SECURITY BRIEFING

2026

ANNUAL SECURITY TRAINING
AS REQUIRED BY THE NATIONAL
INDUSTRIAL SECURITY PROGRAM

FACILITY SECURITY OFFICER:

CHINNA R NEMELIDINNE

INSIDER THREAT OFFICIAL:

CHINNA R NEMELIDINNE

Table of Contents

I Introduction

WELCOME,

Initial Orientation Training is required per DoDM 5220.22M, (National Industrial Security Program Operating Manual [NISPOM]) Chapter 3. This training provides basic security knowledge to recognize and respond to threats to National Security Information.

As a cleared company under the National Industrial Security Program (NISP), we are required to adhere to the United States Code, applicable Executive Orders (EO), the NISPOM, and other Government security directives. This briefing is being provided in accordance with the NISP.

Every employee granted a U.S. Government security eligibility (i.e., clearance) is required to receive an initial security training and sign a Non-Disclosure Agreement (Standard Form 312) prior to any classified access as well as receiving a security refresher training annually. This briefing was developed to meet both training requirements.

What is the Threat?

According to the Defense Counterintelligence and Security Agency (DCSA - formerly known as DSS),

> Suspicious contact reporting suggests"[…] there is a concerted effort to exploit cleared contractors for economic and military advantage."

Additionally,

> "The exploitation of cyberspace continues to be a key area of concern. An increase in unsolicited contacts made with cleared industry employees from compromised accounts amplifies the potential for compromise of cleared individuals, classified programs, or classified systems occurring in the unclassified cyber domain."
>
> — *Defense Security Service/National Counterintelligence and Security Center pamphlet on Counterintelligence Awareness (https://www.dcsa.mil/Portals/91/Documents/CI/ci_awareness.pdf)*

Who is Being Targeted?

Foreign collectors will target ANYONE with access to the information they are trying to gather. Typically, the following are high in the list of targeted collections:

- **Developers** – Scientists, researchers, and engineers working on leading edge technologies
- **Technicians** – Specialists who operate, test, repair or maintain the technology
- **Production personnel** – Those who access production lines or supply chain
- **IT personnel** – System Administrators or others who access associated networks
- **Business Development Personnel**
- **Human Resources personnel** – They have access to personnel records
- **Facility personnel** – Anyone with access to the cleared facility

What is Being Targeted?

The seven most commonly targeted technology categories of the Industrial Based Technology List are:

- **Aeronautic Systems** – Unmanned Aerial Vehicles & Drones; Fixed Wing Combat Aircraft; Rotary Wing Aircraft
- **C4** – Telecommunication Devices (phones, cell phones, radios, radio mounts); Antennas; Common Data Links
- **Electronics** – Circuit Boards; Integrated Circuits; Micro-sensors
- **Radars** – Continuous Wave Radars; Electronically Steered Radars; Pulse Radars
- **Armament & Survivability** – Missiles; Body Armor; Armaments, Explosives
- **Optics** – Optics; Lenses; Reflective Coatings
- **Software –** Modeling & Simulation Software; Software Algorithms; Artificial Intelligence Software

If you don't know whether the technology you work on is being targeted, ask your FSO or Supervisor!

What is an Insider Threat?

"A threat presented by a person who has, or once had, authorized access to information, a facility, a network, a person, or a resource of the Department and wittingly, or unwittingly, commits an act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities or destructive acts, which may include physical harm to another in the workplace" (National Defense Authorization Act 2017)

"The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified NSI." (NISPOM Ch. 2 February 28, 2006)

Insider Threat Awareness

Insider Threats may include:

- Espionage
- Unauthorized Disclosures
- Workplace Violence
- Sabotage
- Fraud
- Security Violations
- Unwitting actions that increase vulnerabilities

Potential Risk Indicators (PRI)

- **Access Attributes** – having access to classified or critical unclassified information, systems, facilities or training.
- **Professional Lifecycle and Performance** – declining or poor performance ratings, reprimands, HR complaints, demotion, suspension, or other negative performance traits.
- **Foreign Considerations** – citizenship, travel to countries of concern, frequent foreign travel, possession of foreign assets, foreign passport or residency, living with a foreign national, unauthorized contact with a foreign intel entity.
- **Security and Compliance Incidents** – Compliance or security violations or infractions, non-compliance with training requirements, timecard fraud, denial suspension or revocation of security clearance, accessing facilities at unusual hours, attempt to gain access to classified information without proper clearance, failure to self-report.

Potential Risk Indicators do not indicate one will commit a hostile act, only that there is a potential.

Potential Risk Indicators (PRI) cont.

- **Technical Activity** – violating acceptable IT user policies, suspicious emails or browsing activity, attempting to introduce unapproved USB devices, large volumes of data transferred, introduction of unauthorized software, disabling firewall or anti-virus, introducing malicious code.
- **Criminal, Violent, or Abusive Conduct** – Violent behavior including sexual assault and domestic violence, exhibiting violence at work, possessing unauthorized weapon, criminal affiliation, threatening violence, self-harm or suicidal ideations.
- **Financial Considerations** – Financial crime, bankruptcy, delinquent debt, not filing tax returns, garnishment of pay, unexplained affluence, gambling problems.
- **Substance Abuse and Addictive Behaviors** – Using or selling illegal drugs, misusing or selling prescription drugs, treatment for abuse of drugs or alcohol.

