Insider Threat Program
Employee Training

The following training is established for all cleared employees in order to meet our DoD Manual 5220-22M, National Industrial Security Program training requirements.

Course Objectives

- Define Insider Threat
- Identify Potential Insider Threat Indicators
- Identify Recruitment Techniques
- Identify Suspicious Behavior
- Identify Reporting Requirements

What is an Insider Threat?

An Insider Threat Is:

- Anyone with authorized access to the information or things an organization values most, and uses that access either wittingly or unwittingly to inflict harm to the organization or national security.

What Do Insider Threats Look Like?

- They look like you and me.
- They look like your friends and neighbors.
- They can be anyone and target anything.

What Motivates Them?

- Money
- Ego
- A cause for another country
- Simply because they can

Insider Threat Case #1

Economic Espionage

Greg Chung, an engineer for a cleared defense contractor, stole over 250,000 documents containing trade secrets about the space shuttle, the Delta IV rocket, and the C-17 military cargo jet. He traveled to China under the guise of giving lectures while secretly meeting with Chinese agents.

In February 2010, he became the first person to be tried under the economic espionage provision of the Economic Espionage Act and was sentenced to over 15 years in prison.

Insider Threat Case #2

Wiki Leaks

The WikiLeaks case represents one of the major catalysts for an insider threat national policy.

In May 2010, Army Private Bradley Manning was arrested for allegedly leaking classified material to the website WikiLeaks. The unauthorized disclosure represents the single largest loss of classified information in U.S. history and includes 250,000 diplomatic cables and 500,000 U.S. Army reports.

Despite reservations stemming from signs of instability, Manning was deployed to Iraq, where he served as an intelligence analyst. As an intelligence analyst, he had access to the DoD's classified networks, SIPRNet and JWICS. During his time in Iraq, he was reprimanded for being persistently late, which led to him overturning a table before being restrained. Shortly after this incident, Manning allegedly began downloading sensitive material, subsequently passing it on to WikiLeaks.

Manning was convicted in July 2013 of violations of the Espionage Act and other offenses and was sentenced in August 2013 to 35 years confinement with the possibility of parole in eight years, and to be dishonorably discharged from the Army.

Insider Threat Case #3

Fort Hood Shooting

vember 2009, an Army Major killed 13 people and wounded 29 others at Fort Hood, Texas. The shooting represents the worst shooting to ever take place at an American military base.

Six months prior to the shooting, the Major had been investigated for expressing extremist views, but was determined not to be a threat as the incident was related to his professional research.

Even before that, when he worked at Walter Reed Medical Center, he had concerned colleagues with his tendency towards conflict and comments concerning the American military presence in Iraq and Afghanistan.

At his court-martial in August 2013 he was convicted of 13 counts of premeditated murder, 32 counts of attempted murder, and unanimously recommended to be formally dismissed from the service and sentenced to death. He is incarcerated at the United States Disciplinary Barracks at Fort Leavenworth in Kansas awaiting execution while his case is reviewed by appellate courts.

Recruitment

While not all insiders are recruited, those who are, are often recruited slowly over time. Recruitment almost always involves contact with individuals or organizations from foreign countries. However, an already committed U.S. spy may attempt to recruit colleagues.

- 3 Phases of Recruitment
  - ✓ Spot and Assess
  - ✓ Development
  - ✓ Handling

Spot and Assess

During this phase, adversaries are not necessarily looking for someone with a high-level access. Sometimes the potential for future access or ability of the recruit to lead to other high-value targets is enough to generate interest.

Spotting and assessing can take place anywhere, but is always approached in a non-threatening and seemingly natural manner.

Put yourself in the shoes of an intelligence officer. How would you recruit a computer scientist? Perhaps at a trade show, through a business contact, at a computer store, or another social event. Even online venues such as chat rooms and social media can be used to recruit.

Note: Online venues have become the medium of choice for intelligence officers because they can pretend to be anyone, even a friend or family member.

