

The logo for AKIMA, consisting of the word "AKIMA" in a bold, white, sans-serif font. The background of the slide features a blue-toned image of a person's hands clasped together, overlaid with a complex, circular, technical diagram resembling a radar or network map.

Annual Security & Insider Threat Awareness

2021

ANNUAL SECURITY & INSIDER THREAT AWARENESS

Why Do We Need This Training?

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

We have been granted a Facility Clearance (FCL) which determines that our company is eligible for access to classified information and/or the award of a classified contract. 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 **National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M** 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 the security team to include 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

How Do I Get Cleared?

The Department of Defense Central Adjudication Facility (DoD CAF) grants security clearance eligibility based upon the personal information you provide on your application (e-Qip) and the completed vetting of your background investigation.

Along with the eligibility determination, your Need-to-Know needs to be established. Do you work on a contract that requires that your position be cleared? If so, check the table below to see what else needs to be considered.

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

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 person being a US Citizen.
- B. Eligibility determination is based on a completed e-Qip investigation and a Need-to-Know 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.

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 based on contract requirements and the position the individual holds.

ANNUAL SECURITY & INSIDER THREAT AWARENESS

What Forms Do I Need to Complete?

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 which is known as the periodic review; a Tier 5 Review (T5R) – Top Secret, SCI or Tier 3 Review (T3R) – Secret or Confidential. The SF86 is 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 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

ANNUAL SECURITY & INSIDER THREAT AWARENESS

Allegiance to the United States, Foreign Preference, Sexual Behavior, and Criminal Conduct are all part of what 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 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.

ANNUAL SECURITY & INSIDER THREAT AWARENESS

Allegiance to the United States, Foreign Preference, Sexual Behavior, and Criminal Conduct are all part of what guidelines?

The Answer is C: These are 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.



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 than 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.

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

Briefing Requirements

All cleared employees are required to receive a Security and Insider Threat briefing prior to accessing classified information. In addition, you may be required to have NATO, COMSEC, SAP, SCI and any contract-specific trainings/briefings.

The DD254, Classification Guide or other instructions/requirements in the contract you work for may include classified safeguarding guidelines and restrictions and/or be based on your specific job/ location.

All employees **must** comply with the client security requirements. This may include access to the client IT systems and any classified information. 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.

Classified Information Categories

Classified Information is any information where unauthorized disclosure could adversely affect the national security of the United States. It is information that is 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.

ANNUAL SECURITY & INSIDER THREAT AWARENESS

Match the following information categories to the correct definition:

- | | |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| A. Top Secret | I. Unclassified government information which cannot be disclosed to the general public and must not be circulated. |
| B. Secret | II. Unauthorized disclosure will cause exceptionally grave damage to the US national security. |
| C. Confidential | III. Unauthorized disclosure will cause serious damage to US national security. |
| D. SBU/CUI | IV. Business information not to be divulged to individuals outside the company. |
| E. FOUO | V. Unauthorized disclosure will cause damage to US national security. |
| F. Company Private
or Proprietary | 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/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

How do you safeguard classified information?

- 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
- Has to be properly marked with classification
- Must be stored in an approved GSA storage container
- Never process 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.



ANNUAL SECURITY & INSIDER THREAT AWARENESS

Milton Waddams has been working on a contract involving classified information for Initech. He has a stack of files containing classified information on his desk awaiting his review. After Milton realizes that a coworker borrowed his red stapler and never returned it, Milton leaves his desk and files unattended to chase down the coworker with his red stapler. Milton properly safeguarded the classified information.

True

Or

False

ANNUAL SECURITY & INSIDER THREAT AWARENESS

Milton Waddams has been working on a contract involving classified information for Initech. He has a stack of files containing classified information on his desk awaiting his review. After Milton realizes that a coworker borrowed his red stapler and never returned it, Milton leaves his desk and files unattended to chase down the coworker with his red stapler. Milton properly safeguarded the classified information.

