Annual Security & Insider Threat Awareness

2020

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).

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

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.

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

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

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

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

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 my 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 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.

Other categories of not classified info that also need to be protected:

- **For Official Use Only (FOUO)** – Unclassified government information which cannot be disclosed to the general public and must not be circulated.
- **Controlled Unclassified Information (CUI)** – Unclassified information that cannot be disclosed to the general public. This includes technical information. Any compromise must be reported within 72 hours of discovery. Data security controls as outlined in SP 800-53 of the National Institute of Standards and Security (NIST) apply. Subcontractors must be provided with data security standards.
- **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

B. Secret

C. Confidential

D. 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 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 technical information.

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.

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

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

Stewart David Nozette was the president, treasurer, and director of the Alliance for Competitive Technology (ACT), a non-profit organization. From 2000 through 2006 he used ACT to defraud the U.S. Naval Research Laboratory, the Defense Advanced Research Projects Agency, and NASA by making more than $265,000 in fraudulent reimbursement claims. Additionally, from 2001 through 2005, he willfully evaded over $200,000 in federal taxes. Nozette held security clearances as high as Top Secret and had regular access to classified information.

In September 2009, an undercover FBI agent contacted Nozette via telephone purporting to be an Israeli intelligence officer. He agreed to provide classified information in exchange for money and a foreign passport to a country without U.S. extradition. A series of contacts followed over the next weeks, including meetings and exchanges in which Nozette took $10,000 in cash left by the FBI at pre-arranged drop-off sites. He provided classified information concerning satellites, early warning systems, defense or retaliation against large-scale attacks, communications, and defense strategy.

Potential risk indicators included fraudulently billing the government and misuse of IT systems.

Nozette pleaded guilty to attempted espionage, conspiracy to defraud the U.S., and tax evasion. He was sentenced to 13 years in prison and ordered to pay $217,000 in restitution to the government agencies he defrauded.

Insider Threat Case: Unauthorized Retention of Classified Information

Reynaldo Regis worked as a cleared CIA contractor between August 2006 through November 2016. Part of his job was to research people in classified databases. He copied classified information into personal notebooks and conducted unauthorized searches of classified databases. Investigators were unable to determine a motive for his actions and found over 60 notebooks containing classified information while searching his home. The classified information found in the notebooks included data relating to highly sensitive Intelligence reports, disclosure of which could cause serious damage to national security. Although, his motivations are unknown, his disregard for security protocol placed this information at risk.

Potential risk indicators included mishandling of classified information, conducting unauthorized searches, lying to federal law enforcement, and suspicious behavior.

Regis pleaded guilty to unauthorized removal and retention of classified materials as well as making false statements to federal law enforcement officers. He was sentenced to 3 months in prison with 3 years of supervised release that included a requirement to notify the CIA of any travel outside the country.

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
- Front companies for third parties 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. 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.

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 ben approved by the employee's manager.

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. 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.

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

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.

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.

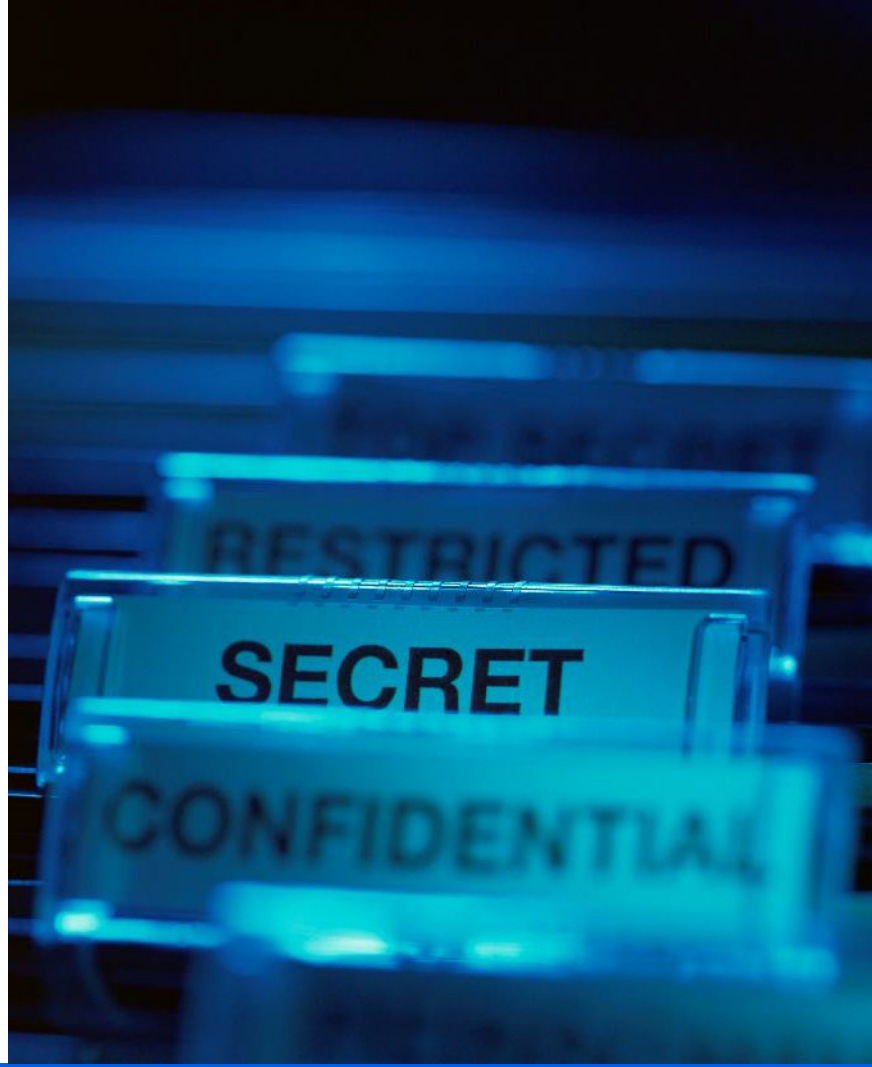
D. My attempts to enlist others in illegal or questionable activities.

