Annual Security & Insider Threat Awareness

2022

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 available for inclusion in your security file. If you have questions, you can seek additional guidance from your supervisor and facility security officer (FSO).

How did I qualify to be cleared?

The Department of Defense Central Adjudication Facility (DoD CAF) grants a security clearance eligibility based on:

- Personal information you provide on your application (e-Qip)
- Complete vetting of your background investigation
- Your contract requires that your position be cleared and 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 Lawful Permanent Resident 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

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

What are the requirements for you to obtain/maintain a security clearance?

A. Eligibility determination is based on a completed e-Qip investigation and a U.S. citizenship.

B. Eligibility determination is based on a completed e-Qip investigation **AND** a “Need-to-Know” has been established based on contract requirements and the position the individual holds.

C. Eligibility determination is based on a person’s legal status.

D. Anyone authorized to work in the U.S. meets the eligibility requirements.

E. I held a clearance in my last job.

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

What are the requirements for you to obtain/maintain a security clearance?

The Answer is B: Eligibility determination is based on a completed e-Qip investigation **AND** a "Need-to-Know" has been established based on contract requirements and the position the individual holds.

Even if you held a clearance in a previous position, it may only be maintained if the all of the above applies to your employment.

How is eligibility determined?

The SF86 form is completed via e-Qip 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 e-Qip 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 Evaluation?

Continuous Evaluation (CE): A new risk management approach and includes measures implemented by DCSA which are intended to mitigate the existing backlog of reviewing periodic review investigations. Favorable screening results from a review of an SF86 will place individuals in CE.

Once enrolled, a set of automated records, checks, and business rules are used to assist with the ongoing assessment of an individual's continued eligibility.

CE supplements, but does not replace, the established personnel security program for scheduled periodic reinvestigations of individuals for continuing eligibility. It is intended to have all cleared personnel be enrolled into the CE program and you may be notified to complete an out of cycle SF86 from our team to comply with this official request.

You may also need to complete a new SF86 if information is self-reported and/or found during the checks outlined above.

Existing eligibility remains valid until:

- You have been removed from CE
- You no longer have DoD affiliation, or
- Your eligibility has been revoked or suspended

Your current clearance will remain valid and you will receive notifications from the Security Team if further action is needed.

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

Allegiance to the United States, foreign influence, financial considerations, and criminal conduct are all part of which guidelines?

A. These are a part of the SF86 form, which is completed via the e-Qip.

B. These are a part of the Briefing Requirements that all cleared employees are required to receive prior to accessing classified information.

C. These are part of the adjudication guidelines used to determine clearance eligibility.

D. These guidelines, and others, are used during the periodic review that is used to maintain clearance eligibility.

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

Allegiance to the United States, foreign influence, financial considerations, and criminal conduct are all part of which guidelines?

The Answer is C: These are part of the adjudication guidelines used to determine clearance eligibility.

ANNUAL SECURITY & INSIDER THREAT AWARENESS

SF312 – Non-Disclosure

Once you receive 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. Even after you no longer have a requirement for a security clearance this expectation is in place.


CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

What form are you required to sign that is a lifelong agreement placing a special trust in you and requires you to protect classified information from unauthorized disclosure?

A. The SF312-which is the Classified Information Non-disclosure Agreement.

B. The SF86-which is completed via the e-Qip and then reviewed to determine suitability for granting eligibility.

C. The SF85-which is completed via the e-Qip and is reviewed to determine suitability for a Public Trust.

D. The e-Qip-which is the application form used to apply for security clearances.

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

What form are you required to sign that is a lifelong agreement placing a special trust in you and requires you to protect classified information from unauthorized disclosure?

The Answer is A: The SF312-which is the Classified Information Non-disclosure Agreement.

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 and 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, classified security violations/infractions, and the consequences of non-compliance.

Contact your supervisor or Security team with any questions you may have.

Information Categories Defined

Classified Information is any information where unauthorized disclosure could adversely affect the national security of the U.S. 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:

- **Sensitive But Unclassified (SBU); For Official Use Only (FOUO) and Controlled Unclassified Information (CUI) -** Cannot be disclosed to the general public. Dissemination requires appropriate markings and safeguarding. SBU includes Critical Infrastructure Information and CUI includes technical information. 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.
- **Company Private or Proprietary Information** – Business information not to be divulged to individuals outside the company.

