AKIMA

# Annual Security & Insider Threat Awareness

FY 2025

# Why do I need to do this training?

**Executive Order 12829, the National Industrial Security Program (NISP)** establishes rules and regulations, to properly protect and control all classified material in our possession or under our immediate control.

Our company has been granted a Facility Clearance (FCL) and is eligible for accessing classified information based on the award of a classified contract(s). As a cleared company, we have entered into a **DoD Security Agreement (DD441)** which outlines our security responsibilities.

As a cleared employee or consultant, **you** are equally bound under the law to provide the same protection as outlined in the **Non-Disclosure SF312** which you signed prior to gaining access to classified information.

In accordance with the **32 CFR Part 117 :: National Industrial Security Program Operating Manual (NISPOM)** you must complete an Annual Security and Insider Threat Briefing. Your completion record is your acknowledgement that you have received this training and that you understand that you have a personal obligation to safeguard national security information. Your completion record will be made available to be included in your security file. If you have questions, you can seek additional guidance from your supervisor and Facility Security Officer (FSO).

ANNUAL SECURITY & INSIDER THREAT AWARENESS

# I am not cleared; do I need to complete this?

**Yes. Our goal is to protect Akima's informational assets[1] against all internal, external, deliberate, or accidental threats.**

This policy provides the framework for setting information security objectives. The policy ensures that:

- Information will be **protected** against unauthorized access
- **Confidentiality** of information will be assured
- **Integrity** of information will be maintained
- **Availability** of information for business processes will be maintained
- **Legislative and regulatory** requirements will be met
- **Business continuity** plans will be developed, maintained, and tested[2]
- Information security **training** will be completed by all employees (cleared and uncleared), and
- All actual or suspected information security breaches will be reported to the Information Security Manager and will be properly and timely investigated.

1 *Information can exist in various forms, and incudes data stored on computers, transmitted over networks, printed, or written on paper, stored on electronic media, or discussed during in-person or telephone conversations.*

2 *This plan allows users to access information and essential services when needed*

# How do I qualify to be cleared?

The DCSA Consolidated Adjudication Services (CAS) granted a security clearance eligibility based upon the personal information you provided on your application (eAPP) and the completed vetting of your background investigation. **And** you work on a contract that requires your position be cleared establishing that you have a "Need to Know" .

The table below shows what else is considered to determine the need to obtain/maintain a clearance:

| Position | Legal Status | Access Levels Allowed |
|---|---|---|
| Requires access to classified information | U.S. Citizen | Secret, Top Secret, SCI |
| Requires access to Controlled Unclassified Information (CUI) | U.S. Citizen<br>Lawful Permanent Resident<br>Resident Aliens | CUI – no government IT systems or technical data access |
| Requires access to CUI/Government IT Systems/ITAR Technical Data | U.S. Citizen | CUI/Government IT Systems/ITAR Technical Data |
| General Positions – no access to classified information | Anyone authorized to work in the U.S. | Low sensitivity information |

# How is eligibility determined?

**The SF86 form** is completed via eApp and reviewed to determine suitability for granting eligibility for a Tier 5 (T5) – Top Secret, SCI or Tier 3 (T3) for a Secret or Confidential eligibility. This form is also used to maintain eligibility; a Tier 5 Review (T5R) – Top Secret, SCI or Tier 3 Review (T3R) – Secret or Confidential. The SF86 is initiated and submitted by your security team.

**The SF85 form** is completed via eApp and reviewed to determine suitability for a Public Trust. There are multiple levels of Public Trust which are Tier 1 (NACI) with favorable results or Tier 2 or 4 (MBI/BI) with favorable results with a credit check. The SF85 is typically initiated and submitted by government agencies.

Once the form is submitted, the following adjudication guidelines are used to determine eligibility:

- Allegiance to the U.S.
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Psychological Conditions
- Criminal Conduct
- Handling Protected Information
- Outside Activities
- Drug Involvement – Note: Possessing and using marijuana is legal in some states but is still a federal crime and will impact your clearance
- Misuse of Information Technology Systems

# What is Continuous Vetting/Evaluation?

Continuous Vetting/Evaluation (CV/CE) is the **clearance review process that was formerly called *periodic reviews***.

