Integrated Information Technology Solutions

Initial Security Orientation and Annual Awareness Training

Initial and annual security orientation and awareness training is required per 32 CFR 117 - NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPOM). As a cleared employee within the **Information Security Program**, you have the responsibility to protect Government assets, people and property, both classified and controlled unclassified, regardless of how it was obtained or what form it takes.

SEE SOMETHING, SAY SOMETHING

Agenda

- National Security Eligibility Process
- Information Security Program
- Pre-Publication Process
- Physical Security Program
- Operations Security (OPSEC) Program
- Security Executive Agent Directive 3 Reporting Requirements

Eligibility Process Phases

Whenever a DOW employee or contractor requires access to classified national security information in the performance of their duties, the individual must be granted national security eligibility at the proper level to access that information. National security eligibility is a favorable determination that affords an individual eligibility for access to classified information or assignment to a national security sensitive position. The National Security Eligibility Process is a four-phased approach that ensures the DOD does not grant access to national security information to people who cannot be trusted.

Personnel Security

The Personnel Security Program: This program provides security policies and procedures; establishes the standards, criteria, and guidelines that personnel security determinations are based upon.

Position Designations:

- Special-Sensitive: Access to Sensitive Compartmented Information (SCI)/Top Secret (TS) or Special Access Program (SAP). Potential for *inestimable damage* to National Security.
- Critical-Sensitive: Access to Top Secret (TS). Potential for *exceptionally grave damage* to National Security.
- Noncritical-Sensitive: Access to Secret or Confidential. Potential for *significant or serious damage* to National Security.
- Non-Sensitive: No eligibility required. Does not pose damage to National Security.

Investigation & Tiers

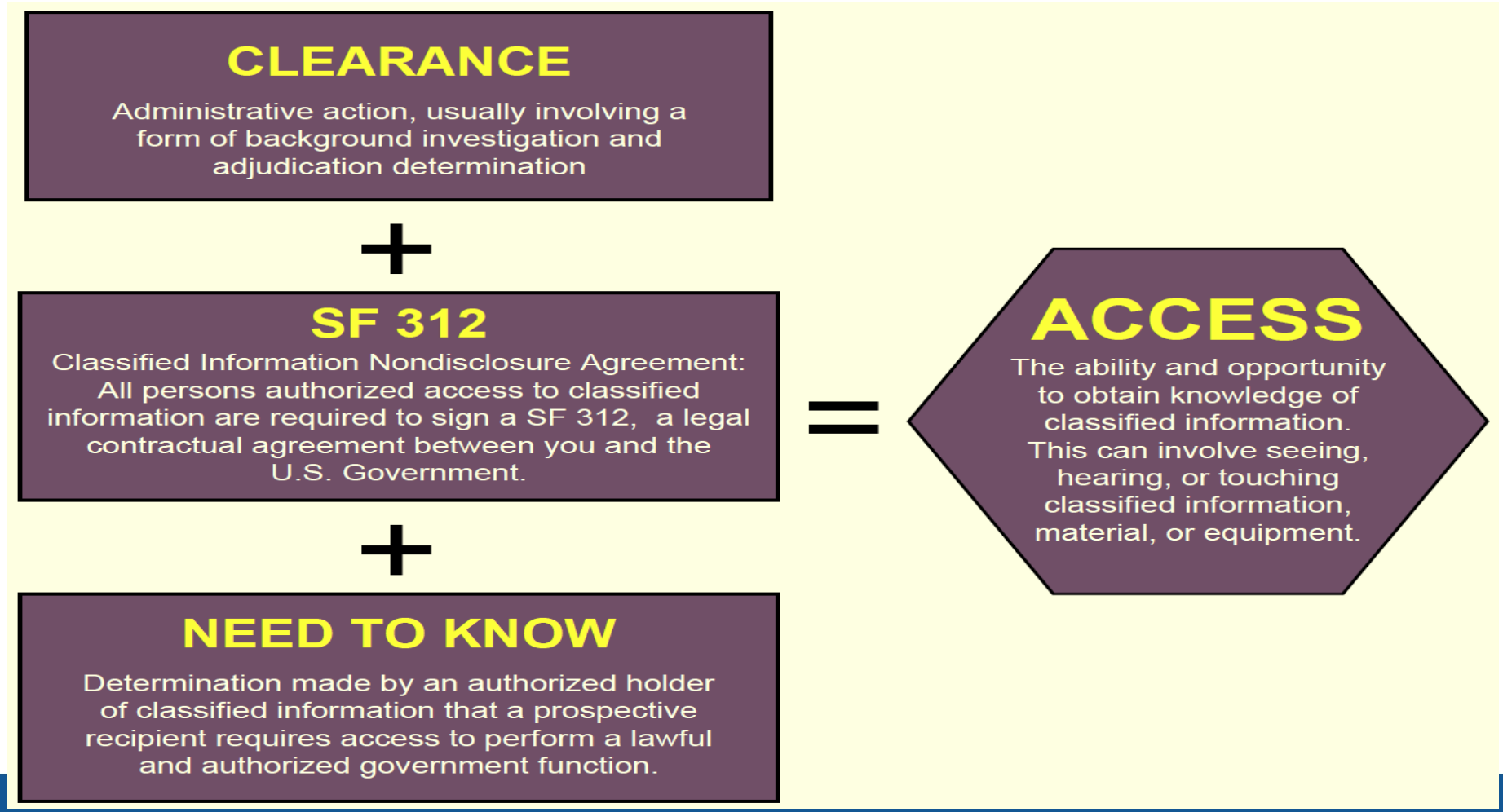
The Federal Investigative Standards (FIS) defines a **five**-tiered investigative model developed in accordance with Executive Order (EO) 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information". The FIS set standard requirements used to conduct background investigations which determine eligibility to access classified information or hold a national security sensitive position.