Potential Risk Indicators do not indicate one will commit a hostile act, only that there is a potential.

Potential Risk Indicators (PRI) cont.

- **Judgement, Character, and Psychological Conditions** – falsifying data, expressing ill will toward U.S. or place of employment, demonstrating extremist views, associating with extremist groups, insanity pleas in criminal case, anti-social or compulsive behavior, mental instability, failure to successfully complete a polygraph.

Potential Risk Indicators do not indicate one will commit a hostile act, only that there is a potential.

II.a Insider Threat Awareness

- Report every threat to protect your company and yourself.
- Early identification and reporting of risk indicators will allow our Insider Threat Program to respond appropriately to mitigate risk and help those in need before it's too late.

Case Study
Read and Consider – What if this wasn't reported???

Local police received a tip about a man displaying concerning behavior. The tip did not indicate any criminal acts, but the police learned the man held a security clearance and shared the information with the "Agency." The Agency's Insider Threat Program (ITP) investigated the matter and followed up with Subject's supervisor who disclosed Subject seemed "off" for a few weeks. Despite this, the supervisor did not report the matter or take any action.

The ITP also followed up with Subject's friend who had filed the initial tip. The friend stated he too had noticed something "off" but wasn't sure what to do about it. Later, Subject asked the friend to hold his guns. When Subject delivered the guns to the friend, they were fully loaded. Subject only offered a vague explanation for why he wanted the guns held and, a few weeks later, asked for them to be returned. The friend sensed something was really wrong, refused to return the guns, and contacted the police.
The ITP worked with Subject to identify the source of the problem and obtain appropriate help. The ITP leveraged the Agency's Human Resources and Employee Assistance Program to provide support to the Subject. With medical intervention the Subject's behavior improved and he returned to work.

II.a

Insider Threat Awareness

What were the Potential Insider Risk Indicators?

- *Altered mental health behavior*
- *Unusual personal interactions*
- *Potential harm to self or others*
- *Potential misuse of weapons*

What was the outcome?

•Agency HR representative (ITP Team member) discussed the concerning behavior with Subject. Subject claimed his new wife was a spy who was sent to assassinate him.
•Further discussion led to an admission by Subject that he had recently increased his prescribed medication without supervision of his doctor.
•Subject was referred to the Employee Assistance Program where he was encouraged to check with his physician.
•The physician adjusted Subject's medications and he returned to work with no further incident.
•The ITP stayed engaged with HR and EAP to evaluate and mitigate potential risks associated with Subject.

What was the Impact?

• High risk behavior by Subject was avoided
•Potential for negative workplace event was reduced
•Subject maintained his job and the Agency retained a valued employee

Insider Threat Reporting Requirements

"If you see something, say something."

- If you have a concern, report it to your **FSO**, your **Insider Threat Program Senior Official**, a member of the **Insider Threat Program (ITP) Committee**, your **direct supervisor**, **or as otherwise directed.**
- All reports may be written or oral. They should be unclassified. They are submitted in confidence. All reports will be investigated.

Common Collection Methods

Acquisition of the Technology – Includes attempts to acquire protected information in the form of controlled technologies, whether the equipment itself or diagrams, schematics, plans spec sheets or the like.

Exploitation of Business Activities – This include joint ventures, partnerships, mergers and acquisitions, foreign military sales, or attempted development of service provider relationships.

Exploitation of Cyber Operation Methods – Phishing attacks, compromised third party websites, removable media.

Request for Information/Solicitation – Conferences, conventions, tradeshows, email, mail, phone, web forms, foreign visits.

Reportable Suspicious Contacts

- Efforts to obtain access to classified information without need-to-know
- Contact with known or suspected intelligence officers
- Any contact that suggests you may be the target of attempted exploitation
- Attempts to entice cleared persons into compromising situations
- Attempts by foreign customers to gain access to information that exceeds the export license
- Attempts to solicit cleared personnel with special treatment, favors, gifts, or money.
- Requests for protected information disguised as a price quote or purchase.

Immediately notify your Facility Security Officer and/or DCSA representative if you observe any of the above behaviors.

Classification System Overview

EO 13526 – Classified National Security Information

- **Original Classification**
  - Initial determination made by a U.S. Government Official authorized to have Original Classification Authority (OCA), that information requires protection against unauthorized disclosure in the interest of national security.

- **Derivative Classification**
  - Reproduction, extraction, incorporation, or paraphrasing of information already classified into a new form.
  - By authorized persons required to restate classified source information.
  - Proper classification markings are to be applied to the newly created work.
  - Duplication or reproduction of existing classified information is NOT derivative classification.

Levels of Classification

- Levels of classification are based on the amount of damage to national security expected to be caused by the unauthorized disclosure of sensitive material.