- Updated investigations are now done at 5-year intervals for all types of clearances requiring a new SF86.
- Once enrolled in the CV/CE program, a set of automated record checks and business rules are used to assist with the ongoing assessment of an individual's continued eligibility.
- Akima's Security team may ask you to complete an out-of-cycle SF86 to comply with an official request based on any anomaly found during this ongoing assessment. You may also need to complete a new SF86 if information is self-reported and/or found during the checks outlined above.

Existing eligibility will remain valid until you have been removed from CV/CE, no longer have DoD affiliation, or if your eligibility has been revoked or suspended. This means your current clearance will remain valid and you will receive notification from the Security team if further action is needed.

ANNUAL SECURITY & INSIDER THREAT AWARENESS

# SF312 – Non-Disclosure

Once you receive notice of eligibility, you are required to sign an SF312 – Non-Disclosure which is an agreement between you and the U.S. government.

This lifelong agreement places a special trust in you. You are responsible to protect classified information from unauthorized disclosure. There are serious consequences should there be a breach to this agreement which can result in the loss of your security clearance, fines, or even jail time.

Prior to completing your SF312 you may be subject to criminal, civil, or administrative consequences because of the unauthorized or unintended disclosure of classified information.

Even after you no longer have a requirement for a security clearance the obligation to protect classified information is still in place.


CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

ANNUAL SECURITY & INSIDER THREAT AWARENESS

# Which of the following is required to access classified information?

A. Fully executed SF312 – Non-Disclosure Form

B. Clearance eligibility at the appropriate level based on contract requirements for your position

C. Your position has been identified as requiring a Need to Know

D. I had a clearance before

E. A, B, and C are required to be granted access to classified information

# Which of the following is required to access classified information?

**The answer is E:** A, B, and C are required to be granted access to classified information

ANNUAL SECURITY & INSIDER THREAT AWARENESS

# Other Briefing Requirements

Every cleared contract is issued a DD254 which may identify specific requirements where additional briefings must be completed. For example, you may be required to have NATO, COMSEC, SAP, SCI or other contract-specific trainings/briefings. These safeguarding guidelines and restrictions could also be based on your specific job/ location.

All employees **must** comply with the client security requirements which can include access to the client IT systems. A violation of a client's security policies and procedures may be grounds for removal from the contract.

You must adhere to the terms of the Standard Practice Procedures (SPP). Contact your Security Team for a copy of the SPP or you can access it via the Security page in the Akima Employee Portal.

You must be knowledgeable of reporting requirements, security violations/infractions related to protection of classified information and facilities and the consequences of non-compliance. Contact your supervisor or security team with any questions you may have.

conte

# Information Categories Defined

Classified Information is any information where unauthorized disclosure could adversely affect the national security of the United States. It is information that us usually owned by, produced by, or for/or under the control of the U.S. government and meets the criteria of Executive Order 12356.

**The categories of classified information are:**

- **Top Secret** – Unauthorized disclosure will cause exceptionally grave damage to the U.S. national security.
- **Secret** – Unauthorized disclosure will cause serious damage to U.S. national security.
- **Confidential** – Unauthorized disclosure will cause damage to U.S. national security.

**Unclassified information categories requiring protection:**

- **Controlled Unclassified Information (CUI)** – Unclassified information that is created or owned by the government which requires safeguarding and dissemination controls. Data security controls as outlined in the National Institute of Standards and Security (NIST) apply to CUI. Any compromise of CUI must be reported within 72 hours of discovery.
- **Sensitive But Unclassified (SBU)** – Unclassified information that cannot be disclosed to the general public including critical infrastructure or technical information.
- **Company Private or Proprietary Information** – Business information not to be divulged to individuals outside the company.

ANNUAL SECURITY & INSIDER THREAT AWARENESS

# Akima Controlled Unclassified (CUI) Handling Procedures

Certain CUI specific designations require additional protection measures and can only be processed or stored on specified Akima systems.

