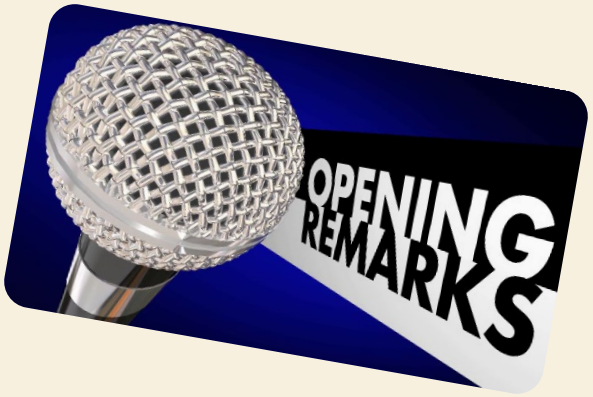
ANNUAL SECURITY BRIEFING

February 2019



We are bound by Executive Order 12829, 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 is a determination that a company is eligible for access to classified information or award of a classified contract. Our cleared companies have completed a DoD Security Agreement (DD441) which outlines its security responsibilities.

As a cleared employee or consultant, YOU are equally bound under the law to provide the same protection.

DO I NEED TO BE CLEARED?

The Department of Defense Central Adjudication Facility (DoD CAF) grants a security clearance based upon the personal information provided on your application (eQIP) and completed background investigation.

Along with the eligibility determination, your Need to Know needs to be established. The table below shows what needs to be considered along with contract requirements and/or DD254 issued.

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

ARE YOU ELIGIBLE?

The Department of Defense Central Adjudication Facility (DoD CAF) grants a security clearance based upon the personal information provided on your application (eQip) and appropriate back ground investigation.

- Completed SF86 forms are reviewed to determine suitability for granting a security clearance and are subject to continuous evaluation submitted by your security team:
  - Tier 5 – Top Secret, SCI
  - Tier 3 – Secret, Confidential
- Completed SF85 forms are reviewed to determine Public Trust suitability and are submitted by government agencies:
  - Tier 1 – NACI with favorable results
  - Tier 2 or 4 – MBI/BI: NACI with favorable results and a credit check

WHAT DETERMINES ELIGIBILITY?

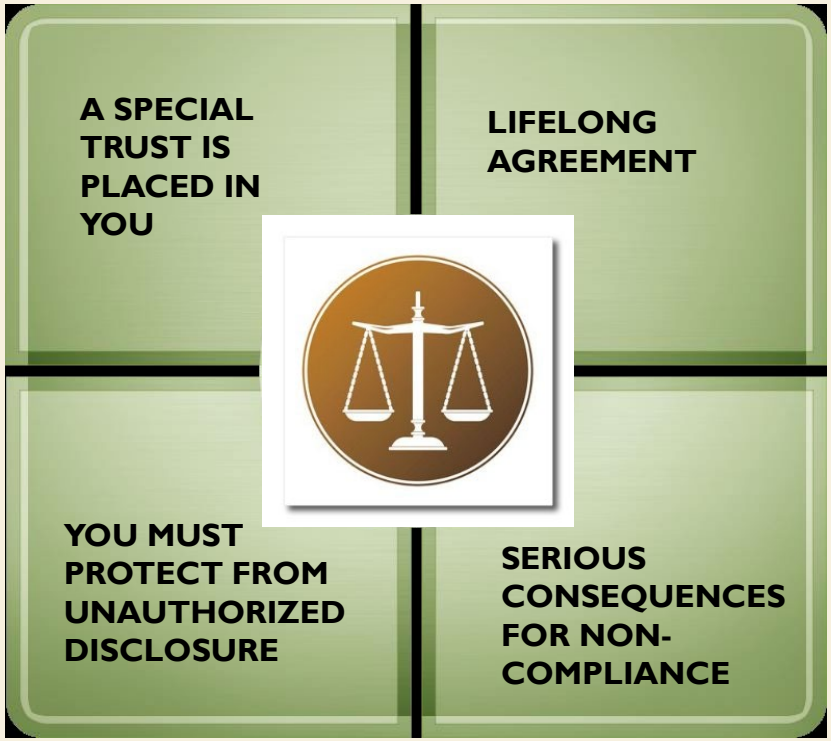
Security eligibility judgment is based on pattern of behavior, not a single action. It is the "whole person" concept and is based on the following Adjudication Guidelines:

- Allegiance to the United States
- Foreign influence
- Foreign preference
- Sexual behavior
- Personal conduct
- Financial considerations
- Alcohol consumption
- Psychological Conditions
- Drug involvement

  NOTE: *Possessing and using marijuana is legal in some states but it is still a federal crime and will impact your clearance.*

- Criminal conduct
- Handling Protected Information
- Outside activities
- Misuse of information technology systems

SF312 NON-DISCLOSURE



Once cleared, you are required to sign a non-disclosure (SF312) is a contractual agreement between you (the employee) and the U.S. government. A special trust has been placed in you; you are responsible to protect classified information from unauthorized disclosure.