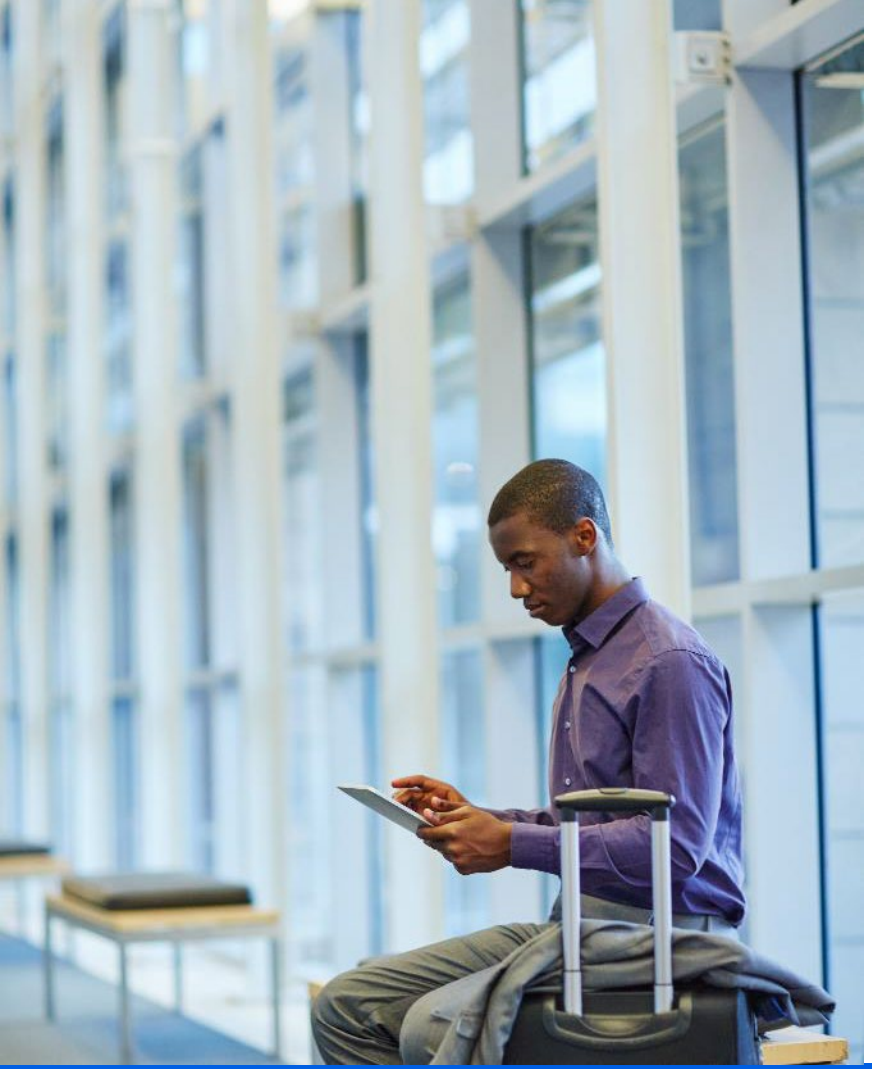
ANNUAL SECURITY & INSIDER THREAT AWARENESS

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.

AKIMA

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

True

Or

False

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 include all steps listed and may necessitate immediate dismissal. For additional information, refer to the Akima Policies and Procedures Manual 2020, #211 – Performance Improvement / Conduct and #212 Termination of Employment.

AKIMA

Your Security Team

Herndon

Steve Bata, Director of Security, Facility Security Officer: 571-323-5209 | Steven.Bata@akima.com
Kendall Miller, Senior Security Specialist: 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

Security Page on the Employee Portal

AKIMA

Thank you for completing your training.

Click here to enter your completion record: Submit

Direct any questions to your

Security Team contact.