TOP SECRET	Expected to cause exceptionally grave damage
SECRET	Expected to cause serious damage
CONFIDENTIAL	Expected to cause damage

Classification System Overview

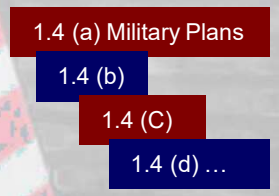
Classification Categories

- Information may only be classified if it concerns one or more of the listed Categories in EO 13526 Sec. 1.4, (a-h)

  Examples: military plans or weapons systems; intelligence activities

Duration of Classification

- Declassify on Specific Date or Event
- Maximum time for classification is 25 years
- Unless exempt (EO 13526, Sec. 3.3 (b))
- Still classified if compromised (think Wikileaks)
- If declassified, public release is NOT automatic



EO 13526
Classified National Security Information

Classification Challenges

- Authorized holders who believe information is improperly classified are encouraged and expected to bring these concerns to the attention of responsible management or security officials who will then bring it to the attention of the appropriate Government Contracting Agency.

Prohibitions and Limitations

- Information shall not be classified, continue to be upheld as classified, or fail to be declassified in order to:
  - Conceal violations of law, inefficiency, or administrative error
  - Prevent embarrassment to a person, organization, or agency
  - Restrain competition
  - Prevent or delay the release of information that does not require protection in the interest of national security
- Avoid passing classified information forward that is improperly classified or marked.
- Compilations of individually unclassified items may be classified if the compiled information shows a classified relationship.

Derivative Classification Principles

- Only use authorized sources for classification guidance.
- Observe and respect Original Classification Authority (OCA) classification determinations.
- Apply standard markings to derivatively classified materials.
- Take necessary steps to resolve classification conflicts.
- The final document will be classified the same as the highest sourced document.
- The Declassify On date will be the same as the source document for a single. source and will be the most restrictive date for multiple source documents.
- Derivative classifiers are required to have training every two years.

Authorized Sources for Derivative Classification

- Security Classification Guide (SCG).
- Properly marked source document.
- DD Form 254 (contract-specific classification instructions).

Derivative Classification Markings

- Markings shall be uniformly and conspicuously applied to leave no doubt about the *(1)* classified status of the information, *(2)* the level of protection required, and *(3)* the duration of the classification.

- Basic Classified Marking Requirements:
  - Date of Document
  - Portion Markings
  - Interior Page Markings
  - Overall Classification
  - Classification Authority Block

Classification Markings

Portion Markings

Placed in front of subjects, titles, subtitles, paragraphs, and illustrations

(TS) TOP SECRET
(S) SECRET
(C) CONFIDENTIAL
(U) UNCLASSIFIED

SECRET

(U) Now is the time for all good men to come to the aid of their country.

(C) A man said to the Universe, Sir, I exist. However, replied the universe, the fact has not engendered in me a sense of obligation.

(S) He either fears his fate too much, or his deserts are small, that puts it not unto the touch.

SECRET

Interior Page Markings

Classification at top and bottom for information on **that** page or the overall document

TOP SECRET
SECRET
CONFIDENTIAL
UNCLASSIFIED

SECRET

(U) Now is the time for all good men to come to the aid of their country.

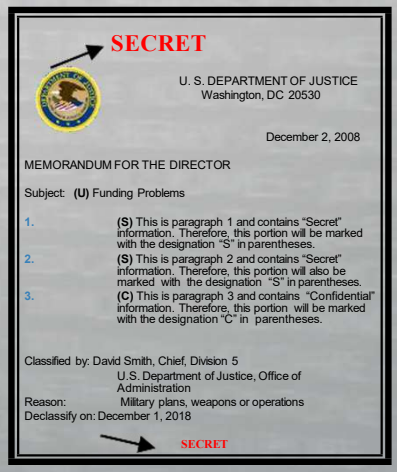
(C) A man said to the Universe, Sir, I exist. However, replied the universe, the fact has not engendered in me a sense of obligation.

(S) He either fears his fate too much, or his deserts are small, that puts it not unto the touch.

SECRET

Overall Classification

The highest level of classified information and caveats contained in a document is the overall marking


SECRET

U. S. DEPARTMENT OF JUSTICE
Washington, DC 20530

December 2, 2008

MEMORANDUM FOR THE DIRECTOR

Subject: **(U)** Funding Problems

1. **(S)** This is paragraph 1 and contains "Secret" information. Therefore, this portion will be marked with the designation "S" in parentheses.
2. **(S)** This is paragraph 2 and contains "Secret" information. Therefore, this portion will also be marked with the designation "S" in parentheses.
3. **(C)** This is paragraph 3 and contains "Confidential" information. Therefore, this portion will be marked with the designation "C" in parentheses.

Classified by: David Smith, Chief, Division 5
U.S. Department of Justice, Office of Administration
Reason: Military plans, weapons or operations
Declassify on: December 1, 2018