- Our Office 365 services (SharePoint Online/OneDrive/Teams) cannot be used to store or transmit **CUI** data.
- Data should be transferred to/from government entities using either DoD email, DoD safe, or other government-provided portal(s).
- If no government-provided solution exists, users with CAC or an approved Medium Assurance certificate can transmit CUI via encrypted emails. The IT Help Desk can assist you if you are not familiar with how to do this. The Office Message Encryption (OME) feature within Outlook is not suitable for CUI data.
- For temporary offline storage, create a folder labeled "CUI" in your Downloads folder to contain working data and to transfer subject data between laptop and approved systems. This will ensure the data does not leave your machine.
- If your project receives or creates any of these data marking types and needs a secure portal, please contact helpdesk@akima.com to setup a site on our compliant system: projects.akima.com.
- If you have any questions regarding the proper handling of CUI, contact your PM or reach out to Akima IT at helpdesk@akima.com. Reference the CUI Procedures Handout here: CUI Procedures Handout.pdf (akima.com)

ANNUAL SECURITY & INSIDER THREAT AWARENESS

# Safeguarding Classified Information Basics

- Never leave classified information unattended
- Never discuss classified information in public places
- Only discuss on secure telephones
- Must be under the control of an authorized person
- Must be properly marked with classification
- Must be stored in an approved GSA storage container
- Never processed on your computer unless approved by the Designated Approval Authority

You must **never reveal or discuss classified information**. It is your **personal responsibility** to **confirm** that the person you are interacting with is both properly cleared and has a need to know. If in doubt, ask your Security Team.

# Which of the following are ways Classified Information can be Safeguarded?

A. Vaults

B. Secure rooms

C. Secure telephones

D. A locked desk drawer

E. Secure GSA approved safes

# Which of the following are ways Classified Information can be Safeguarded?

**The answer is:** A, B, C, and E are acceptable ways to safeguard classified information.

ANNUAL SECURITY & INSIDER THREAT AWARENESS

# Public Release of Information

Any information (classified or unclassified) pertaining to your contract cannot be released for public dissemination except as provided by the **32 CFR Part 117 :: National Industrial Security Program Operating Manual (NISPOM)** unless it has been approved for public release by a U.S. government authority. Proposed public releases shall be submitted for review **and** approval prior to release to the appropriate government approval authority for your contract.

Furthermore, **any** information pertaining to Akima and its subsidiaries will need to be reviewed **and** approved by Marketing & Communications prior to release.

ANNUAL SECURITY & INSIDER THREAT AWARENESS

# An Insider Threat Can Be Anyone

An Insider Threat is any person with authorized access to any U.S. government resources, including personnel, facilities, information, equipment, networks, or systems, who uses that access either wittingly or unwittingly to do harm to the organization or national security. A person presenting an Insider Threat looks no different than you and me. Any person within an organization can be targeted regardless of level of access to information. An Insider posing a threat can be motivated by money, ego, support of a cause for another country and in some cases, just because he/she can.

# How Does an Insider Threat Happen?

- A foreign entity may use exploitable weaknesses to convince an individual with access to provide information to those who do not have the appropriate clearance and a “need-to-know.”
- An individual may choose to sell out their country or organization because of motivators such as greed, disgruntlement, divided loyalties, or ideological reasons.
- An individual may unwittingly give away information through poor security procedures or clever elicitation collection techniques.

# Insider Threat Case: Foreign Espionage

**Victor Manuel Rocha**

- Age 73 at time of sentencing
- Resided in Florida
- Born in Colombia
- Naturalized as a U.S. citizen at age 28

- Rocha served with the U.S. Department of State (DOS) for over 20 years and held high level positions.
- Rocha began secretly working with the Cuban General Directorate of Intelligence (DGI) in 1981 while employed with DOS and continued until he was arrested in 2023.
- On April 12, 2024, Rocha pleaded guilty to conspiring to act as an agent of a foreign government.

[Click here to read the full case study]

**INDICATORS**

- Foreign Influence and Preference
- Allegiance to the United States
- Access Attributes

# Insider Threat Case: Fraud


- Murali Y. Venkata, a former Acting Branch Chief of the Information Technology Division of the United States Homeland Security, conspired to steal proprietary U.S. software and databases.
- Venkata and his co-conspirators disclosed stolen software and databases to software developers in India.
- On April 11, 2022, Venkata was convicted of conspiracy to defraud the U.S. Government.