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

Match the following information categories to the correct definition:

A. Top Secret

B. Secret

C. Confidential

D. SBU/CUI

E. FOUO

F. Company Private or Proprietary

I. Unclassified government information which cannot be disclosed to the general public and must not be circulated.

II. Unauthorized disclosure will cause exceptionally grave damage to the U.S. national security.

III. Unauthorized disclosure will cause serious damage to U.S. national security.

IV. Business information not to be divulged to individuals outside the company.

V. Unauthorized disclosure will cause damage to U.S. national security.

VI. Unclassified information that cannot be disclosed to the general public including critical infrastructure or technical information

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

Match the following information categories to the correct definition:

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

B. **Secret -** Unauthorized disclosure will cause serious damage to U.S. national security.

C. **Confidential -** Unauthorized disclosure will cause damage to U.S. national security.

D. **SBU/CUI -** Unclassified information that cannot be disclosed to the general public including critical infrastructure or technical information

E. **FOUO -** Unclassified government information which cannot be disclosed to the general public and must not be circulated.

F. **Company Private or Proprietary -** Business information not to be divulged to individuals outside the company.

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 know that the person you are interacting with is both properly cleared and has a need to know. If in doubt, ask your Security Team.

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

Read the scenario below and answer the question.

Jeff has been assigned work on a contract involving classified information. He has a stack of files containing classified information on his desk awaiting his review. Jeff receives a call from his supervisor John, asking him to join a meeting immediately in a shared conference room. Jeff quickly locks his computer and turns the files upside down on his desk; however, he leaves his CAC in his computer and the files unattended.

Has Jeff properly safeguarded the classified information?

Yes or **No**

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

Read the scenario below and answer the question.

Jeff has been assigned work on a contract involving classified information. He has a stack of files containing classified information on his desk awaiting his review. Jeff receives a call from his supervisor John, asking him to join a meeting immediately in a shared conference room. Jeff quickly locks his computer and turns the files upside down on his desk; however, he leaves his CAC in his computer and the files unattended.

Has Jeff properly safeguarded the classified information?

The Answer is: No

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 Joseph Pendry, VP Marketing & Communications (joseph.pendry@akima.com), 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 resource, 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.

An Insider Threat looks no different than you or me. Any person within an organization can be targeted regardless of level of access to information.

An Insider Threat can be motivated by money, ego, support of a cause for another country, and in some cases, just because they 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 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: Espionage & Conspiracy

Mark Steven Domingo expressed his desire to seek violent retribution for attacks against Muslims in internet posts and forums. Following multiple attacks covered in the news, Domingo decided to bomb a white supremacist rally in Long Beach, CA.

Domingo purchased several hundred 3½-inch nails to be used as shrapnel for the bombs. In April 2019, Domingo scouted the location he planned to attack. On April 26, 2019, Domingo received what he thought were two live bombs, but were actually inert explosive devices delivered by an undercover law enforcement officer.

He was arrested that same day with one of the bombs in his hands.

At trial, Domingo testified that he was the one who chose to attack the rally, chose to use the bombs, and chose to go through with the plot to commit mass murder.

Domingo was convicted of providing material support to terrorists and attempted use of a weapon of mass destruction and sentenced to 25 years in prison.

INDICATORS

- Criminal, Violent, or Abusive Conduct – Threatening Violence
- Violent Extremist Mobilization

Click here to read the full case study

Insider Threat Case: Unauthorized Disclosure

Reality Winner was a contractor at the NSA facility in Georgia and held a Top Secret/Sensitive Compartmented Information security clearance.

Winner had a deep distrust of the administration, expressed support for the Taliban, and proclaimed that she wanted to burn down the White House.

She installed software on her computer that enabled her to surf the internet, chat, and send instant messages anonymously. She researched whether it was possible to insert a thumb drive into a Top Secret computer without it being detected, then inserted an unauthorized thumb drive into a Top Secret computer.

In May 2017, Winner used the unauthorized software to find and print a classified intelligence report of a U.S. government agency. She removed it from the building and sent a hard copy of the report to an online news outlet.

In an interview with the FBI in June 2017, Winner admitted knowing that the document would be valuable to U.S. adversaries and that the information contained in the report had not been released to the public.

She was sentenced to 63 months in prison followed by a three-year term of supervised release.

INDICATORS

- Access Attributes
- Security and Compliance Incidents
- Technical Activity

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. It's easy for billions of adversaries to follow your posts.

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 Common Methods are 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.

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

Which scenario is considered an Insider Threat?

A. Richard McCreadie, a financial analyst, introduces a virus into his company's systems that steals fractions of pennies from financial transactions being made by the company. Richard's plan assumes that because the transaction amounts are so small, his company would overlook his siphoning off cash to a personal bank account.

