Operator *(correct response)*

**Are you able to perform the essential functions of the job you are applying for, with or without reasonable accommodation?** Yes

**Will Accept:** Part-Time, Full-Time, Temporary

**Shift:** Day, Swing, Graveyard, Rotating

**Salary Desired:** Negotiable

**Date Available:** Immediately

**How did you learn about our company?** Referred by Great Uncle

**Do you have any friends, relatives, or acquaintances working for us?** Yes

**If yes, state name, relationship, and address:** Pham Xuan Hoang An [Uncle] 6a De Tham St. Cau Ong Lanh Ward.1 Dist, Hochiminh, Saigon, Vietnam *(correct response)*

***Data Entry Operator:*** *This applicant is applying for a job much below his 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.*

***Pham Xuan Hoang An:*** *A name check reveals that Pham Xuan Hoang An is the son of Pham Xuan An. Phạm Xuan An was a Vietnamese journalist and correspondent for Time (magazine), Reuters, and the New York Herald Tribune, stationed in Saigon during the war in Vietnam. He was also simultaneously spying for North Vietnam. He was made a general after the war. He was awarded the "People's Army Force Hero" by the Vietnamese government on January 15, 1976.*

### *Part 2*

There are two PRIs in this section. Can you find them both?

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

**EDUCATION AND TRAINING**

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

***College, Business School, Military (Most recent first)***

**Name and Location:** University of Texas
**Dates Attended Month/Year:** From 08/2007 To 05/2011
**Credits Earned | Quarterly or Semester Hours:** 120
**Credits Earned | Other (Specify):**
**Graduate:** Yes
**Degree & Year:** M.S., 2011
**Major or Subject:** Information Technology

**Name and Location:** University of Saigon
**Dates Attended Month/Year:** From 08/1982 To 05/1987
**Credits Earned | Quarterly or Semester Hours:** 120
**Credits Earned | Other (Specify):**
**Graduate:** Yes
**Degree & Year:** B.S., 1987
**Major or Subject:** History

### *Part 2 – Answer Key*

There are two PRIs in this section. Can you find them both?

**EDUCATION AND TRAINING**

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

***College, Business School, Military (Most recent first)***

**Name and Location:** University of Texas
**Dates Attended Month/Year:** From 08/2007 To 05/2011
**Credits Earned | Quarterly or Semester Hours:** 120
**Credits Earned | Other (Specify):**
**Graduate:** Yes
**Degree & Year:** M.S., 2011
**Major or Subject:** Information Technology *(correct response)*

**Name and Location:** University of Saigon *(correct response)*
**Dates Attended Month/Year:** From 08/1982 To 05/1987
**Credits Earned | Quarterly or Semester Hours:** 120
**Credits Earned | Other (Specify):**
**Graduate:** Yes
**Degree & Year:** B.S., 1987
**Major or Subject:** History

***M.S., Information Technology:*** *This applicant is applying for a job much below his 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.*

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

### *Part 3*

There are two PRIs in this section. Can you find them both?

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

**MILITARY SERVICE INFORMATION (Most recent)**

**Branch of Service:** Army of the Republic of Vietnam  
**Date of Entry:** April 22, 1990  
**Date of Discharge:** April 21, 1997

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

- Loyalty Medal (State of Vietnam)
- Military Merit Medal (State of Vietnam)

### *Part 3 – Answer Key*

There are two PRIs in this section. Can you find them both?

**MILITARY SERVICE INFORMATION (Most recent)**

**Branch of Service:** Army of the Republic of Vietnam
**Date of Entry:** April 22, 1990
**Date of Discharge:** April 21, 1997 *(correct response)*

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

- Loyalty Medal (State of Vietnam)
- Military Merit Medal (State of Vietnam) *(correct response)*