The Answer is: False



ANNUAL SECURITY & INSIDER THREAT AWARENESS

Public Release of Information

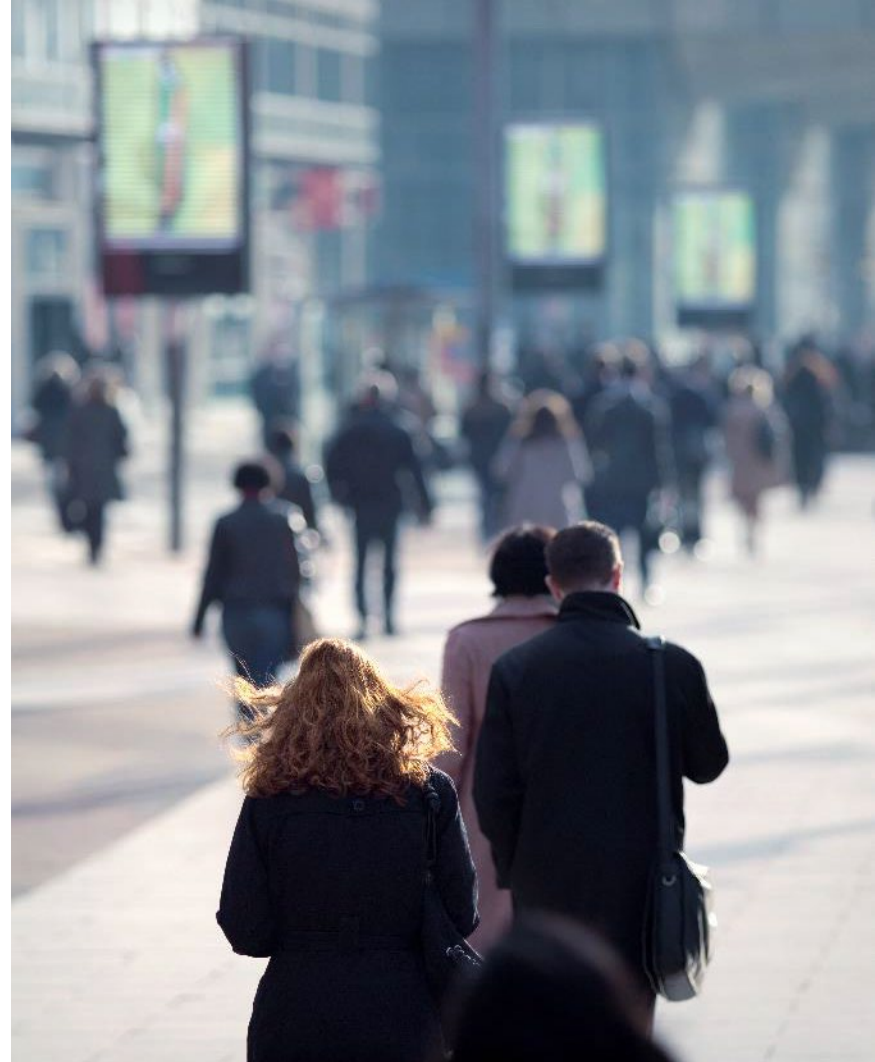
Any information (classified or unclassified) pertaining to your contract cannot be released for public dissemination except as provided by the National Industrial Security Program Operating Manual (NISPOM) unless it has been approved for public release by a U.S. government authority. Proposed public 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

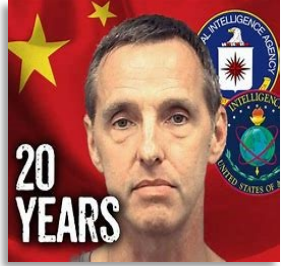
An Insider Threat is any person with authorized access to any U.S. government resources, including personnel, facilities, information, equipment, networks, or systems, who uses that access either wittingly or unwittingly to do harm to the organization or national security. An Insider Threat looks no 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: Espionage & Conspiracy

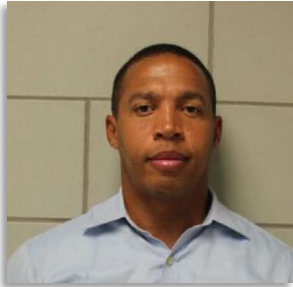


Kevin Patrick Mallory was a self-employed consultant with GlobalEx LLC who spoke fluent Mandarin Chinese. He was targeted by China via a fake profile on a professional networking site and recruited to turn over classified information before being arrested. He had previously held numerous positions with various U.S. government agencies and several defense contractors through which he was granted a Top Secret security clearance. In March and April 2017, Mallory travelled to Shanghai to meet Michael Yang, who claimed to represent a People's Republic of China think tank but was an agent of the People's Republic of China Intelligence Service. Yang gave Mallory a smartphone so they could covertly communicate. FBI analysts determined Mallory had completed all of the steps necessary to securely transmit four documents using the smartphone. One of the documents provided to the Chinese operative contained unique identifiers for human sources who had helped the United States government.

Mr. Mallory was arrested in Leesburg, VA and a federal court sentenced him to 20 years prison for conspiring to transmit national defense information to the People's Republic of China.