B. A hacker working for a foreign competitor found a flaw in a company's public webpage and used this flaw to access confidential information on one of the company's projects. The information gathered allowed the foreign competitor to beat the company to market, costing it millions in lost revenue.

C. Clark Peters, an employee, has received what looks like a phishing email. Clark does not open this email and informs IT of the email. Clark's suspicions were correct, and his actions ensured that this attempted attack was prevented.

D. Karen Fillippelli, a regional manager, has heard a rumor that one of her colleague's employees is working odd hours for no reason. Karen reports this information to the Facility Security Officer (FSO). During an investigation, it is determined that the employee is staying later to finish a project before they go on a vacation, and that this overtime has ben approved by the employee's manager.

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

Which scenario is considered an Insider Threat?

The Answer is A: Richard McCreadie, a financial analyst, introduces a virus into his company's systems that steals fractions of pennies from financial transactions being made by the company. Richard's plan assumes that because the transaction amounts are so small, his company would overlook his siphoning off cash to a personal bank account.

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 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.

If you have questions, you may also 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.

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

What kinds of indicators for an Insider Threat do you watch for and report?

A. Request for critical asset information outside of official channels, or requests for information that does not fall in a person's Need-To-Know.

B. Frequent or unreported foreign travel.

C. Suspicious foreign contacts, or suspected recruitment by foreign or domestic competitive companies.

D. Working odd hours for no apparent reason, or decline in work performance, excessive tardiness, unexplained absences, or conflicts with supervisors.

E. All of the above.

What kinds of indicators for an Insider Threat do you watch for and report?

The Answer is E: 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.

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

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

A. Change to my personal bank account.

B. My local U.S. travel during the holidays.

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

D. Change to my home address.

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

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

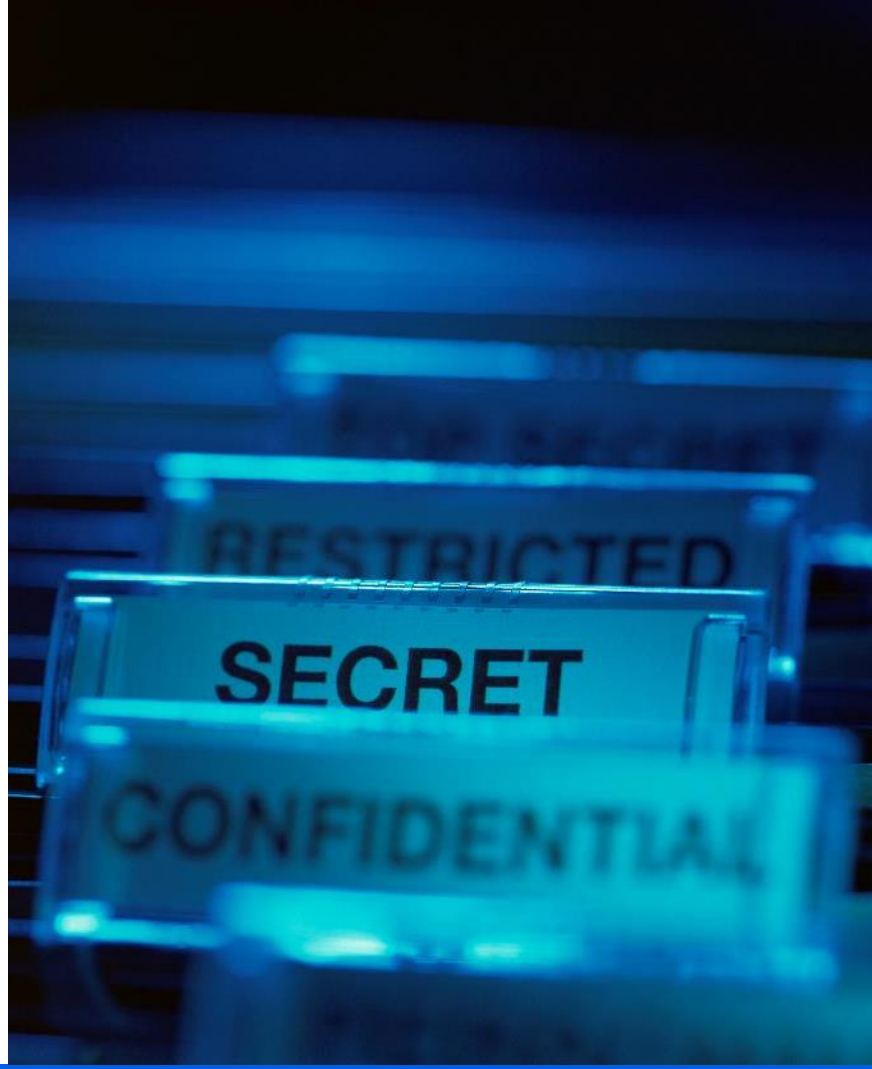
The Answer is C: Change in name, marital status, cohabitation of an intimate nature, and citizen status.