***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.*

### *Part 4*

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

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

**Employer:** Generic Industries, Inc.

**Telephone Number:** (877) 555-1212

**Address:** 9876 South St., Anycity, OK 73101

**Job Title:** Network Administrator

**Number of Employees Supervised:** 12

**From (Month/Year):** 09/2008

**To (Month/Year):** 03/2012

**Hours Per Week:** 40

**Last Salary:** $53,500/year

**Supervisor:** David Manning

**Specific Duties:**

- Established network specifications and security requirements.
- Evaluated network performance issues including availability, utilization, throughput, goodput, and latency
- Defined network policies and procedures.
- Performed network monitoring and analysis, and performance tuning; troubleshooting network problems; escalating problems to vendor.
- Secures network by developing network access, monitoring, control, and evaluation; maintaining documentation.
- Design and conducted user training programs.
- Upgraded network by developing, testing, evaluating, and installing enhancements.

**Reason For Leaving:** Returned home to care for sick mother.

**May We Contact This Employer?** Yes

### *Part 4 – Answer Key*

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

**Employer:** Generic Industries, Inc.

**Telephone Number:** (877) 555-1212

**Address:** 9876 South St., Anycity, OK 73101

**Job Title:** Network Administrator

**Number of Employees Supervised:** 12

**From (Month/Year):** 09/2008 *(correct response)*

**To (Month/Year):** 03/2012

**Hours Per Week:** 40

**Last Salary:** $53,500/year

**Supervisor:** David Manning

**Specific Duties:**

- Established network specifications and security requirements.
- Evaluated network performance issues including availability, utilization, throughput, goodput, and latency
- Defined network policies and procedures.
- Performed network monitoring and analysis, and performance tuning; troubleshooting network problems; escalating problems to vendor.
- Secures network by developing network access, monitoring, control, and evaluation; maintaining documentation.
- Design and conducted user training programs.
- Upgraded network by developing, testing, evaluating, and installing enhancements.

**Reason For Leaving:** Returned home to care for sick mother.

**May We Contact This Employer?** Yes

***From 09/2008:*** *The individual's previously listed position ended four years 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.*

### *Part 5*

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

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

**CERTIFICATIONS AND LICENSES**

**Occupational License, Certificate or Registration:** Cisco Certified Network Professional (CCNP)
**Number:** 12345
**Where Issued:** Texas
**Expiration Date:** 11/21/2018

**Occupational License, Certificate or Registration:** CompTIA Network+
**Number:** 54321
**Where Issued:** Oklahoma
**Expiration Date:** 07/15/2017

**CRIMINAL HISTORY**

**Have you ever been convicted of a criminal offense (felony or misdemeanor)?** Yes
**If yes, please state the 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:** Oklahoma Lion’s Club
**Leadership positions held:** President 2008 – 2009
**Dates of membership:** 2006 – Present

**Organization:** Vietnamese Social Club
**Leadership positions held:** None
**Dates of membership:** 1992 – Present

### *Part 5 – Answer Key*

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

**CERTIFICATIONS AND LICENSES**

**Occupational License, Certificate or Registration:** Cisco Certified Network Professional (CCNP)
**Number:** 12345
**Where Issued:** Texas
**Expiration Date:** 11/21/2018

**Occupational License, Certificate or Registration:** CompTIA Network+
**Number:** 54321
**Where Issued:** Oklahoma
**Expiration Date:** 07/15/2017 *(correct response)*

**CRIMINAL HISTORY**

**Have you ever been convicted of a criminal offense (felony or misdemeanor)?** Yes
**If yes, please state the nature of the crime(s), when and where convicted and disposition of the case:** Trespassing *(correct response)*

**HOBBIES AND ACTIVITIES (List all memberships, associations, or other activities and pursuits)**

**Organization:** Oklahoma Lion’s Club
**Leadership positions held:** President 2008 – 2009
**Dates of membership:** 2006 – Present

**Organization:** Vietnamese Social Club
**Leadership positions held:** None
**Dates of membership:** 1992 – Present

***Certifications and Licenses:*** *This applicant is applying for a job much below his 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 the personal, professional, or financial reasons that impel most job searches.*

***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.*

# Conclusion

### *Case Study: Opening the Espionage Case*

As the fraud investigation continued, law enforcement uncovered further evidence that Stewart Nozette posed a risk to national security. When they executed a search warrant on his home, they found classified documents. Continued investigation into the classified documents revealed an email Nozette sent five years earlier in which he threatened to sell classified information. At this point in the case, a number of PRIs were apparent, including access to classified information, foreign preference, criminal conduct, and financial issues.

