Annual Security & Insider Threat Awareness

2023

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 information security's 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, and
- All actual or suspected information security breaches will be reported to the Information Security Manager and will be thoroughly 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 did 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 (e-Qip/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 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

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

A. Eligibility determination is based on a completed e-Qip/eApp investigation and a person being a US Citizen.

B. Eligibility determination is based on a completed e-Qip/eApp 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 US meets the eligibility requirements.

E. I held a clearance in my last job.

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/eApp 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/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 e-Qip/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?

Continuous Vetting (CV) 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 program, a set of automated records 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, 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.

Financial Considerations, Personal Conduct, Misuse of IT Systems, and Handling Protected Information are all part of what guidelines?

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

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 continuous vetting process to maintain clearance eligibility.

Financial Considerations, Personal Conduct, Misuse of IT Systems, and Handling Protected Information are all part of what 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

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/eApp and than reviewed to determine suitability for granting eligibility.

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

D. The employee policy and procedures acknowledgement form.

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.

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 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 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

Match the following information categories to the correct definition:

A. Top Secret

B. Secret

C. Confidential

D. SBU

E. CUI

F. Company Private or Proprietary

I. Unclassified created or owned government information that requires safeguarding and dissemination controls.

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

III. Unauthorized disclosure will cause serious damage to US national security.

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

V. Unauthorized disclosure will cause damage to US national security.

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

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 US national security.

B. Secret - Unauthorized disclosure will cause serious damage to US national security.

C. Confidential - Unauthorized disclosure will cause damage to US national security.

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

E. CUI - Unclassified created or owned government information that requires safeguarding and dissemination controls

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.

Jeff has been assigned work on a contract involving classified information for XXX, LLC. 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, puts the files in a locked drawer of his desk; and removes his CAC to take with him. Has Jeff properly safeguarded the classified information?

Yes

Or

No

Jeff has been assigned work on a contract involving classified information for XXX, LLC. 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, puts the files in a locked drawer of his desk; and removes his CAC to take with him. 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 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. 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 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: Foreign Espionage

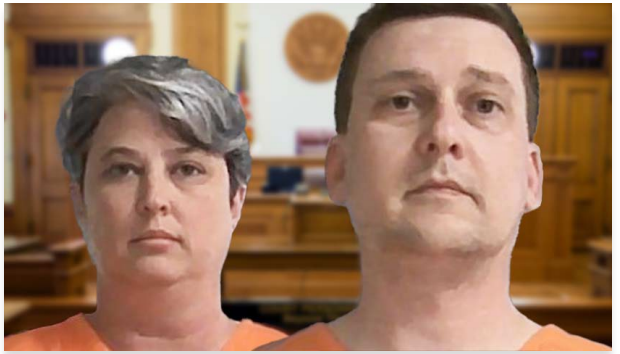
In April 2020, Jonathan Toebbe sent a package to a foreign government containing a sample of Restricted Data and instructions for establishing a covert relationship to purchase additional Restricted Data. Toebbe began corresponding via encrypted email with an individual whom he believed to be a representative of the foreign government. The individual was an undercover FBI agent.

On June 8, 2021, the undercover agent sent $10k in cryptocurrency to Toebbe as a “good faith” payment. On June 26, Toebbe dropped an SD card containing military sensitive information at a pre-arranged dead drop location while his wife, Diana, served as a lookout. After retrieving the SD card, the undercover agent sent Toebbe $20k and Toebbe emailed the decryption key.

This arrangement happened two more times. The FBI arrested Toebbe and his wife on October 9 after he placed yet another SD card at a pre-arranged “dead drop” at a location in West Virginia

INDICATORS

- Access Attributes
- Security and Compliance Incidents
- Financial Considerations



Click here to read the full case study

Insider Threat Case: Unauthorized Disclosure

After leaving the Air Force in July 2013, Daniel Everette Hale was employed by a defense contractor and assigned to the National Geospatial Intelligence Agency (NGA), where he worked as a political geography analyst. In connection with his active-duty service and work for the NSA, and during his time at NGA, Hale held a Top Secret/Sensitive Compartmented Information (TS/SCI) security clearance.