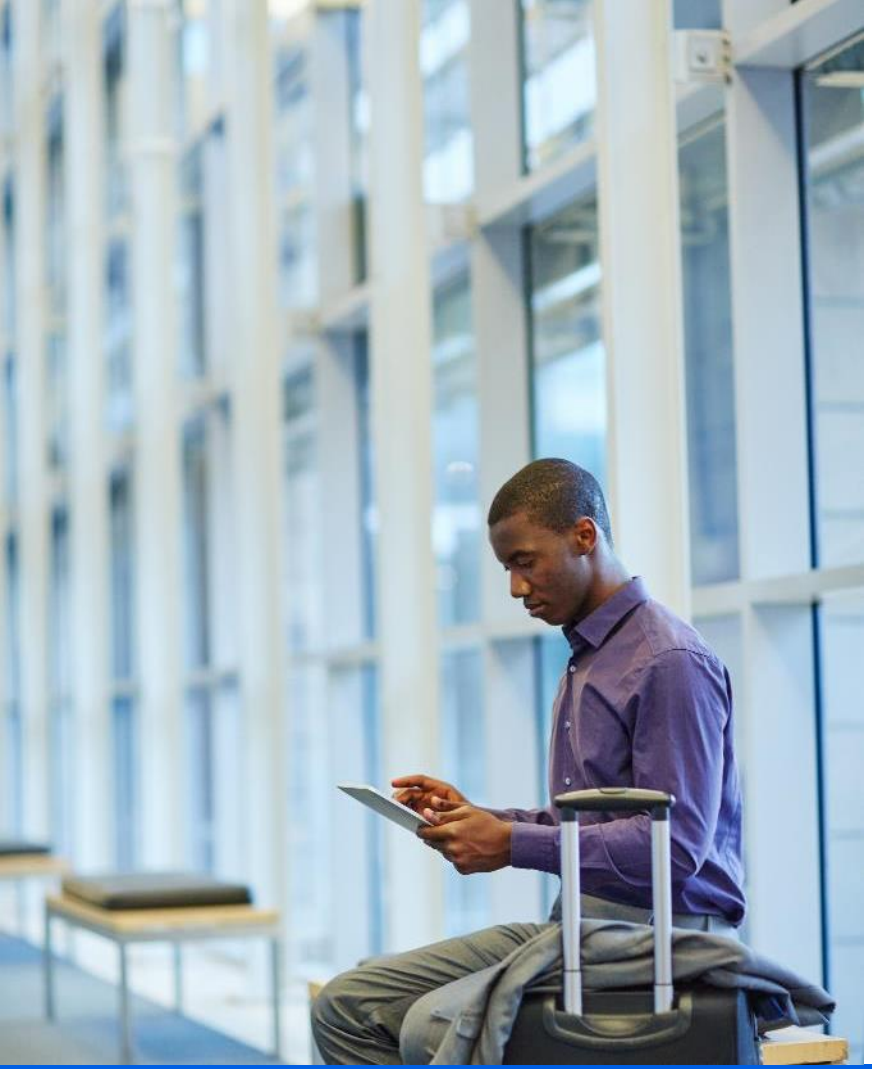
ANNUAL SECURITY & INSIDER THREAT AWARENESS

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 that adversaries might want
- Analyze how the loss of this information will affect your program
- Identify 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 U.S. A foreign contact who lives in the U.S. could pose the same threat as a foreign contact who lives overseas.

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.

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

True or False:

Whether personal or work related, you must report all foreign travel.

KNOWLEDGE CHECK: ANNUAL SECURITY & INSIDER THREAT AWARENESS

True or False:

Whether personal or work related, you must report all foreign travel.

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.

AKIMA

Your Security Team

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

Steve Mumphrey, Sr. Facility Security Officer: 571-482-5326 | Steve.Mumphrey@akima.com

Kendall Miller, Facility Security Officer: 703-766-6776 | Kendall.Miller@akima.com

Karen Jennings, Security Specialist III: 571-482-5358 | Karen.Jennings@akima.com

Matt Hicks, Facility Security Officer: 571-521-0867 | Matthew.Hicks@akima.com

Direct any questions to your Security Team contact.

AKIMA

Thank you for completing your training.

Click here to enter your completion record: Submit

Direct any questions to your

Security Team contact.