SECRET

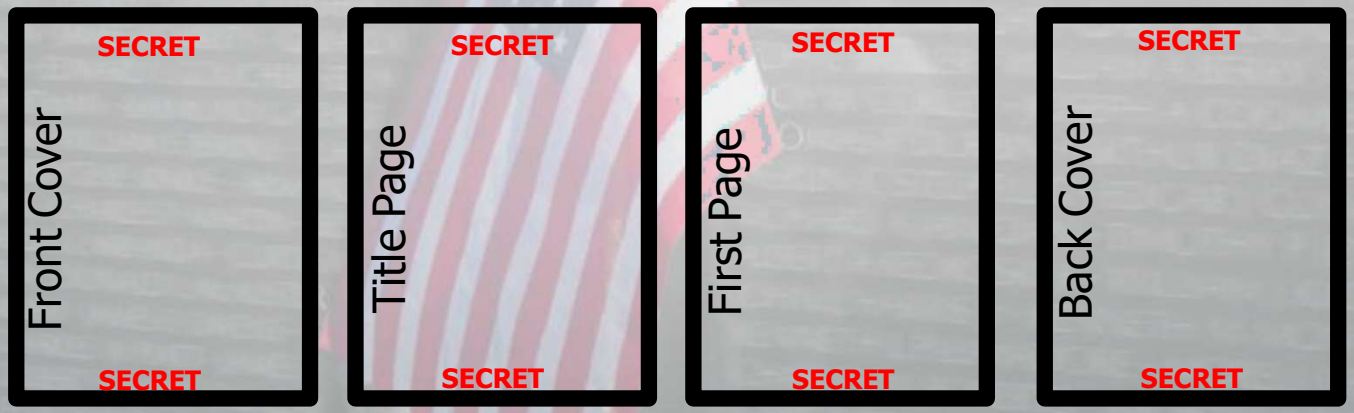
***All markings contained on this slide are for training purposes only. All information is unclassified NISPOM 4-216**

Overall Classification

Multi Page Documents

The overall marking is to be conspicuously marked or stamped at the top and bottom on the outside of the front, the title page, the first page, and on the outside of the back.

Please don't forget to mark the outside back of the material or use a second cover sheet for the back.



***All markings contained on this slide are for training purposes only. All information is unclassified NISPOM 4-216**

Classification Authority Block

This required block shows the source of classification and instructions for declassification:

Derivative Classification Block	
"Classified By" line	Identifies derivative classifiers by name and position, or by personal identifier – company name, address, and when applicable, the division or branch will follow if not apparent on the face of the document.
"Derived From" line	Cite the source document or the classification guide on this line, including the title, date, agency and, where available, the office of origin.
"Declassify On" line	The derivative classifier will carry forward the instructions on the "Declassify On" line from the source document to the derivative document, or the duration instruction from the classification or declassification guide.

Classification Authority Block Examples

***All markings contained on this slide are for training purposes only. All information is unclassified NISPOM 4-216**

Original

SECRET

U. S. DEPARTMENT OF HELP

Washington, DC 20530

January 5, 2011

MEMORANDUM FOR THE DIRECTOR

Subject: (U) Funding Problems

1. (S) This is paragraph 1 and contains "Secret" information , Therefore, this portion will be marked with the designation "S" in parentheses.

2. (S) This is paragraph 2 and contains "Secret" information. Therefore, this portion will be marked with the designation "S" in parentheses.

3. (C) This is paragraph 3 and also contains "Confidential" information. Therefore, this portion will be marked with the designation "C" in parentheses.

Classified by: David Smith, Asst. Director, Division 5
U.S. Department of Help, Office of Administration
Reason: 1.4 (a)
Declassify on: January 1, 2026

SECRET

Derivative

SECRET

ACME Corporation

111 Main St. NW, Washington, DC 20530

January 5, 2015

MEMORANDUM FOR THE DIRECTOR

Subject: (U) Funding Problems Future Analysis

1. (S) This is paragraph 1 and contains "Secret" information , Therefore, this portion will be marked with the designation "S" in parentheses.

2. (S) This is paragraph 2 and contains "Secret" information. Therefore, this portion will be marked with the designation "S" in parentheses.

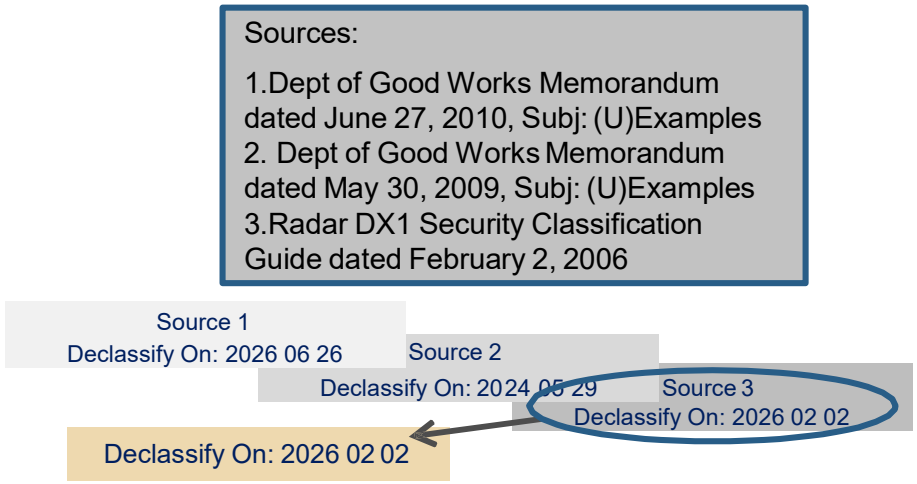
3. (C) This is paragraph 3 and also contains "Confidential" information. Therefore, this portion will be marked with the designation "C" in parentheses.