The FBI has produced a CI Video based on this case. To watch access: [The Nevertime Connection — FBI](#)

Insider Threat Case: Illegally Accessing and Damaging a Computer Network



Shannon Stafford worked in the IT department of a global company with thousands of employees and offices around the world. He had access to the system login credentials of other employees and was authorized to use them while performing his technical support duties. He was also responsible for disabling users' network access credentials at the end of their employment. In 2014, Stafford was promoted to manager and technical site lead. In 2015, he was demoted back to an IT support role due to performance issues. He was eventually fired in 2016 and did not return his company laptop. He made several attempts to access the company's network using multiple credentialing. While most attempts were unsuccessful, he was finally able to access and he erased all file storage drives at one location, then changed credentials for the storage management system.

Mr. Stafford was convicted in federal court and sentenced to 12 months plus one day in prison followed by 3 years of supervised release. Furthermore, he was ordered to pay restitution in the amount of \$193,258 to his former employer

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.

ANNUAL SECURITY & INSIDER THREAT AWARENESS

Which scenario is considered an Insider Threat?

- A. Peter Gibbons, a computer programmer at Initech, introduces a virus into Initech's systems that steals fractions of pennies from financial transactions being made by the company. Pete's plan assumes that because the transaction amounts are so small, Initech would overlook Pete siphoning off the cash to a personal bank account.
- B. A hacker working for a foreign competitor found a flaw in Initech's public webpage, and used this flaw to access confidential information on one of Initech's projects. The information gathered allowed the foreign competitor to beat Initech to market, costing Initech millions in lost revenue.
- C. Michael Bolton, an employee of Initech has received what looks like a phishing email. Michael does not open this email, and informs IT of the email. Michael's suspicions were correct, and his actions ensured that this attempted attack was prevented.
- D. Karen Fillippelli, a regional manager for Initech, 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 been approved by the employee's manager.

Which scenario is considered an Insider Threat?

The Answer is A: Peter Gibbons, a computer programmer at Initech, introduces a virus into Initech's systems that steals fractions of pennies from financial transactions being made by the company. Pete's plan assumes that because the transaction amounts are so small, Initech would overlook Pete siphoning off he 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.

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.

ANNUAL SECURITY & INSIDER THREAT AWARENESS

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.
- Adverse information which includes criminal activities, 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.

ANNUAL SECURITY & INSIDER THREAT AWARENESS

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

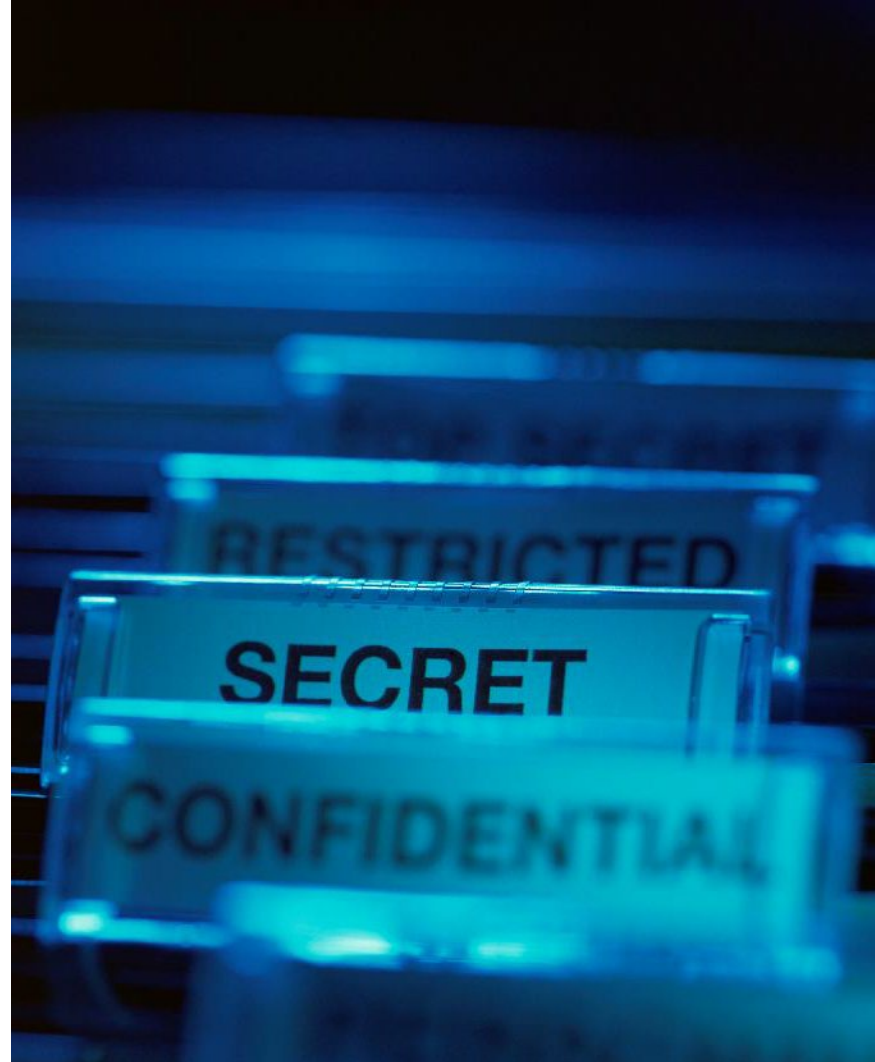
The Answer is C: Change in name, marital status, cohabitation of an intimate nature, and citizen status.