Clearance Eligibility Adjudication

DOD Consolidated Adjudications Facility (DOD CAF) is the primary authority for making security eligibility determinations for DOD personnel

- Utilizes whole person concept (looks at all available and reliable information about an individual's past and present prior to reaching an adjudicative determination)
- Uses 13 Adjudicative Guidelines

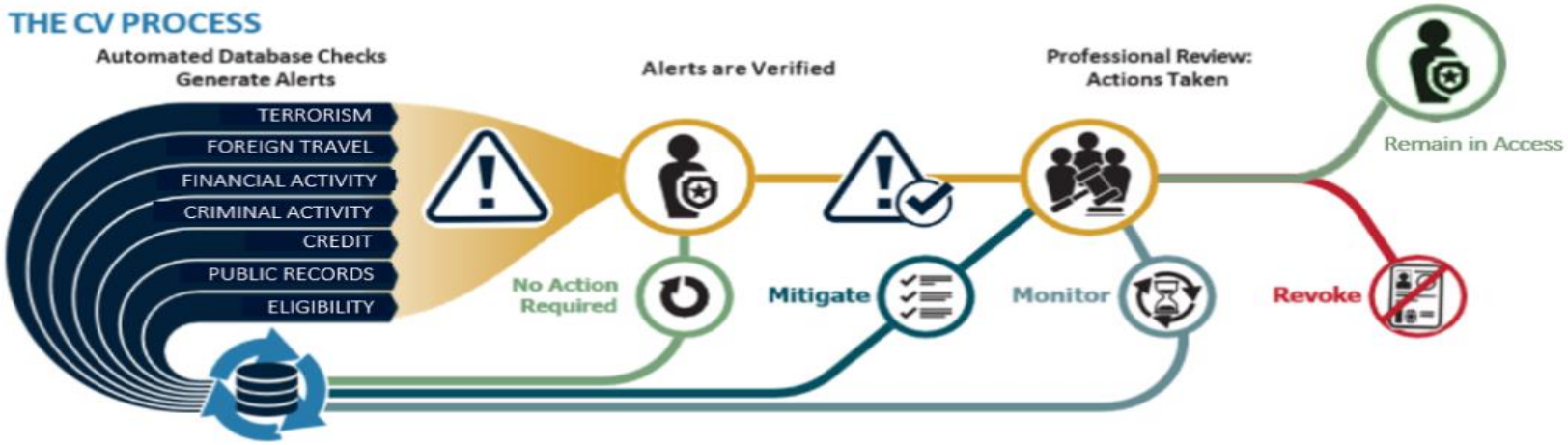
Personnel Security Adjudication



Access Equation

How does the Continuous Vetting (CV) process work?

