Initial NSI Orientation
Objectives

After completion of this training session, you will:

• Be familiar with the National Security Information (NSI) Program

• Understand the basic security clearance process

• Know how to identify and properly mark classified documents

• Understand the classification process

• Know the proper procedures to safeguard classified information

• Understand your roles and responsibilities

• Understand the SF 312 Nondisclosure Agreement
National Security Information Program

Directives

• Executive Order (EO) 13526 - Prescribes the system for classifying, safeguarding & declassifying NSI

• Information Security Oversight Office (ISOO) 32 C.F.R. Part 2001 - Sets forth guidance for NSI program

• EPA’s NSI Handbook – Incorporates and expands on the guidance from E.O. 13526 and ISOO 32 CFR 2001 for the agency. Official document for EPA employees (federal and non-federal) that outlines standards and procedures to be followed.

All references may be obtained on the NSI Program Intranet website
What is Classified Information?

Government information that, if subjected to unauthorized disclosure, could reasonably be expected to result in damage to the national security of the United States of America.
National Security Information Program

What type of information could be NSI?

a) Military plans, weapons systems, or operation

b) Foreign government information

c) Intelligence activities (including covert action), sources, methods or cryptology

d) Foreign relations or foreign activities of the United States

e) Scientific, technological, or economic matters relating to national security

f) United States programs for safeguarding nuclear materials or facilities

g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security

h) Development, production, or use of weapons of mass destruction
# Access to Classified Information

## Clearance Requirements

### Investigation
- Inquiry into your past to gather information to help determine whether you can be granted access to classified information
- Completed by an appropriate government authority
- Is not your “clearance”

### Adjudication
- Investigation reviewed by appropriately trained security personnel (adjudicators) to determine your eligibility for access (or award of a security clearance)
- Whole-person concept

### Continued Evaluation
- Based on continued need for access to classified information
- For Top Secret security clearances, marriage, same sex or opposite sex cohabitation must be reported. A spousal NAC is required on the Subject's spouse or cohabitant (same or opposite sex)
- Secret – Reinvestigation every 10 years
- Top Secret – Reinvestigation every 5 years

Trustworthy, Honest, Reliable, Loyal
Access to Classified Information

Access Requirements

**APPROPRIATE CLEARANCE LEVEL + NEED-TO-KNOW = ACCESS**

- Individuals are authorized access to classified information up to and including their level of clearance if they have a valid need-to-know

- No employee has a right to gain access to classified information solely by virtue of title, position, or level of security clearance
Classification Levels and Marking

Levels of Classified Information

**Top Secret**
Classified information that if disclosed to unauthorized individuals could cause “exceptionally grave damage” to national security

**Secret**
Classified information that if disclosed to unauthorized individuals could cause “serious damage” to national security

**Confidential**
Classified information that if disclosed to unauthorized individuals could cause “damage” to national security
Classification Markings

• Classification markings are a requirement

• Markings leave no doubt about:
  - The classification level of the information
  - The level of protection required
  - The duration of classification

• Classification markings include:
  - Overall page markings
  - Classification authority
  - Declassification instructions
  - Paragraph/portion markings
1. (U) This picture shows individuals what a portion marking looks like.

2. (C) A portion marking shall always precede the text within a paragraph.

3. (S) Other agencies may put their portion markings at the end of the paragraphs; however, this is not the policy of the EPA.

Classified by: Gina McCarthy, EPA Administrator
Reason: 1.4(g)
Declassify on: July 15, 2022
Memorandum
From:
To:
Subject: (U) Water Tables of the U.S.

1. (S) This picture shows individuals what a portion marking looks like.

2. (U) A portion marking should always precede the text within a paragraph

3. (S) Other agencies may put their portion markings at the end of the paragraphs; however, this is not the policy of the EPA.

Classified by: Lisa Jackson, Administrator, EPA
Reason: 1.4(a) and (d)
Declassify on: July 15, 2022

For training purposes only
Understanding the Classification Process

- **Original Classification**
  - The initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure. Original classification is only authorized by the EPA Administrator.

- **Classification Guide**
  - Document identifying the elements of information regarding a specific subject(s) that must be classified and establishing the level and duration of classification for each such element. The classification guide also serves as a declassification guide.

- **Derivative Classification**
  - 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.
Understanding the Classification Process

- **Declassification**
  - The determination that information contained in a classified document no longer requires classification and may be released and/or disseminated openly.