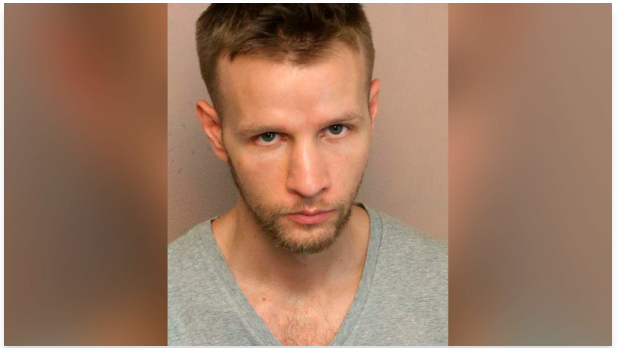
Hale admitted that he took classified documents he had no right to retain from his work at the NGA and sent them to a reporter while purposefully disregarding the law.

Hale became an anti-war activist and released documents because of his opposition to war and the use of drone warfare. After the release of the Drone Wars Papers, he spoke at events and gave multiple interviews.

After providing the documents to journalists, they were published, which led investigators to investigate the source of the documents, ultimately leading them to Hale as the source.

INDICATORS

- Access Attributes
- Security and Compliance Incidents
- Technical Issues



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.

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.

Which scenario is considered an Insider Threat?

A. Richard McCreadie, a Financial Analyst at XXX, LLC, introduces a virus into XXX'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, XXX would overlook his siphoning off cash to a personal bank account.

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

C. Clark Peters, an employee of XXX 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 for XXX, has heard a rumor that one of her colleagues' employee 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.

Which scenario is considered an Insider Threat?

The Answer is A: Richard McCreadie, a Financial Analyst at XXX, LLC, introduces a virus into XXX'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, XXX 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. Although 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 this 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)

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.

ANNUAL SECURITY & INSIDER THREAT AWARENESS

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. 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?

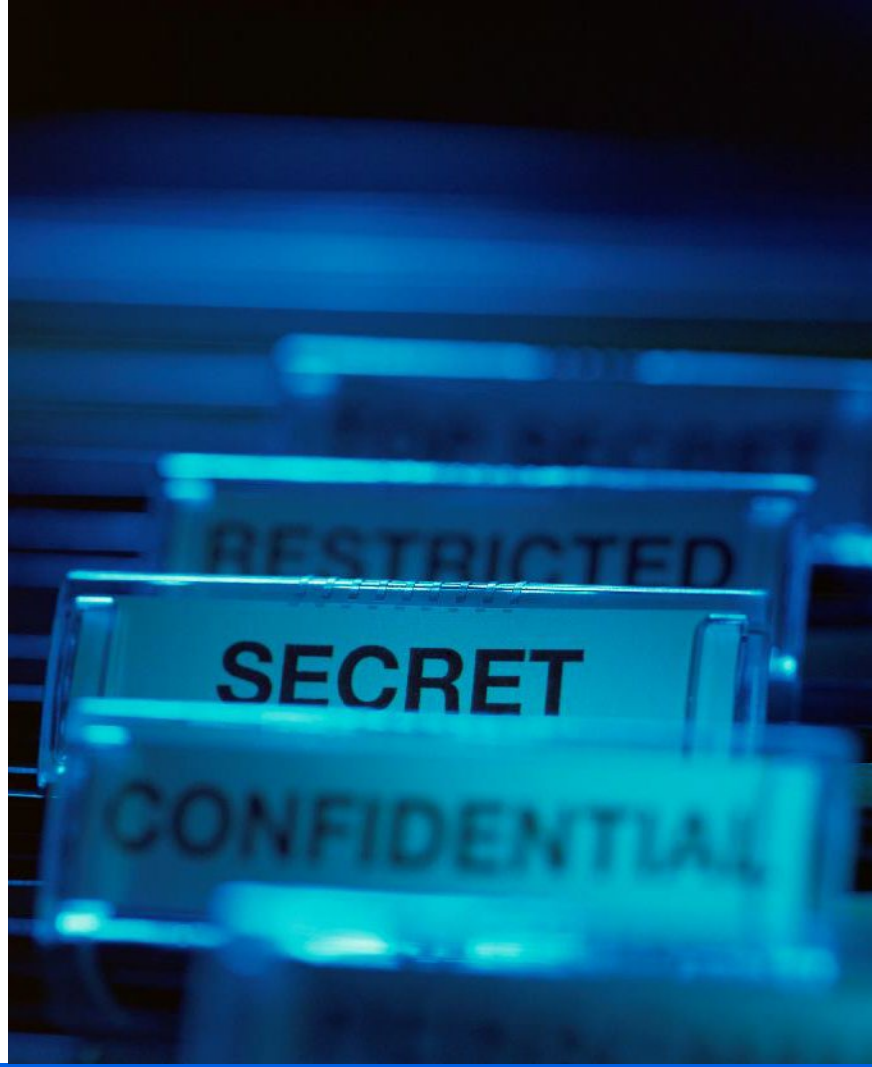
The Answer is C: Change in name, marital status, cohabitation of an intimate nature, and citizen status.