Automated record checks pull data from criminal, terrorism, and financial databases, as well as public records, at any time during an individual's period of eligibility. When DCSA receives an alert, it assesses whether the alert is valid and worthy of further investigation. DCSA investigators and adjudicators then gather facts and make clearance determinations. CV helps DCSA mitigate personnel vetting situations before they become larger problems, either by working with the cleared individual to mitigate potential issues, or in some cases suspending or revoking clearances.



Continuous Vetting (CV)

Personnel Security Self-Reporting

IF YOU DON'T SELF REPORT, SOMEONE ELSE MIGHT.

Self-Reporting

Report changes in:

Status: Marriage, co-habitation, addition of new family member, divorce, receipt of large sum of cash

Adverse Information:

- Criminal activity (domestic violence, issuance of restraining order)
- DUI/DWI
- Traffic tickets over $300
- Excessive indebtedness, financial difficulties, bankruptcy
- Use of illegal drugs (Federal law supersedes State law)

Foreign Contacts and Foreign Travel

See The Security Executive Agent Directive 3 for more information.
Reporting does not automatically result in revocation of eligibility, so don't be afraid to report!

Information Security Program

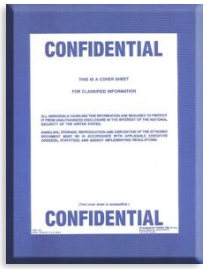
The IntegrITS Information Security Program (ISP) is a system of policies, procedures, and requirements established to protect classified and controlled unclassified information (CUI) that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to National Security.

Information Security Levels of Classified Information

All classified documents require a cover sheet. Classified media such as CDs, DVDs, hard drives, and thumb drives require medium tags or stickers.

Top Secret: Could cause exceptionally grave damage to national security that the Original Classification Authority (OCA) is able to identify or describe (SF703)

Secret: Could cause serious damage to national security that the OCA is able to identify or describe (SF704)



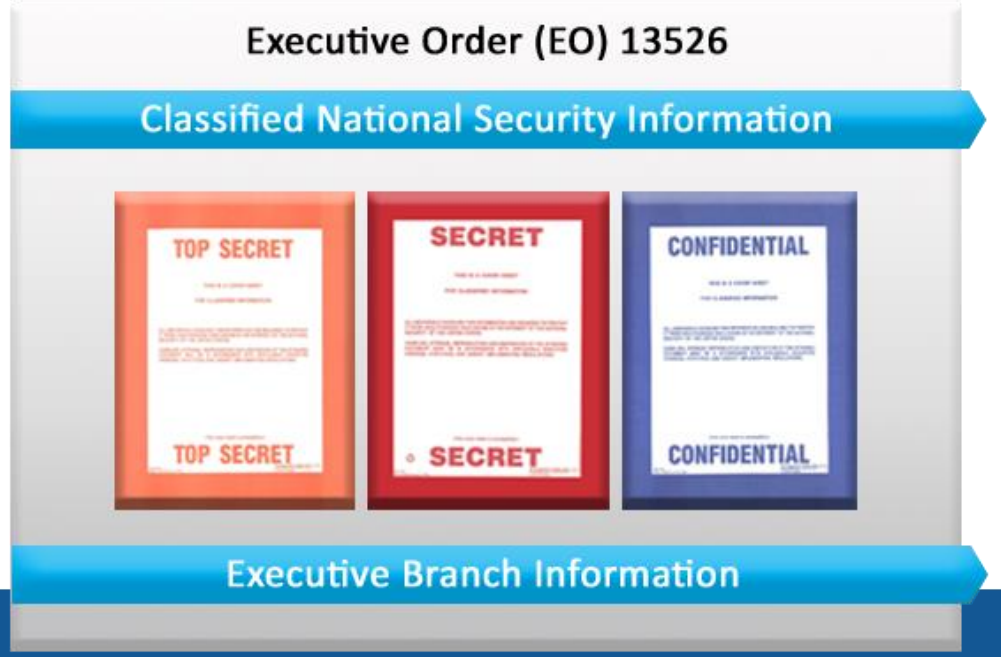
Confidential: Could cause damage to national security that the OCA is able to identify or describe (SF705)