This NDA is binding for life even if you no longer require a security clearance. Any breach of the terms of this agreement can result in serious consequences including a loss of your security clearance, fines, and even jail time.

BRIEFING REQUIREMENTS

- All cleared employees will receive a Security and Insider Threat briefing prior to accessing classified information. This may include NATO, COMSEC, SAP, SCI and any contract specific trainings/briefings as well.
- Dependent upon your specific job and location, security procedures will be based upon instructions provided by the client through DD 254; Classification Guide or other instruction/requirement stated in your contract which may include classified safeguarding guidelines and restrictions.
- All employees must comply with the client security requirements to include security briefings; access to client provided IT systems and classified information.
- A violation of client security policies and procedures may be grounds for removal from the contract.
- You must be knowledgeable of reporting requirements, classified security violations/infractions and the consequences of non-compliance.
- Must adhere to the terms of the Standard Practice Procedures (SPP).

WHAT IS CLASSIFIED INFORMATION?

Information where the unauthorized disclosure of which could adversely affect the national security of the United States.

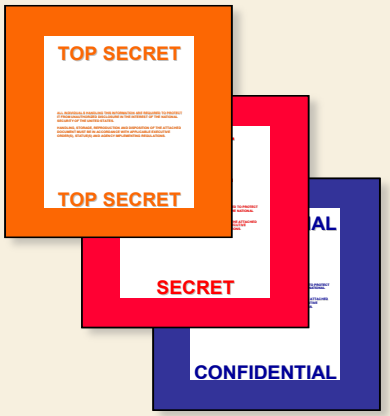
Information that falls under one or more categories of Section 1.4 of Executive Order 13526 may be eligible to be classified:

a) military plans, weapons systems, or operations
b) foreign government information
c) intelligence activities (including covert action), intelligence sources, methods, or cryptology
d) foreign relations or foreign activities of the United States, including confidential sources
e) scientific, technological, or economic matters relating to the national security
f) United States Government programs for safeguarding nuclear materials or facilities
g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security
h) the development, production, or use of weapons of mass destruction

It 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.

You have a responsibility to report information that you believe is improperly or unnecessarily classified. Contact your security official for additional guidance for submitting a classification challenge.

CLASSIFIED CATEGORIES



- **Top Secret**-The unauthorized disclosure of information will cause exceptionally grave damage to US national security.
- **Secret**-The unauthorized disclosure of information will cause serious damage to US national security.
- **Confidential**-The unauthorized disclosure will cause damage to US national security.
- There are other categories of information which, while not classified, also deserve mention:

- **For Official Use Only (FOUO)** is unclassified government information which is exempt from general public disclosure and must not be given general circulation.
- **Company private or proprietary information** is business information not to be divulged to individuals outside the company.

CONTROLLED
UNCLASSIFIED
INFORMATION

- **Controlled Unclassified Information.** The treatment of this type of information will be addressed in follow on slides

CONTROLLED UNCLASSIFIED INFORMATION

CUI

Controlled Unclassified Information refers to unclassified information that is to be protected from public disclosure. There are many subcategories to this information and includes technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. The term does not include information that is lawfully publicly available without restrictions. There are no exceptions for commercial items.

- Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

Contractors are required to safeguard unclassified controlled technical information and to report the compromise of such information to the DoD within 72 hours of discovery.

Contractors subject to the clause and are required to implement data security controls identified in **National Institute of Standards and Security (NIST)** publication SP 800-53

Contractors are **responsible for assuring that their subcontractors** that are provided with controlled technical information also comply with the data security standards.

"KEEP IT SAFE"

Safeguarding Classified information:

- Must never be left unattended.
- Must never be discussed in public places.
- May only be discussed on secure telephones
- Must be under the control of an authorized person.
- Must be properly marked.
- Stored in an approved GSA storage container.
- Never be processed on your computer unless approved by the Designated Approval Authority.

It is your personal responsibility to know the person you are interacting with is both properly cleared and has a need to know.

You must never reveal or discuss classified information with anyone other than those that are properly cleared and have a need to know.