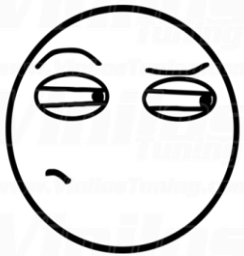
Development

During the development phase, meetings with the recruit will become more private and less likely to be observed or reported. This is when the adversary begins to cultivate a relationship with the individual. This phase could span a period of months or even years.

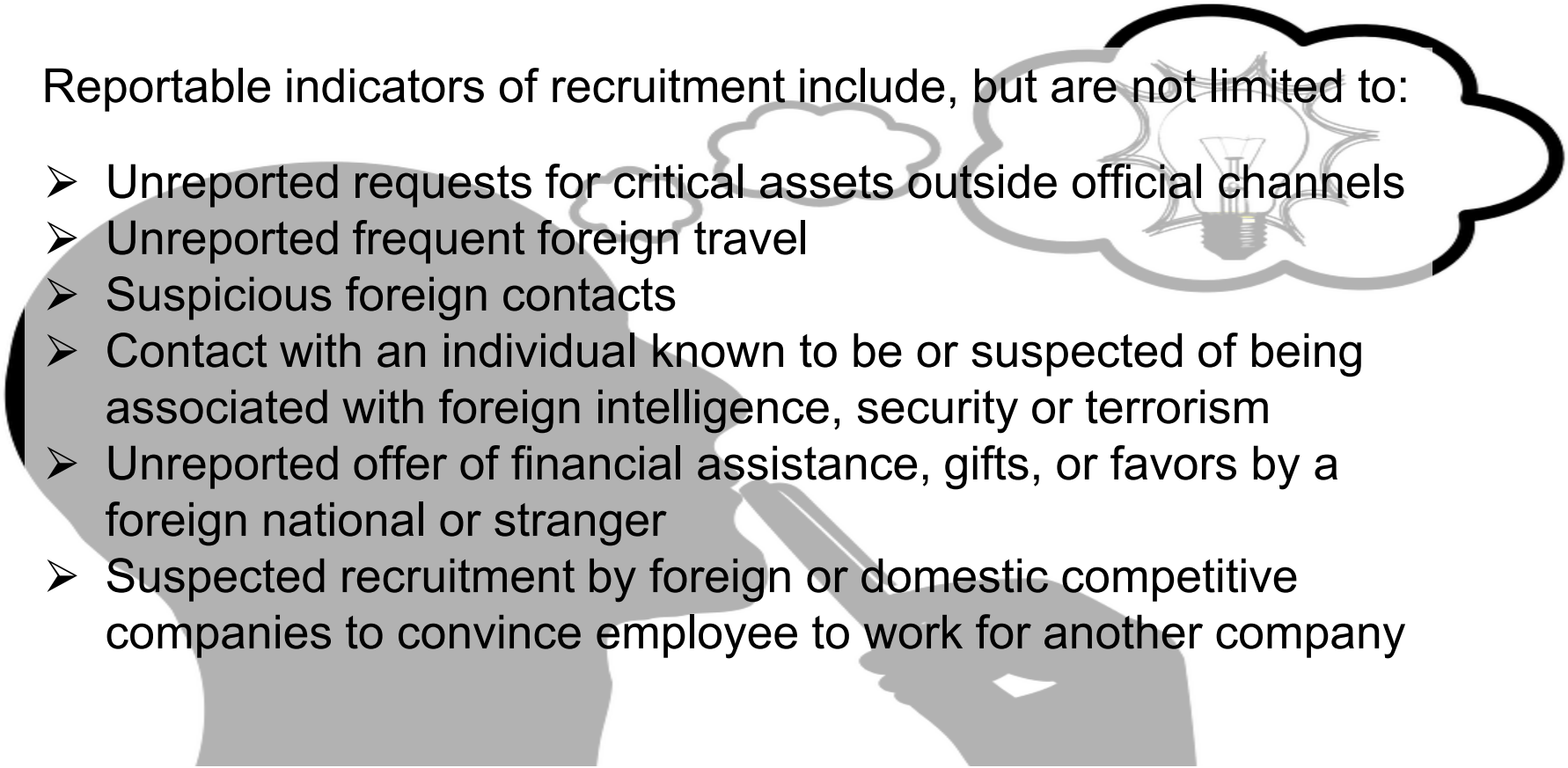
Handling

By the time the “Handling” phase is initiated, the individual is likely emotionally tied to the adversary. The actual recruitment may involve appeals to ideological learning, financial gain, blackmail, coercion, or any other of a number of motivators unique to that recruit. Some of these may manifest as observable and reportable behaviors.

Indicators of recruitment include signs of sudden or unexplained wealth and unreported foreign travel.



Recruitment Indicators



Reportable indicators of recruitment include, but are not limited to:

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

Information Collection

Before someone can steal information, they must first collect the information.

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

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

Regardless of method used, anytime a person attempts to access information without authorization, it should be of concern.

Information Collection Indicators

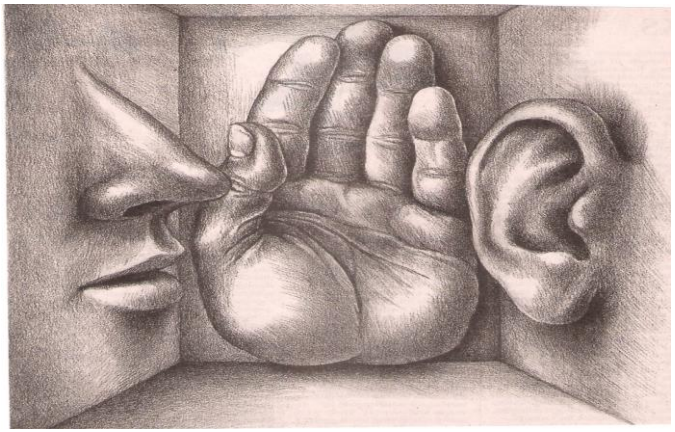
Reportable indicators of information collection include, but are not limited to:

- Unauthorized downloads or copying of files, especially for employees who have given notice of termination of employment
- Keeping critical assets at home or any other unauthorized place
- Acquiring access to automated information systems without authorization
- Using unauthorized cameras, recording devices, computers, or storage devices such as thumb drives in areas where critical assets are stored, discussed, or processed