ORIGINAL CLASSIFICATION: The initial government decision that an item of information could reasonably be expected to cause identifiable or describable damage to national security if subjected to unauthorized disclosure and requires protection in the interest of national security.

- Information may be originally classified only by the Secretary of Defense, the Secretaries of the Military Departments, and other officials to whom they delegate this authority in writing.
- Delegation of OCA shall be limited to the minimum number of officials required for effective operation of the Department of Defense (DOD).
- The authority shall be delegated to, and retained by, only those officials who have a demonstrable and continuing need to exercise it.

Information Security Original Classification

Top Secret, Secret, and Confidential may only be used to mark Executive Branch information that has been properly designated as classified national security information under Executive Order (EO) 13526. Information shall not be classified for any reason unrelated to the protection of national security.



Information Security Original Classification

DERIVATIVE CLASSIFICATION: Defined as incorporating, paraphrasing, restating, or generating in new form, information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information.

Derivative Classification Requirements

- Appropriate security eligibility
- Need-to-know
- Properly trained

Information Security Derivative Classification

Information Security Marking Syntax

Banner lines are at the top and bottom of the document and provide the overall classification of the document.

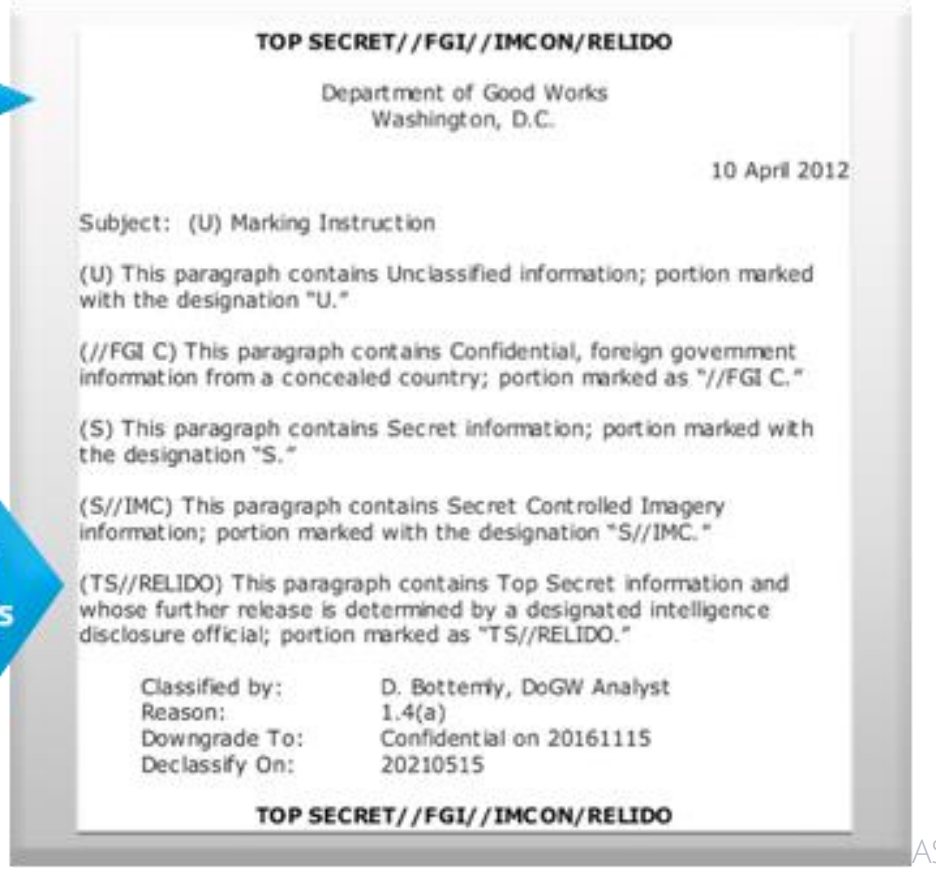
Portion markings denote the classification for each paragraph, sub-paragraph, or section in the document.