**INDICATORS**

- Access Attributes
- Technical Activity (Security Violations)
- Criminal Conduct


Click here to read the full case study.

# Online Recruitment

Social networks are often used to recruit individuals because it is easy to impersonate anyone, someone you worked with, a friend, a friend of a friend, or even a family member.

**LinkedIn** is a treasure trove for adversaries who may connect with you or through your connections to get information used to get a foothold within an organization.

**Facebook** is accessed by adversaries who can get personal information to gain access to you, your family, and your livelihood.  Assume that **anyone** can see any information that you post and share.

**Twitter** is only 280 characters, but a lot of information can be gained by individuals who "follow" you. Billions of search queries are done daily.

**Instagram** allows users to upload photos and short videos, follow other users' feeds and geotag images. Hashtags are used to help other users discover similar content. It's easy for billions of adversaries to follow your posts.

**Threads** is 500 characters and is a mix between Instagram and Twitter. It links identity data that adversaries can use to try to connect with you and your followers.

Be mindful of what you post – adversaries check social media regularly. Make sure you review your security/privacy settings and your connections. Anytime you receive an update to your social accounts, check your settings since they may be affected. Only establish and maintain connections with people you know and trust. Remove anyone that is no longer relevant and report suspicious connections.

# Bad Actors

## Who Are They?

- Foreign or multinational corporations
- Foreign government-sponsored educational and scientific institutions
- Freelance agents – some are former intelligence officers
- Computer hackers
- Terrorist organizations
- Revolutionary groups
- Extremist ethnic or religious organizations
- Drug syndicates
- Organized crime

## What Are Common Methods Used?

- Blackmail and Coercion
- Cultivating a relationship through social media
- Cyber intrusions, viruses/malware, backdoor attacks, phishing emails
- Front companies used to acquire technology
- Price quotes and market surveys to request information
- Sales, rep, or agency offers, RFI/RFP responses for tech or business services
- Resume submissions, applications, or references

**If you encounter any of these situations that seem suspicious, contact your security team.**

# Best Practices for Insider Threat Prevention

What are some of the best practices for Insider Threat Prevention?

A. Performing an enterprise-wide risk assessment
B. Enforcing policies and controls
C. Establishing physical security in the work environment
D. Using software solutions to secure access
E. Implementing proper access controls
F. Regularly monitoring activities to detect unauthorized actions
G. All the above

# Best Practices for Insider Threat Prevention

**The answer is G:** All of the above are best practice prevention methods for Insider Threats.

# What to Look for and Report

**Information to be reported needs to be based on facts not rumors:**

- Requests for critical asset information – classified information, proprietary information, intellectual property, trade secrets, personnel security, facilities, and personnel – outside of official channels. Requests to access information that he/she does not have a need to know.
- Unreported or frequent foreign travel.
- Suspicious foreign contacts – contact with an individual who is known to be, or is suspected of being, associated with foreign intelligence, security, or terrorism.
- Known or suspected espionage or sabotage, suspicious contacts.
- Unreported offer of financial assistance, gifts, or favors by a foreign national or stranger. Unexplained affluence or financial difficulties.
- Suspected recruitment by foreign or domestic competitive companies to convince an employee to work for another company. Any employment or service (paid or unpaid) with any business enterprise organized under the laws of another country.
- Substance abuse (alcohol or drugs), arrests or criminal conduct, treatment for emotional or mental disorders, out-of-character behavior.

# What to Look for and Report (continued)

**Information to be reported needs to be based on facts not rumors:**

- Working odd hours for no apparent reason.
- Divided loyalty or allegiance to the United States.
- Conflicts with supervisors, decline in work performance, excessive tardiness, and unexplained absence are usually associated with disgruntled employees and may be an indicator of susceptibility to becoming an insider threat.

If you suspect a possible Insider Threat, you must report it. You can reach out to your supervisor, Human Resources, and Akima's EthicsPoint helpline at akima.ethicspoint.com or 844-675-7686. Any IT related items can be reported through the IT Help Desk at hd@akima.com or 866-933-4643. Ultimately you must report such circumstances to your Facility Security Officer (FSO). Failing to report could result in loss of your security clearance and termination of employment. Individuals may also be subject to criminal charges.