- Asking you or anyone else to obtain critical assets to which the person does not have authorized access
- Seeking to obtain access to critical assets inconsistent with present duty requirements

Information Transmittal

Insiders must have a way to transmit the information they are compromising. Some reportable information transmittal indicators include:

- Removing critical assets from the work area without authorization
- Extensive use of copy, facsimile, or computer equipment to reproduce or transmit critical asset-related information that may exceed job requirements
- Discussing critical asset-related information in public or on an unsecure telephone
- Using an unauthorized fax or computer to transmit classified information



- Attempting to conceal any foreign travel while possessing a security clearance whether work-related or personal travel
- Improperly removing the classification markings from documents

General Suspicious Behaviors

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

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

Reporting

If you suspect a possible insider threat, you must report it. You cannot assume someone else will do so. Every one of us is an owner of security – both the security of information and the security of personnel.

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

Reporting Processes

Ultimately, reports must reach Radwan Rouzky, Facility Security Officer (FSO) but, as with other reporting processes, you have similar reporting channels available:

- Site supervisor or Program manager: TBA
- Corporate Facility Security Officer (FSO): Radwan Rouzky
- HR and legal: TBA
  Administrative & HR Assistant
  (T)919-234-1984 (F) 928-438-1742
- Ethics hotline for anonymous complaints: 1-877-576-4033

For cleared employees, reporting is not an option, it's a requirement. Failing to report could result in loss of security clearance and termination of employment. Individuals may also be subject to criminal charges.