The Classification Authority Block (CAB) must include the name and position title or personal identifier of the DERIVATIVE classifier and, if not otherwise evident, the Component and office of origin, the source document or classification guide that the document was derived from, downgrade instructions if applicable, and the declassification date. The CAB must be on the face of the document.

Information Security Marking Syntax

Banner Line

Portion Markings



TOP SECRET//FGI//IMCON/RELIDO

Department of Good Works
Washington, D.C.

10 April 2012

Subject: (U) Marking Instruction

(U) This paragraph contains Unclassified information; portion marked with the designation "U."

(//FGI C) This paragraph contains Confidential, foreign government information from a concealed country; portion marked as "//FGI C."

(S) This paragraph contains Secret information; portion marked with the designation "S."

(S//IMC) This paragraph contains Secret Controlled Imagery information; portion marked with the designation "S//IMC."

(TS//RELIDO) This paragraph contains Top Secret information and whose further release is determined by a designated intelligence disclosure official; portion marked as "TS//RELIDO."

Classified by: D. Bottemly, DoGW Analyst
Reason: 1.4(a)
Downgrade To: Confidential on 20161115
Declassify On: 20210515

TOP SECRET//FGI//IMCON/RELIDO

Classification Markings are for Training Purposes Only

Classification by Compilation

Classification by compilation occurs when unclassified elements of information are combined to reveal classified information, or when classified elements are combined to reveal information at a higher classification level than the individual elements.

The portion markings will continue to be marked appropriately, but the overall classification marking will be at a higher level, along with a note at the bottom of the page that explains the document is classified by compilation.

Slide Presentations

- Mark first slide with overall classification marking
- Mark successive slides with either the overall classification or with the classification of the individual slide and portion markings for bullets
- Mark charts, graphics or figures by the classification of the portion, not of the chart/graphic/figure itself
- Classification authority block shall be placed on the first or last slide (less preferred)

Working Papers

- Mark with highest classification of any information contained in the document
- Date and annotate as “Working Papers”
- Destroy when no longer needed, remark within 180 days as a finished document or when released by the originator outside the originating activity

Information Security Marking Slides and Working Papers

Classified information shall be reproduced only to the extent required by operational necessity or for complying with applicable statutes or directives.

Reproduction Guidelines

- Use equipment approved at the appropriate level
- Ensure copies are subject to the same controls as original
- Limit reproduction to what is mission essential
- Ensure personnel are knowledgeable of the procedures for classified reproduction and aware of the associated risk involved with the specific reproduction equipment
- Comply with reproduction limitations
- Facilitate oversight and control

Additional Reproduction Guidelines

- At IntegrITS HQ – Authorization from the FSO is required prior to any classified information reproduction and review of current local procedures and specific equipment.
- Personnel aboard government/customer facilities and locations shall fully comply with local instructions and guidelines of that facility/site/location.

Information Security Reproduction

Rules for Processing Information: Use systems assessed or authorized to process information at the appropriate level.

Do Not

- Install software without approval
- Use another person's username and password
- Allow an unauthorized person to use your computer
- Circumvent or defeat security systems
- Permit unauthorized access to any sensitive computer network
- Modify or alter operating system configuration
- Write down your password

Additional Information Systems Process Guidelines

- At IntegrITS HQ – Authorization from the FSO is required prior to any classified information processing.
- Personnel aboard government/customer facilities and locations shall fully comply with local instructions and guidelines of that facility/site/location.