For a complete listing of reporting requirements go to ISL2021-02_SEAD-3.pdf (dcsa.mil)

# Behaviors can manifest as indicators for an Insider Threat. Which of the below are considered Insider Threat activity?

A. Espionage
B. Terrorism
C. Unauthorized disclosure of information
D. Corruption, including participation in transnational organized crime
E. Sabotage
F. Workplace violence
G. All the above

# Behaviors can manifest as indicators for an Insider Threat. Which of the below are considered Insider Threat activity?

**The Answer is G:** All of the above

ANNUAL SECURITY & INSIDER THREAT AWARENESS

# Other Reporting Requirements

- Changes to name, marital status, cohabitation of an intimate nature, and citizenship status.
- Loss or suspected loss, compromise or suspected compromise, of classified or proprietary information. This includes evidence of tampering with a container used for storage of classified information.  If you find an unlocked security container which is unguarded or left unlocked after-hours.
- Lost or stolen badges.
- Willful disregard for security procedures.
- Attempts to enlist others in illegal or questionable activity.
- Inquiries about operations/projects where no legitimate need to know exists.
- Unauthorized removal of classified information.
- Fraud, waste, or abuse of government credit cards.
- Criminal activities, arrests, restraining orders, alcohol or drug related incidents, or financial difficulties including garnishments.

# Which is the correct answer regarding information you should self-report to the Security Team?

A. When I defraud or abuse company/government credit cards

B. My willful disregard of security procedures

C. Change in name, marital status, cohabitation of an intimate nature, and citizen status

D. Adoption of non-U.S. children

E. My attempts to enlist others in illegal or questionable activities

# Which is the correct answer regarding information you should self-report to the Security Team?

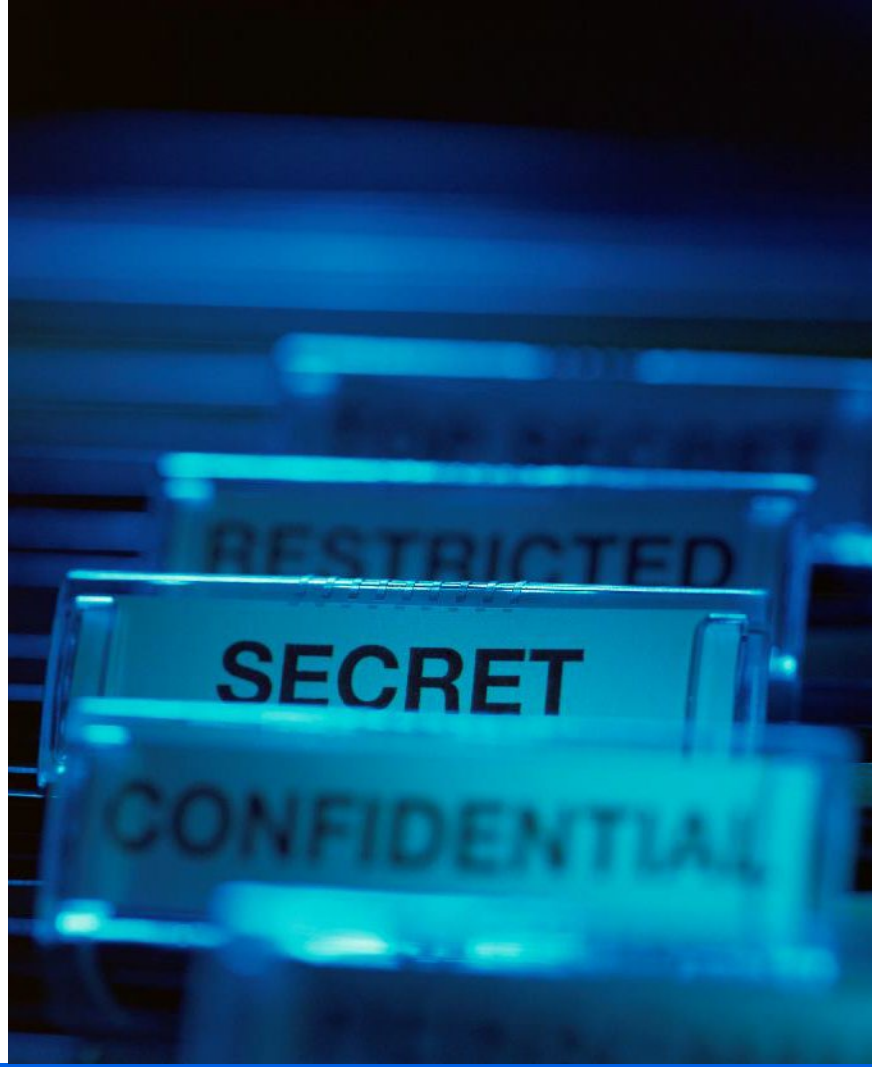
**The Answer is C & D**: Change in name, marital status, cohabitation of an intimate nature, and citizen status. As well as adoption of non-U.S. children.