Reporting

The insider threat is real, and the risks are high. Hopefully this training has provided you with the indicators needed to identify a potential threat, and the important role you play in identifying and reporting. You are the first line of defense!

If you suspect a potential insider threat or become a target of recruitment, you must report it.

SEAD-3-Awareness

Office of the Director of National Intelligence
National Counterintelligence and Security Center

SECURITY EXECUTIVE AGENT DIRECTIVE (SEAD) - 3

Reporting Requirements for Personnel With Access to Classified Information or Who Hold a Sensitive Position

Overview SEAD - 3

• Pursuant to Executive Order 13467, as amended, the Director of National Intelligence (DNI) serves as the Security Executive Agent (SecEA), responsible for developing, implementing, and overseeing uniform policies and procedures governing the conduct of investigations and adjudications for eligibility for access to classified information or to hold a sensitive position.

• On December 14, 2016, the DNI signed Security Executive Agent Directive (SEAD) 3, Reporting Requirements for Personnel With Access to Classified Information or Who Hold a Sensitive Position, effective 12 June 2017.

• This briefing describes the foundation of that landmark policy, how it applies to individuals working for the federal government, and applicable reporting requirements.

Foundation for SEAD 3 Development

• SEAD 3 establishes standardized reporting requirements across the federal government for all “covered individuals” (defined on Slide 5) who have access to classified information or hold a sensitive position.

• SEAD 3 was developed with subject matter experts across the federal government to promote consistency in personnel security reporting requirements for all covered individuals.

• The reporting requirements outlined in SEAD 3 address the need for covered individuals to report information to their department or agency (D/A) in a more timely manner.

• SEAD 3 was designed to strengthen the safeguarding of national security equities, such as national security information, personnel, facilities, and technologies.

Key Definitions

• Classified national security information or classified information: Information that has been determined pursuant to EO 13526 or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure.

• National Security Eligibility: Eligibility for access to classified information or to hold a sensitive position, to include access to sensitive compartmented information, restricted data, and controlled or special access program information.

• Unauthorized Disclosure: A communication, confirmation, acknowledgement, or physical transfer of classified information, including the facilitation of, or actual giving, passing, selling, publishing, or in any way making such information available to an unauthorized recipient.

Key Definitions (con’t)

• Covered individuals: Individuals (to include contractors, subcontractors, licensees, certificate holders, grantees, experts, and consultants) who:

- ❏ Perform work for or on behalf of the executive branch who have been granted access to classified information or who hold a sensitive position;
- ❏ Perform work for or on behalf of a state, local, tribal, or private sector entity, who have been granted access to classified information; or
- ❏ Serve in the legislative or judicial branches and have been granted access to classified information

• Sensitive Position: Any position within or in support of an agency in which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on national security regardless of whether the occupant has access to classified information and regardless of whether the occupant is an employee, military service member, or contractor. The designation levels of Noncritical-sensitive, Critical-sensitive, and Special-sensitive determine the degree to which any person in the position could cause a “material adverse effect on national security.”

Why is Reporting Important?

• Covered individuals incur a continuing security obligation to be aware of the risks associated with foreign intelligence operations and/or possible terrorist activities directed against them in the U.S. and abroad, and to be aware they possess or have access to information that is highly sought after by our foreign adversaries and competitors, including, but not limited to:

- ❏ Classified or sensitive information vital to national and economic security
- ❏ Emerging technologies and pioneering research and development
- ❏ Information relating to critical infrastructure sectors
- ❏ Proprietary secrets
- ❏ Security or counterintelligence information

• Covered individuals have a special and continuing obligation and responsibility for recognizing and avoiding personal behaviors and activities that may impact their continued eligibility for access to classified information or to hold a sensitive position.