Information Security Processing Classified Information

CUI: Unclassified information associated with a law, regulation, or government-wide policy and identified as needing safeguarding. Unauthorized disclosure of CUI could cause foreseeable harm.

Examples of CUI

- Investigation documents
- Inspection reports
- Agency budgetary information
- Procurement bids/proposals
- Personally Identifiable Information (PII)
- Information protected under Privacy Act of 1974

CUI DOES NOT INCLUDE CLASSIFIED INFORMATION

Information Security Controlled Unclassified Information (CUI)

Information shall not be designated CUI to:

- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a person, organization, or agency
- Prevent open competition
- Control information not requiring protection under a law, regulation, or government-wide policy, unless approved by the CUI EA at the National Archives and Records Administration (NARA), through the Under Secretary of Defense for Intelligence and Security (USD(I&S))

Information Not Designated CUI

Safeguard Classified Information (During/After working hours)

- General Services Administration (GSA) approved containers / vaults
- Secure rooms
- Secure telephone
- Maintain control, never leave unattended
- Do not talk around using codes or hints
- Do not divulge to unauthorized persons

Safeguard CUI

- Locked cabinets, file cabinets, bookcases
- Rooms with locked outer office doors
- Key or cipher locked rooms
- Similarly secured areas
- Comply with local site instructions and policies

Information Security Safeguarding

Storage Containers

GSA Approved Containers: Required for storing all classified materials

Standard forms to be completed:

- **SF700: Security Container Information**
  - ✓ Record combinations to security containers, secure rooms, and controlled area doors and to identify personnel to be contacted in an emergency
- **SF701: Activity Security Checklist**
  - ✓ Must be completed after all areas have been secured
- **SF702: Security Container Checklist**
  - ✓ Record date and time when opening or closing security container

[Add additional guidance as required]

Preparing Classified Documents for Mailing

Checklist for Mailing Classified Information

- Cover sheet required; opaque envelopes
- Mark (INNER envelope only) with highest classification level of documents
- Mark INNER envelope with recipient and return address in case outer envelope is damaged
- Wrap and tape inner and outer envelope to mitigate tampering
- Obtain address for an official US Government activity or cleared DOD contractor facility
- Mark OUTER envelope with return and mailing address. NO PERSONAL NAMES should be annotated on the outer envelope.
- Complete a document receipt and destruction certificate (if needed)

Information Security
Top Secret Transmission

Transmit/Transport Top Secret/SCI

- Direct contact between cleared U.S. personnel
- Protected secure communication system (facsimile, data, e-mail voice)
- U.S. Transportation Command, Defense Courier Division
- Appropriately cleared U.S. Military, Government and DOD contractor

Comply with local site instructions and policies

- Do Not Send Via:
  - U.S. Postal Service
  - Overnight Express (FedEx)

Information Security Secret Transmission

Transmit/Transport Secret

- Any of the means approved for the transmission of Top Secret information
- Appropriately cleared contractor employees if applicable
- U.S. Postal Service registered mail or express within U.S. and Puerto Rico
    - Check “Signature is Required” box
- U.S. Postal Service registered mail through Army, Navy, or Air Force Postal Service outside the U.S. and territories
    - Information may not pass out of U.S. citizen control
- Commercial delivery for urgent, overnight delivery only
- Open incoming packages immediately and secure

Comply with local site instructions and policies

Information Security Confidential Transmission

Transmit/Transport Confidential

- Any of the means approved for the transmission of Secret information
- U.S. Postal Service certified mail to DOD contracting companies or non-DOD agencies
- U.S. Postal Service first class mail between DOD components in the U.S. and its territories
- Outer envelope marked “Return Service Requested”