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, assessing 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

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

True

Or

False

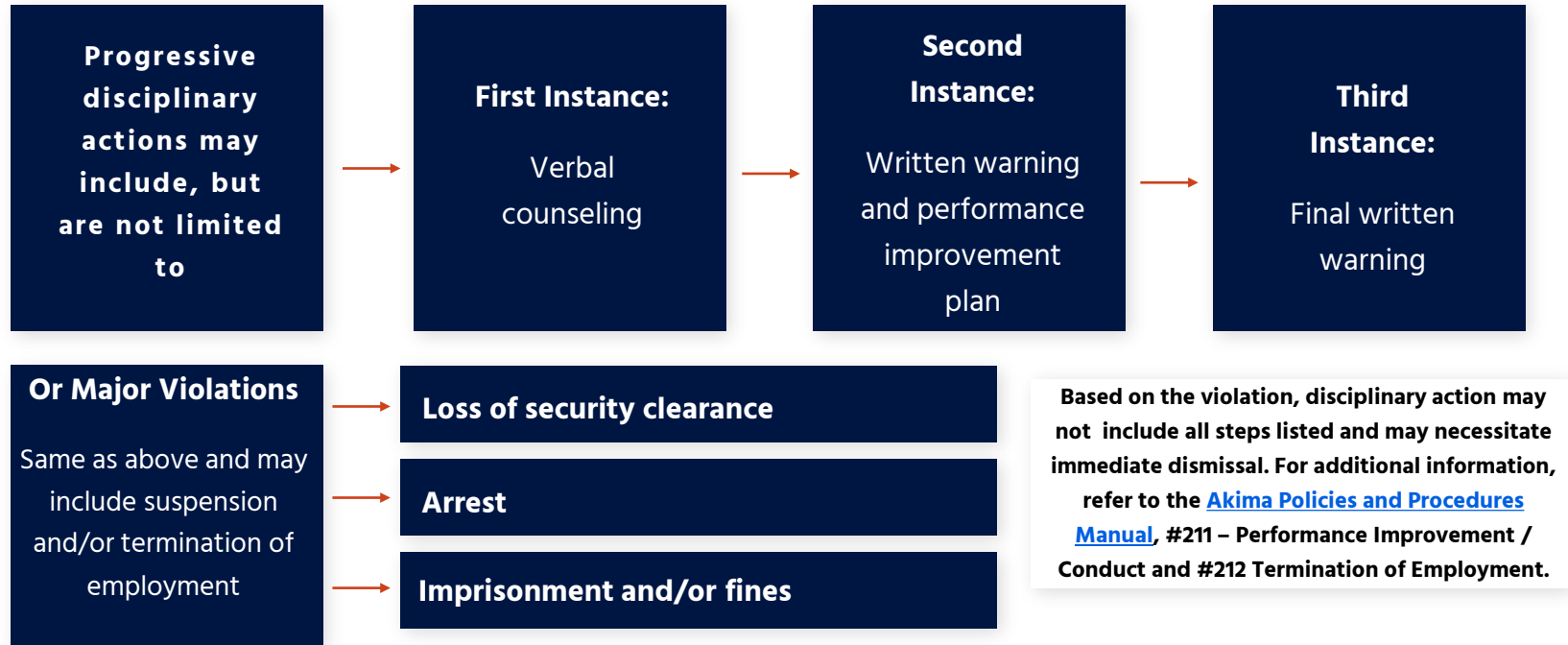


ANNUAL SECURITY & INSIDER THREAT AWARENESS

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

The Answer is: True

Disciplinary Graduated Scale Actions for Security Violations



The AKIMA logo is displayed in a bold, white, sans-serif font at the top center of the slide. The background features a dark blue color with a faint, circular graphic of concentric lines and a central keyhole, suggesting a focus on security and technology.

Your Security Team

Herndon

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

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

Manassas

Adam Santee, Facility Security Officer: 571-323-6169 | Adam.Santee@jadecreekllc.com

Colorado Springs

Melissa Graham, Facility Security Officer: 719-355-2298 | Melissa.Graham@akima.com

Huntsville

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

[Security Page on the Employee Portal](#)

AKIMA

Thank you for completing your training.

Click here to enter your completion record:



Direct any questions to your

Security Team contact.