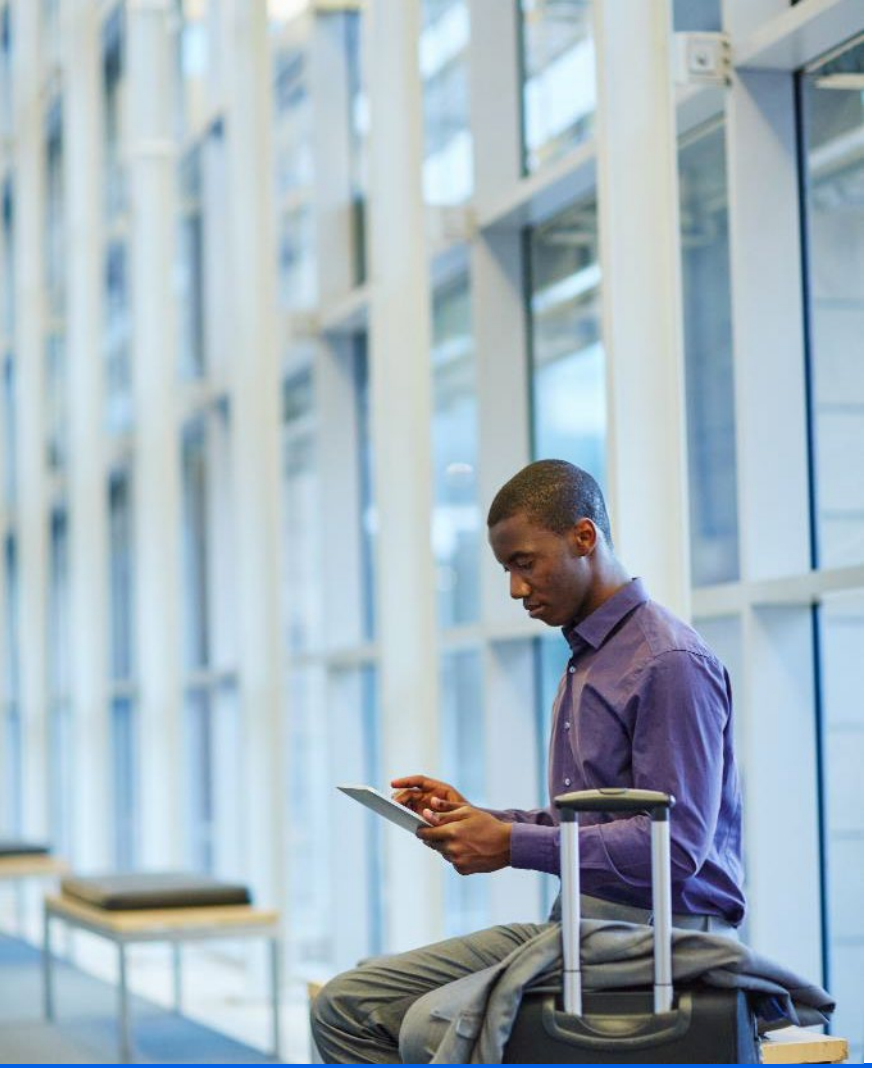
ANNUAL SECURITY & INSIDER THREAT AWARENESS

# Operations Security: OPSEC

OPSEC is used to mitigate vulnerabilities and to protect sensitive, critical, or classified information. The process includes identifying critical information, analyzing the threat, know the vulnerabilities, accessing the risk, and implementing countermeasures.