DO NOT use external or street side mail collection boxes

Information Security
CUI Transmission

Transmit/Transport CUI

- U.S. Postal Service certified mail, parcel post, or fourth class mail
- Approved secure communications systems
- Avoid wireless telephone transmission of CUI when other options are available.
- Facsimile if appropriate protection is available at receiving location

Information Security Hand Carry

Hand Carry Requirements

- Prepare inventory of material (one copy for your office and another with a responsible person)
- Double wrap material (lockable briefcase or zippered pouch may serve as outer wrapping and approved for carrying classified material)
- Keep under constant control
- Deliver to authorized person ONLY
- Receive courier briefing
- Carry courier card
- Carry courier letter (if transporting via commercial air)
- Trips that involve overnight stopovers are NOT permitted unless arrangements for storage in a U.S. Government office or a cleared contractor facility have been previously made.

Information Security Destruction

Classified material shall be destroyed completely to prevent anyone from reconstructing the information. The preferred method of destruction is shredding by using a National Security Agency (NSA) approved shredder.

Other Means of Destroying Classified Material

- Burning
- Wet pulping
- Mutilation
- Chemical decomposition
- Pulverizing

Destruction of Record and non-record CUI

- Same methods as classified
- Other methods that would not allow recognition or reconstruction
- Ensure law, regulation, or government-wide policy doesn't specify a specific method of destruction

Security Incidents

A Security Incident can be categorized as an infraction or violation.

Infraction

- No loss or compromise of classified information
- Requires an inquiry to prevent a future violation but does not require an in-depth investigation

Violation

- Loss – information cannot be accounted for or physically located
- Compromise – Unauthorized disclosure of classified information to person(s) without valid clearance, authorized access or need to know.
- Negligent Discharge of Classified Information (NDCI) – the unauthorized disclosure of classified data on an information system not authorized for the appropriate security level access controls.

Report ALL infractions and violations immediately to your Security Officer

Examples of Incidents

Examples of Incidents

- Classified material not properly stored
- Classified container not properly secured
- Permitting personnel access to classified information without verifying need-to-know
- Failing to mark classified information
- Discussing classified information in unauthorized areas

For more information on security incidents refer to DODM 5200.01 Vol. 3 available in the resources.

Sanctions

You are subject to sanctions if you knowingly, willfully, negligently:

- Disclose classified or CUI to unauthorized persons
- Classify information or continuing the classification of information in violation of DOD regulations

Sanctions include:

- Warning
- Reprimand
- Loss/denial of classified access
- Suspension without pay
- Termination of employment
- Discharge from military service
- Criminal Prosecution

Classified Information in the Public Media

- Do not confirm or deny
- Do not respond to questions about programs or projects including those released through:
    - Radio or TV
    - Newspapers
    - Magazines
    - Trade journals
    - Social media sites, such as Facebook, Twitter, Pinterest, or LinkedIn
- Do not view or download from unclassified IT systems. Make a note of the URL and other significant details.

Refer all questions to the Public Affairs Office (PAO) and your Security Officer

Information Security Classified Information/Public Media

You are responsible for protecting official information and complying with the pre-publication process

Materials subject to pre-publication review include:

- Books, manuscript, or articles sent to the publisher, editor, movie producer, or game purveyor, or their respective support staffs
- Speech, briefing, article, or content that will be publicly disseminated
- Information being released to the public, even through Congress or the courts
- Official government products as well as materials submitted by cleared or formerly cleared personnel.
- See DoDI 5230.29 “Security and Policy Review of DoD Information for Public Release” for more information.

The Defense Office of Prepublication and Security Review (DOPSR) is responsible for reviewing materials for public and controlled release.

Pre-Publication Process

Industrial Security Program

Working with Contractors

- Contractors may or may not be cleared
  - Verify eligibility through a valid visit authorization request or system of record
  - Cleared under National Industrial Security Program (NISP)
  - Follow requirements of the National Industrial Security Program Operating Manual (NISPOM)
  - Required to comply with your organization's security program

Check with your security office for information on verifying contractor employee clearance eligibility and need to know.