# Lesson 6: Sharing and Reporting Information

## Introduction

### *Welcome*

*Analyst: "He has a lot of security violations. This could be a big problem."*

### *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)

## 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 Chapter 1, Section 301 of the National Industrial Security Program Operating Manual (NISPOM) 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.

| 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.

| 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<br>• Provides a centralized capability within the DoD to consolidate and analyze specified DoD reporting of potentially adverse information<br>• 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: "He has a lot of security violations. This could be a big problem."*

*Supervisor: "What are you going to do about it?"*

### *Review Activity 1*

Question 1 of 4. What action would you take with unreported foreign travel?

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

○ Share

○ Report

○ Ignore

Question 2 of 4. What action would you take with unexplained employment gaps?

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

○ Share

○ Report

○ Ignore

Question 3 of 4. What action would you take with possible loss of classified information?

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

○ Share

○ Report

○ Ignore

Question 4 of 4. What action would you take with inconsistent education history?

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

○ Share

○ Report

○ Ignore

### *Review Activity 2*

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

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

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

# Conclusion

### *Case Study: Undercover Operation*

Based on the PRIs uncovered in the fraud investigation and the Federal Bureau of Investigation (FBI)'s subsequent inquiry, the FBI decided to conduct an undercover operation. An undercover FBI agent contacted Stewart Nozette via telephone, claiming to be an Israeli intelligence officer from the Mossad. Nozette met with the undercover agent several times and provided classified information, including details about U.S. satellites, early warning systems, and defense strategy, in exchange for $11,000.

Please note that there was no allegation that the government of Israel or anyone acting on its behalf committed any offense under U.S. laws in this case.

# Lesson 7: Course Conclusion

## Conclusion

### Case Study: Outcome

> *Stewart Nozette:*
>
> *“And then—that’s not including the launching and integrating the satellites. So if you say, okay, that probably brings it to almost a billion dollars, but the part of it that’s the information—that was to fly, so it’s okay now you have a flight. So it’s at least $200 million, so I would say, you know, theoretically, I should charge you certainly, you know, at most one percent.”*

Stewart Nozette was arrested soon after this meeting. Nozette was charged with attempted espionage, and in the fraud case he was charged with conspiracy to defraud the United States and tax evasion. He was sentenced to 13 years in prison and a $217,000 fine. Refer to the end of this Student Guide for a summary of this case study.

### 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
- Identify 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. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to register for the online exam. Otherwise, select the Take Exam button on the last screen of the course to take the online exam and receive your certificate.

# Appendix A: Answer Key

## Lesson 2 Review Activities

### Review Activity 1

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

☑ It will help the Program to corroborate or mitigate what Carl'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 Carl'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 Carl?

○ 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 Carl's personnel file. It contains personal information, including his social security number and birth date. What should you do?

- ○ Request a release from Carl.
- ○ 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 Carl's university to confirm his graduation date. What should you do?

- ○ Request a release from Carl.
- ○ 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 Carl.
- ⦿ 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)
□ National Personnel Records Center (NPRC)
□ National Crime Information Center (NCIC)

***Feedback**: The PSI file (DoD only) is the most comprehensive source of information available about the individual.*

Question 2 of 4. Which data source(s) contain military service information?