Classified By: Dr. Tim Doe, Sr. Analyst, Mission Support Division
Derived from: Memo Dated 1/2/2011, Subject: (U) Funding Problems, U.S. Dept. of Help, Office of Administration
Declassify on: January 1, 2026

SECRET

- When using multiple source documents, the "Derived From" line shall appear as:
  - Derivative classifiers will include a listing of the source materials on, or attached to, each derivatively classified document.
  - The "Declassify On" line shall reflect the <u>longest duration of classification of all sources.</u>

Derived from multiple sources:



Obsolete Declassification Instructions (OADR) (MR) (X1 – X8)

- Documents that are classified derivatively from a source with one of these obsolete instructions:
  - OADR *(Originating Agency's Determination Required)*
  - MR *(Manual Review)*
  - X1, X2, X3, X4, X5, X6, X7, or X8 *(Exemption Codes)*

- Derivative classifiers shall calculate a date 25 years from the date of the source document for the "Declassify On" line

- Do not continue with the obsolete instructions

OADR or MR Information Block Example:

Source Document (Dated 2 FEB 1994)
Classified By: John E. Doe, Chief Division 5
Reason: 1.4(a)
Declassify On: OADR

Derivative Document
Classified By: Joe Carver, Director
Derived From: Department of Good Works

Memorandum dated 2 Feb1994
Subj: (U) Examples
Declassify On: 2019 02 02

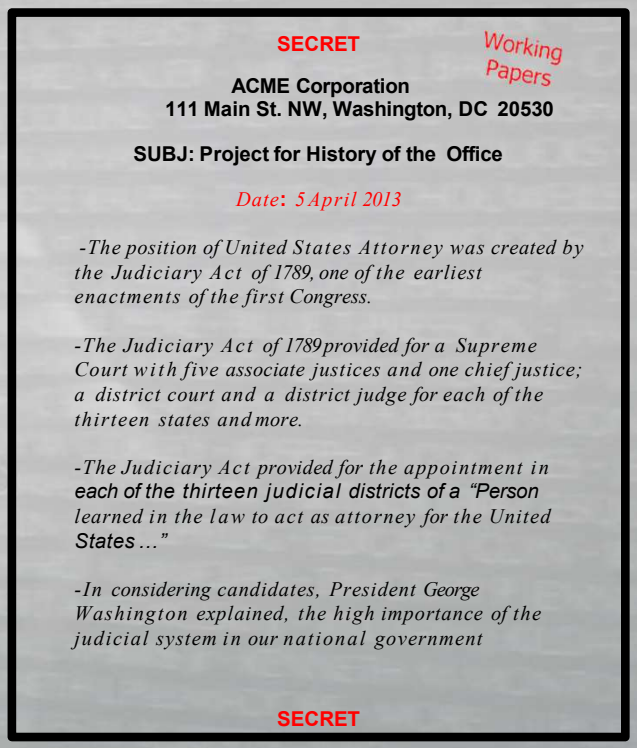
X1 – X8 Information Block Example:

Source Document (Dated 20 AUG 2002)
Classified By: John E. Doe, Chief Division 5
Reason: 1.4(a)
Declassify on: X3

Derivative Document
Classified By: Joe Carver, Director
Derived From: Department of Good Works
Memorandum dated 20 Aug 2002
Subj: (U) Examples
Declassify On: 20270820

Classified Notes or Working Papers

- Classified notes or "Working Papers" must have:
  - Overall Classification marked on the top and bottom on the outside (both front and back)
  - Date of origination
  - Safeguarded as classified material
    - Must have complete markings (all portion marks and classification Authority block) before:
    - Its transmission out of a facility
    - Being retained past 180 days
    - Filed permanently



SECRET

Working Papers

ACME Corporation
111 Main St. NW, Washington, DC 20530

SUBJ: Project for History of the Office

Date: 5 April 2013

-The position of United States Attorney was created by the Judiciary Act of 1789, one of the earliest enactments of the first Congress.

-The Judiciary Act of 1789 provided for a Supreme Court with five associate justices and one chief justice; a district court and a district judge for each of the thirteen states and more.

-The Judiciary Act provided for the appointment in each of the thirteen judicial districts of a "Person learned in the law to act as attorney for the United States…"

-In considering candidates, President George Washington explained, the high importance of the judicial system in our national government

SECRET

***All markings contained on this slide are for training purposes only. All information is unclassified NISPOM 4-216**

Disciplinary Action

- Personnel will be subject to appropriate disciplinary actions if they knowingly, willfully, or negligently:
  - Disclose to unauthorized persons, information that is properly classified
  - Classify or continue the classification of information in violation of EO 13526
  - Create or continue a special access program contrary to the requirements of EO 13526
  - Contravene any other provision of EO 13526 or its implementing directives

- Specific graduated scale of disciplinary actions may be found in the employee handbook and may include:
  - Reprimand
  - Suspension without pay
  - Removal
  - Loss or denial of access to classified information
  - Other sanctions in accordance with applicable laws and agency regulations

Controlled Unclassified Information (CUI)

- The Controlled Unclassified Information (CUI) Program standardizes the way the Executive branch handles unclassified information that does not meet the criteria required for classification under E.O. 13526, "Classified National Security Information," or the Atomic Energy Act but must still be protected. CUI **does not include** classified information.