Physical Security Program

Physical Security:

Active and passive measures to prevent unauthorized access to personnel, equipment, installations, and information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity.

Physical Security Countermeasures:

- Barriers/Fencing establish boundaries and deter individuals
- Intrusion Detection System (IDS) is used to deter, detect, document, deny, or delay intrusion by detecting a change in the environment.
- Security forces are made up of DOD, military, contract personnel, and trained dogs
- Lighting is used to deter intruders for fear of being seen

Physical Security Employee Identification

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

- DOD wide form of identification
- Used by civilians, contractors, and military personnel
- Contains personal identifying data and Public Key Infrastructure (PKI) certificate
- Used for email encryption, digital signing, and network access

If your CAC card is either lost or stolen, report it to your security office immediately.

Physical Security Escort Requirements

Escort Requirements

- Ensure all visitors sign the Visitor Log upon entry
- All visitors shall be escorted by employee
- Notify Facility Coordinator of maintenance/service providers requiring access

Operations Security (OPSEC)

OPSEC: Process of protecting critical information that can be used against us by preventing our adversaries access to information and actions that may compromise an operation.

OPSEC Practices:

- Remove ID badge when leaving your facility and secure it in a safe place
- Loss of any form of ID should be reported IMMEDIATELY to your security office
- 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 an UNCLASSIFIED phone line
- Watch for and report suspicious activity

Security Executive Agent Directive 3 (SEAD 3) Reporting Requirements

Individuals in the federal government and industry (contractors) with access to classified information or hold sensitive positions should be aware of established reporting requirements SEAD 3 implementations may vary for industry, DOD departments and agencies.

Reporting requirements for ALL covered individuals include Foreign Travel, Foreign Contacts and Reportable Actions by Others.

Foreign Travel

All industry personnel (contractors) with access to classified information or hold sensitive positions shall provide advance notice of foreign travel plans to their Security Office and receive approval prior to foreign travel.

Foreign Travel Requirements:

- Obtain defensive foreign travel security briefing prior to travel or at least once a year
- Obtain country specific briefing from the Counterintelligence Office (if required)
- Antiterrorism/Force Protection Level 1 training completion must be current
- Contact nearest U.S. Consulate, Defense Attaché, Embassy Regional Security Officer, or Post Duty Officer if detained or subjected to harassment or provocation

Foreign Travel SCI

SAP and/or SCI indoctrinated personnel planning foreign travel, personal or officially must follow the previous steps in addition to:

- Complete a foreign travel questionnaire prior to travel
- Provide complete copy of itinerary
- Be aware of nearest U.S. Consulate, Defense Attaché, Embassy Regional Security Officer, or Post Duty Officer
- Upon arrival from travel, complete return questionnaire

Foreign Contact Reporting

All industry personnel (contractors) with access to classified information or hold sensitive positions **must report foreign relationships to their Security Office.** SEAD 3 requires that all unofficial contacts be reported if the contact:

- Is Continuing
- Involves bonds of affection, personal obligation, or intimate contact
- Involves the exchange of personal information

This reporting requirement is based on the continuing association with the foreign national, regardless of whether the relationship has continued in person, online or via mail.

Reportable Contact By Others

SEE SOMETHING, SAY SOMETHING

All industry personnel (contractors) with access to classified information or hold sensitive positions should report any activity that raises doubt whether another employee's continued national security eligibility is clearly consistent with the interests of national security.

The following activities must also be reported:

- Unexplained affluence or excessive indebtedness
- An unwillingness to comply with rules and regulations
- Suspected mental health issues
- Illegal use of drugs
- Excessive alcohol consumption
- Criminal conduct

Summary

Now that you have completed this course, you should be familiar with the following:

- National Security Eligibility Process
- Information Security Program
- Pre-Publication Process
- Physical Security Program
- Operations Security (OPSEC) Program
- SEAD 3 Reporting Requirements

Next Steps

Integrated Information Technology Solutions

Please email Jim Lyon, FSO, confirming you have reviewed the Annual Training.