If in doubt ask your Security Team

PUBLIC RELEASE OF INFORMATION

Any information (classified or unclassified) pertaining to your contract shall not 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 US Government authority. Proposed public releases shall be submitted for review and approval prior to release to the appropriate government approval authority identified 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.

INSIDER THREAT

An Insider Threat can be anyone….

WHAT TO LOOK FOR AND REPORT

Information to be reported based on facts ***NOT*** rumors:

- Unexplained affluence or financial difficulties
- Substance abuse (alcohol or drugs), arrests or criminal conduct, treatment for emotional or mental disorders, out of character behavior
- Requests to access information he/she do not have a need to know
- Working odd hours for no apparent reason
- Foreign relations - close & continuing relationship and if approached about classified information and/or acts suspiciously
- Any employment or service (paid or unpaid) with any business enterprise organized under the laws of another country.
- Known or suspected espionage or sabotage, suspicious contacts
- Divided loyalty or allegiance to the US

REPORTING REQUIREMENTS

Other items you are required to report are:

- Changes to Name, Marital Status, Cohabitation of an intimate nature, Citizenship
- Loss, compromise, (or suspected loss or 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 of 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

SOCIAL MEDIA

Have you checked your social media accounts lately? Social Media – including Facebook, Twitter, Google+ and LinkedIn, can be used for foreign adversaries to gather information about you, your family and your work history. Here's some tips to help protect your info:

- Only establish and maintain connections with people you know and trust. Review your connections often. Report any foreign and/or suspicious connections to your security team.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share. Update your privacy settings.
- Ensure that your family takes similar precautions with their accounts; their privacy data can expose your data.
- Avoid posting or tagging images of you or your family that clearly show your face. Never post your Smartphone photo.
- Use a secure browser when possible and monitor your browsing history to ensure that you recognize all access points.

FOREIGN TRAVEL

- You must report all work or personal Foreign Travel and a foreign travel briefing is required. Personnel holding TS/SCI may have additional reporting requirements. Check with your government client or FSO. It is your responsibility to make those arrangements BEFORE you leave.
- You will need to complete the briefing and complete a reporting form detailing your trip. You may even get a telephone call from your FSO to discuss your trip prior to and upon your return as well.
- Develop a personal travel plan and give it to your office and family
- Learn the cultures, customs and laws of the country you visit.
- Visit https://travel.state.gov to find country specific information such as:
  - What countries are on the national threat list
  - What countries have high crime/type
  - Shots required
  - Visa/Passport requirements, etc..

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

For Major Violations

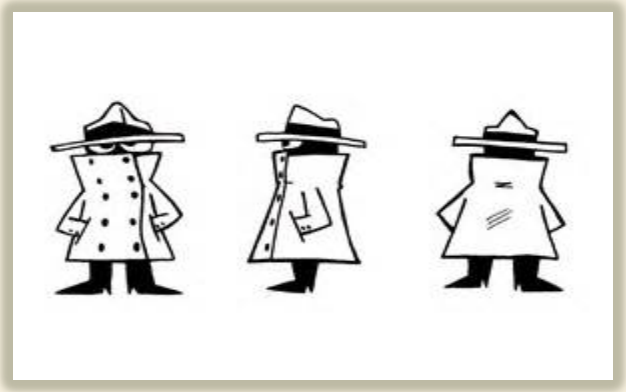
- Same as above and may include suspension/termination of employment
- Loss of security clearance
- Arrest
- Imprisonment and/or fines

Based on the violation, disciplinary action may not include all steps listed and may necessitate immediate dismissal. For additional information refer to the Employee Handbook; Policy 211 Employment – Performance Improvement/Conduct; and Policy 212 Employment – Termination of Employment.

WHAT ARE WE DEFENDING?

Information concerning military capabilities, locations, equipment; and technology is protected for a reason. Unauthorized release of this information, whether classified or sensitive can have a detrimental effect on the Warfighters' survivability.

CI AWARENESS
ECONOMIC & INDUSTRIAL ESPIONAGE



Every day in the United States and abroad, spies attend trade shows, send e-mails, monitor communications, troll social media and use other legal & illegal methods to steal proprietary, unclassified and classified information.

The increasing value of technology and trade secrets in the global and domestic marketplaces, along with the temporary nature of many high-tech employments have increased both opportunities and incentives for espionage.

WHO ARE THE ADVERSARIES?