- There are two types of CUI Categories: CUI Basic and CUI Specified.

- This briefing is just to make employees aware of additional controlled materials they may come in contact with. Employees must review their specific agency's CUI policy prior to marking or handling any CUI. The handling of CUI must be in accordance with E.O. 13556, "Controlled Unclassified Information".

Obligation to Report (Self-Reporting)

- If you hold a security clearance, you are required to report certain events that may impact the status of that clearance. Such events may include:
  - Allegiance to the United States
  - Foreign influence
  - Foreign preference
  - Sexual behavior
  - Personal conduct
  - Financial considerations
  - Alcohol consumption
  - Drug involvement
  - Psychological conditions
  - Criminal conduct
  - Handling protected information
  - Outside activities
  - Use of Information Technology

--The 13 Adjudicative Guidelines **- Guidelines established for determining eligibility for access to classified information.**

Reporting Obligations and Requirements

- **Employment Termination:**
  - Prior notice is required
  - All employees, both cleared and uncleared must be out-briefed by the appropriate security officer

- **Out-briefing includes:**
  - Completing security debriefing forms
  - The return of all keys, access cards, and equipment
  - Verify with your exiting FSO clearance information for future employment
    - Provides you with copies of security paperwork
    - Provides you with information regarding your clearance

These steps enable your future employer the ability to service and maintain your clearance.

Reporting Obligations and Requirements

Foreign Travel Briefing

- All personnel with a security clearance are required to report foreign travel to their security team prior to departure.
- If you have a security clearance Foreign Travel to Cuba is prohibited (Please see the Department of State website for more information).
- Foreign travel increases the risk of you becoming a target for foreign intelligence services.

Collection techniques include:

- Intrusions or searches of hotel rooms, briefcases, luggage, etc.
- Tracking activity via ATM transactions and Internet usage.
- Bugged hotel rooms or airline cabins.
- Intercepts of fax and email communications.
- Recording of telephone calls and communications.
- Recruitment or substitution of airline employees.
- Unauthorized access to or theft of electronic devices to install malicious software.

Reporting Obligations and Requirements

Foreign travel security countermeasures include:

- Don't publicize travel plans and limit sharing of this information to people who need to know
- Obtain pre-travel security information (Department of State)
- Keep hotel room doors locked (Take note of how the room looks when you depart)
- Limit sensitive conversations - public areas are rarely suitable for the discussion of sensitive information
- Hotel rooms could have electronic surveillance devices hidden within
- Never use computer or fax equipment at foreign hotels or business centers for sensitive matters
- Ignore or deflect intrusive or suspected inquiries and conversations about professional or personal matters
- Keep unwanted sensitive material until it can be disposed of securely

Bottom Line: Be Alert … Be Aware … Report Suspicious Occurrences!

Reporting Obligations and Requirements

Employee Reporting is Critical!

Cleared employees are required to report changes in personal status:

- Death
- Name change
- Termination of employment
- Change in citizenship

As well as:

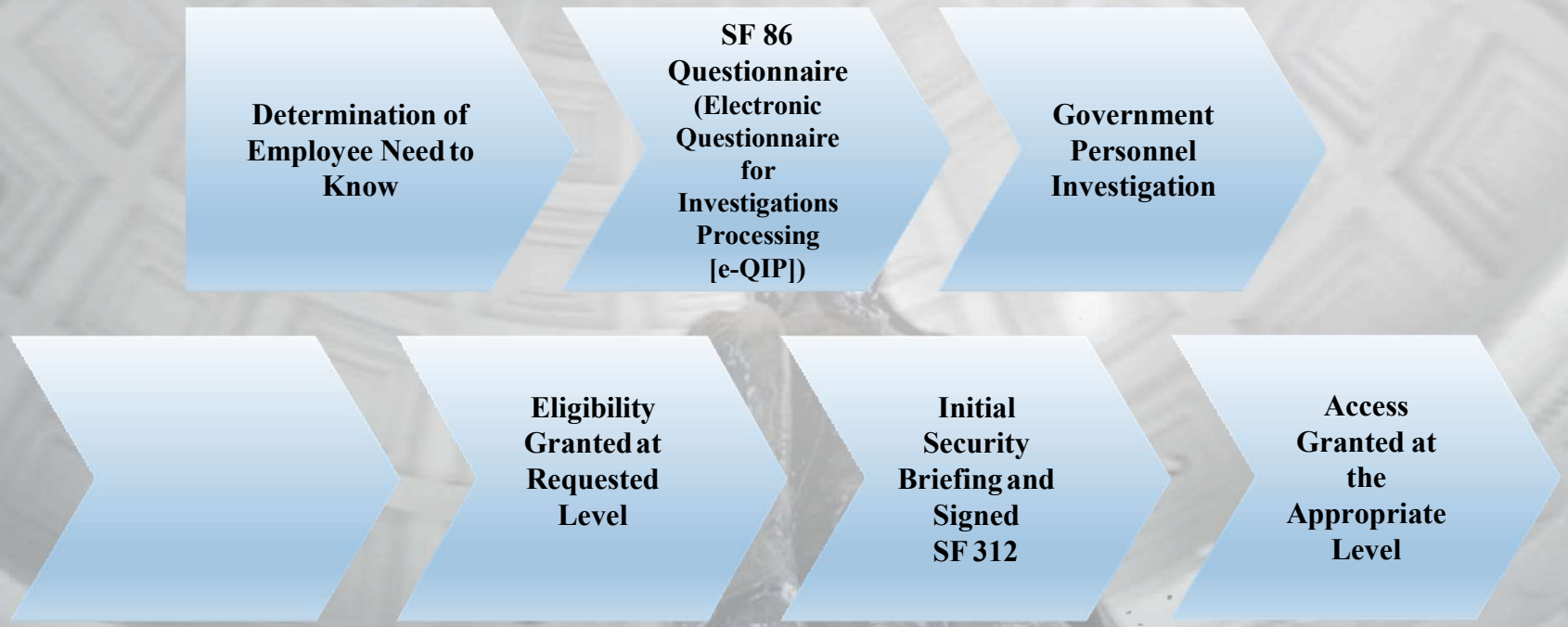
- Security violations
- adverse information