☑ Personnel Security Investigation (PSI) File *(correct response)*
☑ Defense Manpower Data Center (DMDC) *(correct response)*
☑ National Personnel Records Center (NPRC) *(correct response)*
□ National Crime Information Center (NCIC)

***Feedback**: The PSI file, DMDC, and NPRC may contain military records.*

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

☑ Personnel Security Investigation (PSI) File *(correct response)*
☑ Defense Manpower Data Center (DMDC) *(correct response)*
☑ National Personnel Records Center (NPRC) *(correct response)*
□ National Crime Information Center (NCIC)

***Feedback**: The PSI file, DMDC, and NPRC may contain employment information.*

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

☑ Personnel Security Investigation (PSI) File *(correct response)*
□ Defense Manpower Data Center (DMDC)
□ National Personnel Records Center (NPRC)
☑ National Crime Information Center (NCIC) *(correct response)*

***Feedback**: The PSI file and NCIC may contain law enforcement records.*

# Lesson 4 Review Activities

## *Review Activity 1*

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

☑ The information could have a detrimental impact on Carl's career, even if it turns out to be untrue. *(correct response)*

☑ The Insider Threat Program could inaccurately assess the risk Carl 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 news item a primary source or a secondary source?

○ Primary source

⦿ Secondary source *(correct response)*

***Feedback**: A news article 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 Carl's friends about it.

⦿ Get a copy of the police report. *(correct response)*

○ Find it mentioned in another 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*

Question 1 of 4. What action would you take with unreported foreign travel?

⦿ Share *(correct response)*

○ Report

○ Ignore

***Feedback****: You should share this information with your Insider Threat Program.*

Question 2 of 4. What action would you take with unexplained employment gaps?

⦿ Share *(correct response)*

○ Report

○ Ignore

***Feedback****: You should share this information with your Insider Threat Program.*

Question 3 of 4. What action would you take with possible loss of classified information?

○ Share

⦿ Report *(correct response)*

○ Ignore

***Feedback****: You should report this information to the FBI (DoD and Federal) or DCSA (cleared industry) immediately.*

Question 4 of 4. What action would you take with inconsistent education history?

⦿ Share *(correct response)*

○ Report

○ Ignore

***Feedback****: You should share this information with your Insider Threat Program.*

### *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.*

Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

INSIDER THREAT JOB AID

# Awareness in Action: Case Study

Who could become an insider threat? Anyone with authorized access to U.S. Government resources who uses that access - either wittingly or unwittingly - to harm national security. Insider threats can have far reaching consequences and impacts on national security.

## Stewart David Nozette

- Contractor for 15+ years
- Arrest date: 07 September 2011
- Age at arrest: 54
- Charges: Pled guilty to attempted espionage
- Sentence: 13 years in prison plus $217,000 fine

## Potential Risk Indicators

- Fraudulently billed the Government
- Worked for a foreign company
- Foreign influence and preference
- Misuse of IT systems

## What Happened

- Nozette was the president, treasurer, and director of the Alliance for Competitive Technology (ACT), a non-profit organization that he began in March 1990.
- A program manager at the National Aeronautics and Space Administration (NASA) accused Nozette of padding his expenses and escalated it to the Inspector General (IG).
- The NASA IG checked Nozette's records and found that ACT had a suspicious contract. The IG referred the case to the Federal Bureau of Investigation (FBI).
- The FBI opened an inquiry that involved pulling additional records and interviewing people. Customs records reflected suspicious travel, and the FBI launched an undercover sting operation.
- An FBI undercover employee contacted Nozette via telephone purporting to be an Israeli intelligence officer. Nozette agreed to provide classified information in exchange for money and a foreign passport to a country without extradition to the United States.
- Overall, Nozette used ACT to defraud the Naval Research Laboratory (NRL), Defense Advanced Research Projects Agency (DARPA), and NASA from 2000 through 2006 and willfully evaded more than $200,000 in Federal taxes.

## Learn More

This case study examined a real-life insider threat. Your awareness is key to protecting our national security from insider threats like this one. Visit the Center for Development of Security Excellence's website (http://www.cdse.edu) for additional case studies, information, materials, and training or go directly to the Insider Threat Tool Kit at http://www.cdse.edu/toolkits/insider/index.php

If you SEE something, SAY something.

# 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 |
| **Navy Absentee Collection and Information Center (NACIC)** | | X | | | | | | | | | |
| **Human Resources** | X | | | | | | | | | | |
| **National Personnel Records Center (NPRC)** | 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 |