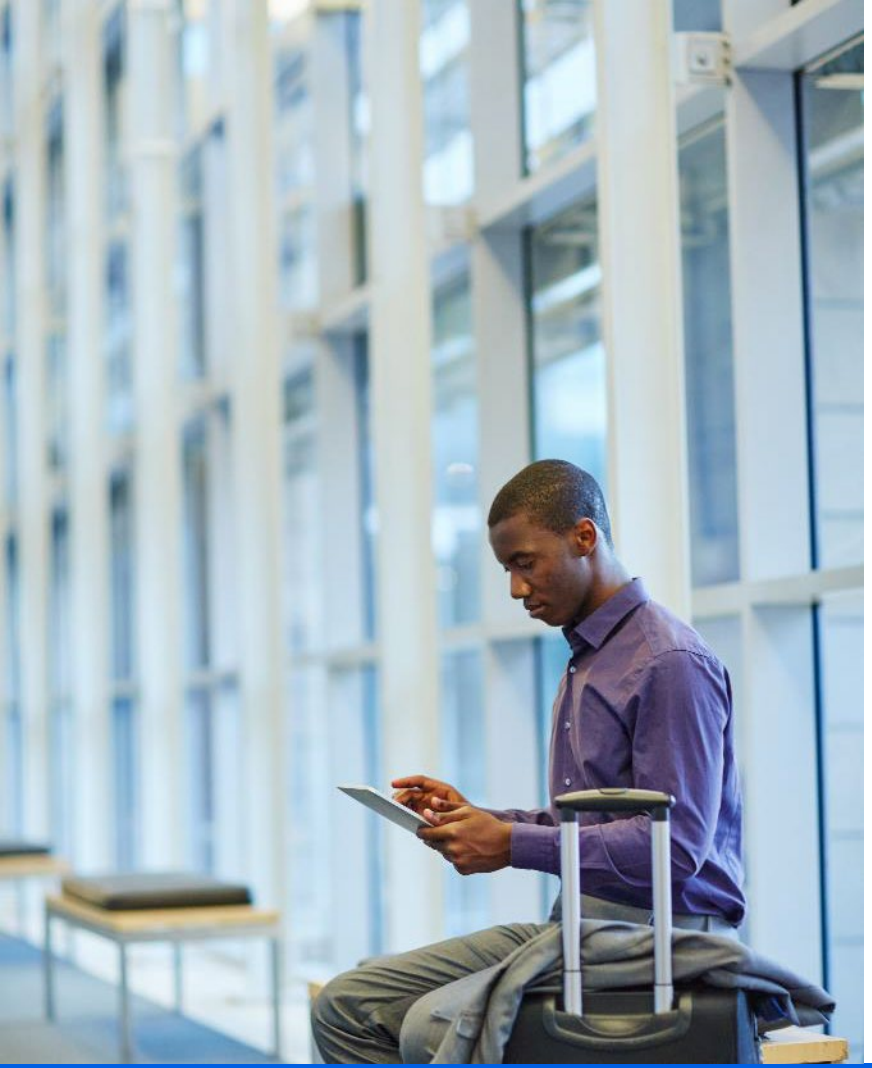
ANNUAL SECURITY & INSIDER THREAT AWARENESS

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 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.

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

Adam Santee, Security Specialist: 571-323-6169 | Adam.Santee@akima.com

Security@akima.com