Reporting Obligations and Requirements

Security Infractions

- Leaving a safe containing classified material open and unattended.
- Allowing uncleared individuals to have access to classified material, either by viewing classified material or by conducting classified discussions in a non-secured area or over unapproved communication lines.
- Leaving classified material unattended.
- Removing classified material from a location without approval.
- Copying or destroying classified material without approval.
- Generating, viewing or processing classified material on a non-approved computer.

Personnel Security Clearance Process



Clearance Levels

There are three clearance levels:

- Top Secret
- Secret
- Confidential

Investigation levels:

- T5 for Top Secret and SCI eligibility
- T3 for Secret and Confidential eligibility
- T1, T2, and T4 are used for public trust determinations

Clearance Processing Times

- There are many variables involved in the security clearance process that affect timelines.
- Average time for a clearance varies from 9 months for a T3 up to 16 or more months for a T5

MYTH: SCI is high level security clearance.
FACT: SCI is an access level granted to individuals with a need-to-know to work with Classified National Intelligence.

SF 312 – Non-Disclosure Agreement (NDA)

- Special trust and confidence is granted to you by the U.S. Government.
- This agreement is life-binding.
- You are to protect classified information from unauthorized disclosure.
- Criminal and/or civil penalties may result from non-compliance (United States Code (USC), Title 18 and 50).
  - USC Title 18: https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-front&num=0&edition=prelim
  - USC Title 50: https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title50-front&num=0&edition=prelim
- The SF 312 must be signed with the appropriate security office BEFORE access to classified is granted.

Homeland Security Presidential Directive 12 (HSPD 12) Common Access Card (CAC)

- Employees may need badges to access certain government facilities and systems.
- Please make sure your security team is aware of each badge you have (This includes Common Access Cards (CAC), Base Access Passes, etc.).
- These cards contain personal identifying data and Public Key Infrastructure (PKI) certificates.
- Used for email encryption, digital signing, and network access.

VII

Hotline Numbers

- Federal agencies have hotlines for government and contractor employees to anonymously report (without fear of reprisal) known or suspected instances of serious security irregularities and infractions.

Always attempt to call the Security Team first!

- **Defense Hotline 800-424-9098**
- **NRC Hotline 800-695-7403**
- **DOE Hotline 800-541-1625**
- **FBI Hotline 202-324-3000**
- **CIA Hotline 703-874-2600**
- **DNI Hotline 703-733-8600**

VIII Job Specific Policies and Procedures

The following slides cover various security topics related to operations either here at this facility or at the customer site.

Operations Security (OPSEC)

- It is an analytic process used to deny an adversary information, generally unclassified, that deals with friendly intentions and capabilities by identifying, controlling, and protecting indicators associated with the planning processes or operations.
- OPSEC does not replace other security disciplines, it supplements them.
- OPSEC is simply denying an enemy information that could harm you and benefit them. OPSEC is both a process and a mindset. By educating yourself on OPSEC risks and methodologies, protecting sensitive information becomes instinct.

Operations Security (OPSEC)

OPSEC is a 5 Step Analytic Process:

1. Identification of Critical Information
2. Threat Analysis
3. Vulnerability Assessment
4. Risk Assessment
5. Application of Countermeasures

Operations Security (OPSEC)

Identification of Critical Information

- Basic to the OPSEC process is figuring out what information, if available to one or more adversaries, would harm an organization's capability to effectively carry out an operation or activity. This critical information constitutes the "core secrets" of the organization, i.e., the few pieces of information that are central to the organization's mission or the specific activity.

Threat Analysis

- It is important to determine who the enemies are and what information they would need to create damage.

Vulnerability Assessment

- Determining vulnerabilities involves analyzing how our operations and/or activities are conducted. Activities need to be looked at from the point-of-view of the enemy, which thereby provides the basis for understanding the true risks of how a unit or organization really operates.

Operations Security (OPSEC)

Risk Assessment

- Where vulnerabilities are great and the adversary threat is evident, the risk of enemy exploitation is expected. Therefore, a high priority for protection needs to be assigned and corrective action taken. Where the vulnerability is slight and the adversary has a low collection capability, the priority should be low.