- 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

METHODS USED INCLUDE:

- **Coercion/Blackmail**
- **Cultivation of Relationships**
  - Social media friend requests; professional requests used to glean your information and information from people you are connected to
- **Suspicious Network Activity**
  - Cyber Intrusion; Viruses/Malware; Backdoor Attacks; Acquiring User Names/Passwords
- **Attempted Acquisition of Technology**
  - Front Companies for Third Parties use to get Protected Info; Controlled Technologies; Equipment; Diagrams; and Plans
- **Request for Information**
  - Attempt to get info through price quotes or market surveys
- **Solicitation or Marketing Services**
  - Foreign entities through sales, rep or agency offers; RFI/RFP responses for technical or business services
- **Seeking Employment**
  - Resume submissions, applications and references – be especially careful with connections with foreign entities

If you encounter any of these situations that seem suspicious, contact your security representative

OPSEC – OPERATIONS SECURITY

OPSEC is a systemic process that is used to mitigate vulnerabilities and protect sensitive, critical, or classified information. This process increases the overall security in any organization. It helps you identify critical information, analyze the threat, know the vulnerabilities, assess the risk, and implement counter measures.

IDENTIFY CRITICAL INFORMATION ANALYZE THE THREAT

Identify:

- Know what needs protecting…what information do we have that our adversaries might want to get their hands on? This is not always classified information either –
- UNCLASSIFIED does not mean it is not important. Adversaries will take any piece of information they can get their hands on.
- They can be quite clever and very patient…it may take months or years for them to gather information one piece at a time. When they have found all of the right pieces, they can form the big picture of their potential target(s).

Analyze:

- Research and analysis of intelligence, counterintelligence, and open source information to identify likely adversaries to a planned operation
- Ask yourself these questions…
- How would the loss of sensitive data effect your program?
- What would be the cost of losing sensitive or classified information?

VULNERABILITIES

These are some of the most common vulnerabilities and some consistent indicators of an Insider Threat:

- Not locking your work station when needing to leave your desk
- Inappropriate use of email/attachments and the web
- Lack of awareness
- Leaving sensitive information out in the open
- Attempt to obtain info without a genuine "need to know" that info.
- Repeated, unusual or unnecessary overtime
- Unauthorized removal of classified, sensitive, or proprietary info from a work area
- Being caught repeatedly for bringing electronic devices in sensitive work areas
- Excessive hoarding of sensitive information
- Network user account is identified as using excessive storage space; printing an abnormally high volume of documents; sending an abnormal amount of emails with large file attachments
- Sudden purchase of high-value items for which no logical source of income exists
- Extensive or regular gambling losses or financial indebtedness
- Upon return from travel, the employee has a difficult time describing travel details
- Employees demeanor suddenly changes for the worse; disgruntled, depressed, angry, moody, temperamental, sad, isolationist, and/or defeatist.

As cleared individuals, it's important for you to remember that it IS your responsibility to challenge and report anyone that may be a potential threat to national security

RISKS & COUNTERMEASURES

Assessing the Risk

- First, analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability.
- Second, specific OPSEC measures are selected for execution based upon a risk assessment done by management and then informs the staff and gives the proper action.

Examples of some counter measures used when facing a threat:

- "NEED TO KNOW"
- Visitor Control
- Report Suspicious Activities
- Agency Badge Removal
- Public Conversations
- Sanitize bulletin boards
- Safe Combinations
- Use COMMON SENSE

WHO TO CALL

- Defense Department 1-800-424-9098, (703) 693-5080
- Defense Intelligence Agency (703) 907-1307
- National Security Agency (301) 688-6911
- Department of Army 1-800-CALLSPY (1-800-225-5779)
- Naval Criminal investigative Service 1-800-543-NAVY (1-800-543-6289)
- Air Force Office of Special Investigations (202)767-5199
- Central Intelligence Agency Office of the Inspector General (703) 874-2600
- Department of Energy (202) 586-1247
- US Nuclear Regulatory Commission Office of the Inspector General 1-800-233-3497
- US Customs Service 1-800-BE-ALERT (1-800-232-5378)
- Department of Commerce/Office of Export Enforcement (202) 482-1208 or 1-800-424-2980 (to report suspicious targeting of US export-controlled commodities)
- Department of State Bureau of Diplomatic Security (202) 663-0739
- When traveling overseas, suspect incidents should be reported to the Regional Security Officer (RSO) or Post Security Officer (PSO) at the nearest U.S. diplomatic facility

SUBMIT YOUR COMPLETION RECORD

Now that you have reviewed this presentation click here to enter your completion record:

This will acknowledge that you have received the briefing, have been given an opportunity to ask questions and that you understand that you have a personal obligation to safeguard national security information.

The Security Team will get an email confirmation attesting your completion of this briefing.

Thank you.