- Identify what needs to be protected – information the adversaries might want
- Analyze how the loss of this information will affect your program
- What are the vulnerabilities in protecting this information
- Assess the risk and apply the appropriate countermeasures





ANNUAL SECURITY & INSIDER THREAT AWARENESS

# Foreign Travel

- You must report all work or personal foreign travel even if is only for a day and you will receive a required briefing. If you hold a TS/SCI you may have additional reporting requirements – check with your government client or FSO. It is your responsibility to report this **before** you leave.
- Detailed reporting forms prior to and upon your return need to be completed which are reviewed by your FSO. You may receive a request for additional information to clarify what you have submitted.
- It is best practice to develop a personal travel plan to give to your office and family.
- Learning about the cultures, customs, and laws of the country you visit will help you when traveling.
- Visit https://travel.state.gov to find country specific information, like: What countries are on the national threat list or have high crime, shots that may be required, visa/passport requirements, tips for safe travels, etc.

ANNUAL SECURITY & INSIDER THREAT AWARENESS

# Foreign Contacts

Generally, you should report any relationship with a foreign national that involves bonds of friendship, affection or personal obligation.  Contact with a representative or an element of a foreign government that is not part of your official duties should also be reported.

Foreign contacts are not just limited to those met outside of the continental US.  A foreign contact that lives in the US versus one that lives overseas could potentially pose the same threat.

Casual, passing relationships of those that you might see occasionally, such as a clerk at local vendor that you frequent, is not reportable.  However, depending on the information you share, a friend on social media may be reportable.

Contact the Security Team for the questions and form to report this interaction.

# Any travel that requires the use of a passport must be reported.

True

or

False

# Any travel that requires the use of a passport must be reported.

**The Answer is**: True

# Disciplinary Graduated Scale Actions for Security Violations

**Progressive disciplinary actions may include, but are not limited to**

→ **First Instance:** Verbal counseling

→ **Second Instance:** Written warning and performance improvement plan

→ **Third Instance:** Final written warning

**Or Major Violations**

Same as above and may include suspension and/or termination of employment

→ **Loss of security clearance**

→ **Arrest**

→ **Imprisonment and/or fines**

**Based on the violation, disciplinary action may not include all steps listed and may necessitate immediate dismissal. For additional information, refer to the Akima Policies and Procedures Manual, #211 – Performance Improvement / Conduct and #212 Termination of Employment.**

# Reporting Tools

**Security Team:** You can reach out to us individually or use our general email: Security@akima.com

**Akima Company Intranet –** Go to the Akima intranet Security page for more information about security reporting and requirements: Home (akima.com)

**DoD Hotline:** DOD maintains a hotline to provide an open avenue for employees to report, without fear of reprisal, known or suspected instances of serious security irregularities concerning government contracts, programs, or projects. The Defense Hotline numbers are (800) 424-9098 or (703) 693-5080.

AKIMA

# Your Security Team

Melissa Graham, Director of Security: 719-355-2298 | Melissa.Graham@akima.com

Seth Bayer, Security Specialist: 256-489-1445 | Seth.Bayer@akima.com
Alice Gallegos. Security Specialist: 719-355-2389 | Alice.Gallegos@akima.com
Kendall Miller, Sr. Facility Security Officer: 703-766-6776 | Kendall.Miller@akima.com
Steve Mumphrey, Sr. Facility Security Officer: 571-482-5326 | Steve.Mumphrey@akima.com
Lisa Myatt, Facility Security Officer: 938-225-0989 | Lisa.Myatt@akima.com
Adam Santee, Security Specialist: 571-323-6169 | Adam.Santee@akima.com

Security@akima.com

AKIMA

Thank you for completing your training.

Click here to enter your completion record: Submit

Direct any questions to your

Security Team contact.