Application of Countermeasures

- Countermeasures are developed to eliminate the vulnerabilities, threats, or utility of the information to the adversaries. Possible countermeasures should include alternatives that may vary in both effectiveness and feasibility.

Operations Security (OPSEC)

General Categories of Potential Critical Information That Needs to Be Protected (including but not limited to):

- Current and Future Strategic Plans
- Travel Itineraries
- Usernames and Passwords
- Access/ID Cards
- Operations and Financial Planning Information
- Personal Identifiable Information (PII)
- Capabilities and Weaknesses
- Address and Phone Lists
- Copyright/Intellectual Property/Proprietary Information
- Research and Development
- Contract/Proposal information

A Culture of Security

Each of us must analyze our own behavior; here are a few suggestions to exercise caution.

DON'T:

- Discuss future destinations
- Discuss future operations or missions
- Discuss dates and times of conducting an exercise
- Discuss readiness issues or numbers
- Discuss specific training equipment
- Discuss people's names and billets in conjunction with operations or programs
- Speculate about future operations

DO:

- Assume the enemy is trying to collect information that can cause harm to you or to National Security
- Be smart, and always think OPSEC when using email, phone, or any other medium of information transfer

Operations Security (OPSEC)

OPSEC Practices

- Remove ID badge when you leave your facility
- Do not post or send sensitive information over the web
- Guard against calls to obtain sensitive information
- Do not discuss sensitive information in public, or over the telephone
- Watch for and report suspicious activity

Security Control (SecCon) Software

- A self-service portal that will help maintain our company's compliance with the NISPOM.
- This portal will be required to be used by all cleared employees and/or consultants.
- The portal includes a reporting tool for all employees and consultants.
- This portal is your self-service center for all things related to security.
- This portal also includes access to:
  - All your security information
  - Points of contact for everyone in security
  - Copies of the NISPOM and all Industrial Security Letters issued by DCSA
  - Security Training, Standard Practice Procedures, Insider Threat Plan, and Security Newsletters

SECURITY CONTROL

Security Control (SecCon)

In this portal you can:

- View the status of both your security clearance and special accesses.
- Update/make changes to your employee profile (name, contact information, job title, etc.).
- Submit reports as required by both our company and NISPOM such as:
  - Upload/View your security documents such as:
    - Foreign Travel
    - Insider Threats
    - Adverse Information
    - Suspicious Contacts
    - Cyber Intrusions
    - Changes in your personal status (marital status, citizenship, etc.)
    - Training Certificates
    - SF 312/Non-Disclosure Agreement (NDA)
    - Special Access Briefings
    - Privacy Policies

This software will provide you with automated notifications when an action is required.
You are required to complete your security actions in order to maintain access to classified material.

IX Definitions

- **Access** - The ability or opportunity to obtain knowledge of national security information.
- **Classified Information** - Classified information is material that a government body claims is sensitive information that requires protection of confidentiality, integrity, or availability. Access is restricted by law or regulation to particular groups of people, and mishandling can incur criminal penalties and loss of respect.
- **Need-to-Know** - Need for access to specific classified information in order to perform or assist in both lawful and authorized government duties or contracts.
- **Authorized Person** - A person with an appropriate clearance level for access to classified information, has signed an approved non-disclosure agreement, and has a need-to-know.
- **Adverse Information** - Any information that adversely reflects on the integrity or character of a cleared employee that suggests that his or her ability to safeguard classified information may be impaired, that his or her access to classified information clearly may not be in the interest of national security, or that the individual constitutes as an Insider Threat.
- **Compromise** - Unauthorized disclosure of classified information.

IX Definitions

- **Controlled Unclassified Information (CUI)** - CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies. CUI is not classified information. It is not corporate intellectual property unless created for or included in requirements related to a government contract.
- **Classification guide** - A document, typically issued by a government agency that identifies the elements of information regarding a specific subject that must be classified and prescribes the level and duration of classification and appropriate declassification instructions. (Classification guides may be provided to contractors by the Contract Security Classification Specification, or equivalent.)
- **Document** - Any recorded information, regardless of the nature of the medium, or physical form or the method or circumstances of recording.
- **Security Violation** - Failure to comply with the policy and procedures established by this Manual [NISPOM] that reasonably could result in the loss or compromise of classified information.

X Conclusion

- You and your colleagues are the first line of defense against espionage and protection of our national security.
- Properly protecting classified information and reporting all suspicious behavior helps to protect our national security, our war fighters, our company, and your job.

Remember **…**

Having a government security clearance is a privilege, not a right. This privilege comes with a very high level of responsibility along with several requirements. If you aren't sure, don't be afraid to ask your FSO, AFSO, ITPSO or your supervisor.

2026 SECURITY TRAINING

CERTIFICATE OF COMPLETION

I certify that I have been provided and completed the following training classes in accordance with the National Industrial Security Program Operating Manual (NISPOM):

• 2026 Initial/Refresher Security Training	• 2026 Derivative Classification Training
• 2026 OPSEC Training	• 2026 Insider Threat Training

_____ , 2026

Print Name — Date

_____

Signature

Please sign, scan and send this certificate to your FSO.
If you do not have access, please email this certificate to: chinna@indexsystemsinc.com