Why is Reporting Important? (con't)

- Covered individuals shall report to their agency head or designee, any planned or actual involvement in any of the activities prior to participation in such activities or otherwise as soon as possible following the start of their involvement.
- SEAD 3 entrusts all covered individuals with the critical responsibility to report behavior or activities of those around them that could compromise classified information, workplace safety, and/or our national security. Important examples:
  - ❏ You may be targeted by foreign intelligence entities when traveling abroad. This could include direct elicitation (a pitch, either in-person or otherwise), human targeting (meeting someone who shares your interests at a professional conference), surveillance (either physical or electronic), or being subjected to questioning at an international airport or other point-of-entry.
  - ❏ Prompt reporting serves as a mechanism to get the necessary attention and support before the situation escalates.
  - ❏ By providing your organization with information about when you are traveling, where you are venturing to, and who you are meeting with, your organization can inform you of any applicable threats beforehand, and provide needed assistance should unexpected developments occur during your travel.
  - ❏ In the aftermath of several espionage cases, co-workers commented that they noticed unusual behavior, but did not know how to report concerns, or to whom.
  - ❏ REMINDER : Foreign intelligence services often operate in countries other than their own, including those that are friendly to the U.S. You do not have to travel to an adversarial country to be targeted by a foreign intelligence service!

Reportable Activities – Foreign Travel

• Foreign Travel – D/A Heads or designees shall determine requirements for reporting foreign travel as part of the covered individual's duties.

• Unofficial Foreign Travel (unrelated to official government business)

- ❏ Individuals must submit an itinerary
- ❏ Unanticipated border crossings are discouraged. and receive advance approval prior to travel .
- ❏ Individuals are required to report all deviations from their approved itinerary within five business days of return.
- ❏ Travelers shall receive a defensive security awareness or counterintelligence briefing prior to any travel (official or unofficial). Exceptions to the requirement to submit an itinerary and receive prior approval: Travel to Puerto Rico, Guam or other U.S. possessions and territories is not considered foreign travel and need not be reported. Unplanned day trips to Canada or Mexico shall be reported within five business days of return.
- ❏ *D/A heads may have more stringent requirements, including prohibitions, may insert D/A-specific travel guidelines here, as applicable, and provide specific examples of reported situations.*

Reportable Activities – Foreign Contacts

• Foreign Contacts – D/A Heads or designees shall determine requirements for reporting contact with a foreign national as part of the covered individual's duties.

• Unofficial Contacts

- ❑ With a known or suspected foreign intelligence entity.
- ❑ Continuing association with known foreign nationals that involve bonds of affection, personal obligation, or intimate contact; or any contact that involves the exchange of personal information. This requirement applies regardless of where or how the contact was made (personal contact, Internet, etc.).
- ❑ Following initial reporting of the contacts, updates regarding continuing unofficial association shall occur only for significant changes in the nature of the contact.
- ❑ Individuals are still responsible for reporting suspicious interactions, activity or unexpected events when traveling or meeting foreign nationals for official business.
- ❑ Foreign intelligence services often operate in countries other than their own, including those that are friendly to the U.S. You do not have to travel to an adversarial country to be targeted by foreign intelligence services.
- ❑ *D/A Heads may have more stringent requirements, including prohibitions, and may insert D/A-specific guidance on foreign contacts here, as applicable, and provide specific examples of reported situations.*

Reportable Activities - Actions by Others

• To ensure protection of classified information or other information specifically prohibited by law from disclosure, individuals shall alert agency officials should they become aware of the following activities that may be of potential security, insider threat, or counterintelligence concern of other covered individuals:

- ❏ An unwillingness to comply with rules, regulations, or security requirements
- ❏ Unexplained affluence or excessive indebtedness
- ❏ Alcohol abuse
- ❏ Illegal use or misuse of drugs or drug activity
- ❏ Apparent or suspected mental health issues where there is reason to believe it may impact the individual's ability to protect classified information or other information prohibited by law from disclosure
- ❏ Criminal conduct
- ❏ Any activity that raises doubts as to whether the individual's continued national security eligibility is clearly consistent with national security interests
- ❏ Misuse of U.S. Government property or information systems

Additional Reportable Activities – Access Levels

• Covered individuals who have been identified by their respective D/A head in accordance with EO 12968, as amended, Section 1.3.(a), shall file a financial disclosure report, as appropriate.

• In addition to the aforementioned reporting requirements, individuals with different levels of access to national security information or position sensitivity levels are to report additional activities:

- ❑ Secret or Confidential information, “L” access, or holding a Noncritical-sensitive position
- ❑ Top Secret information, “Q” access, or holding a Critical-sensitive or Special-sensitive position

Individuals With Access to Secret or Confidential Information, “L” access, or holding a Noncritical-sensitive Position

Foreign Activities

- ❏ Application for and receipt of foreign citizenship
- ❏ Application for, possession, or use of a foreign passport or identity card for travel

Other Activities

- ❏ Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified or other “protected” information
- ❏ Media contacts, other than for official purposes, where the media seeks access to classified or otherwise “protected” information, whether or not the contact results in an unauthorized disclosure
- ❏ Arrests
- ❏ Bankruptcy or over 120 days delinquent on any debt
- ❏ Alcohol or drug-related treatment

Individuals with Access to Top Secret Information, “Q” access, or holding a Critical-sensitive or Special-sensitive Position

Foreign Activities

- ❏ Direct involvement in foreign business
- ❏ Foreign bank accounts
- ❏ Ownership of foreign property
- ❏ Foreign citizenship
- ❏ Application for and receipt of foreign citizenship
- ❏ Application for, possession, or use of a foreign passport or identity card for travel
- ❏ Voting in a foreign election
- ❏ Adoption of non-U.S. citizen children

Individuals with Access to Top Secret Information, “Q” access, or Holding a Critical-Sensitive or Special-Sensitive Position (con’t)

Other Activities

- ❏ Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified or other information specifically prohibited by law from disclosure regardless of means
- ❏ Media contacts where the media seeks access to classified or other information specifically prohibited by law from disclosure, whether or not the contact results in an unauthorized disclosure
- ❏ Arrests
- ❏ Financial anomalies
- ❏ Foreign national roommate(s)
- ❏ Cohabitant(s)
- ❏ Marriage Alcohol or drug-related treatment

Summary

• SEAD 3 establishes reporting requirements for all covered individuals who have access to classified information or who hold a sensitive position.

• Covered individuals have a special and continuing security obligation and responsibility for recognizing, avoiding, and reporting personal behaviors of a potential security, counterintelligence, and/or insider threat concern.

• Individuals must alert their D/A should they become personally involved with or aware of certain activities of other covered individuals that may be of potential security, counterintelligence, and/or insider threat concern.

• SEAD 3 was designed to strengthen the safeguarding of national security equities

KLTD Security Solutions, Inc.
Security Training/Insider Threat Training Acknowledgement Receipt

I certify that I have attended/reviewed a required Security Briefing provided by KLTD Security Solutions, Facility Security Officer in accordance with:

NISPOM Chapter 3-107 Initial - Prior to being granted access to classified information, an employee shall receive an initial security briefing.

NISPOM Chapter 3-108 Refresher Briefing - Refresher training shall reinforce the information provided during the initial security briefing and will keep cleared employees informed of appropriate changes in security regulations.

NISPOM 3-103b Insider Threat Training - Training on insider threat awareness is required for all cleared employees before being granted access to classified information and annually thereafter.

NISPOM – (ISL) Industrial Security Letter 2021-02, which covers SEAD 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position", DCSA's Counterintelligence Division has updated the Foreign Travel brief.

I understand the trust that has been afforded to me by the United States Government by granting me access to classified information, documents, and equipment. I also understand the importance of protecting this information and how unauthorized disclosure could harm National Security.

Employee

Print name: _____

Signature: _____ Date: _____