- **Over-Classification**
  - The application of a higher level of classification (original or derivative) to a document than is authorized or appropriate based on the source information or potential for damage to the national security of the United States.
  - Whenever there is a doubt as to the classification of a document, the lower classification shall be applied to avoid possible over classification.

- **Change in Classification**
  - The determination that an originally classified document is required to remain classified but the damage caused by release to an unauthorized individual is higher or lower than when the document was originally classified, requiring a change in the overall classification level.
Understanding the Classification Process

EPA Cleared Personnel

• Challenging Classification
  - As a clearance holder, you can challenge a document’s classification status if you believe it to be improper
  - Must be in writing explaining why the information is or is not classified at a certain level
  - Promotes proper and thoughtful classification actions
  - Non-retribution for presenting a challenge
  - Submit to the Original Classification Authority through NSI Representative and NSI Program Team
Safeguarding Classified Information

Secure Areas

- Classified information must be reviewed, handled, stored, discussed, and processed in accredited areas
  - Types of accredited areas:
    - Secure area (Closed storage)
    - Open storage area
  - Accreditation process:
    - Request is sent to the NSI
- An orientation of the secure area will include a discussion of:
  - Standard operating procedures
  - Uncleared personnel in secure area
    - Procedures for ensuring only cleared employees access classified information
    - Procedures preventing unauthorized disclosure
    - Escort procedures
  - Protection and storage of classified information and material
Safeguarding Classified Information

Storage – Security Container

**Lock combinations**
- Memorize – combinations recorded using SF 700
- Same level of classification as the approved contents of the security container
- Given only to those who need-to-know
- Change combination
  - New container
  - Someone no longer requires access
  - When compromised

**Container requirements**
- GSA approved
- Type 5 or 6 (Letter or Legal)
- X-07 or X-09 lock
Fill it out each time the container is:

- Unlocked
- Locked
- End of day check

The SF 702 should be retained for three months after it has been completely filled out. After the three month period, the SF 702 can be destroyed.
Safeguarding Classified Information

Drawer Inventory Log

- The Drawer Inventory Log is used to inventory the contents of a security container.

- The person responsible for the security container must ensure an accurate inventory for each drawer containing classified material is maintained and updated.
Safeguarding Classified Information

Storage – Activity Security Checklist (SF 701)

- End of Day Security Check
  - Check the entire work area for classified material
  - Check the security container to ensure that it is locked
  - Record the end of day check on SF 701 (Activity Security Checklist)
Safeguarding Classified Information

Transmission - Secure Communications

- Only discuss classified information over an approved secure phone - Secure Terminal Equipment (STE)

- Can only be conducted in appropriately accredited areas

- Use requires Crypto Card to operate the STE in a classified mode

- Remove and properly store the card
Safeguarding Classified Information

Processing – Classified Information Systems

- Process classified information only on designated computers

- Systems will be clearly marked to indicate the level of information that can be processed

- Media will be clearly marked to indicate the level of information contained on them
Safeguarding Classified Information

Packaging Procedures

1. Inner Package
2. Outer Package

NOTE: Ensure addressee’s name is located on inner and outer envelopes.
Safeguarding Classified Information

Transmission – Mailing

Top Secret
- Transmit by direct contact between authorized persons
- Transmit by an authorized government service or escort with a Top Secret clearance
- Transmit via electronic means over an approved secure communications system
- Do not transmit via U.S. Postal Service

Secret
- Any method established by Top Secret
- GSA approved commercial delivery services (i.e. FedEx)
- U.S. Postal Service Priority Express Mail
- A signature is required

Confidential
- Any method established by Secret authorized mailing
- U.S. Postal Service Certified Mail
- U.S. First Class Mail (when sent to a U.S. Government facility)
- Do not transmit to government contractor facilities via U.S. First Class mail
Transporting – The Courier Program

• NOT everyone is authorized to hand carry classified information outside of EPA workspaces

• The EPA Courier Program authorizes designated, cleared and trained individuals to transport NSI up to the authorized clearance level on their courier card

• Must be designated for EPA Courier Program by Manager. Courier training is required prior to transporting classified information outside of EPA controlled space
Safeguarding Classified Information

Reproduction and Destruction

- Any copier used for reproduction of classified information must be authorized by the NSI Program Team or the NSI Representative and located in an accredited space.

- Reproduction of classified information must be limited to the amount needed for operational purposes.

- Shredding is the only approved method for destroying classified information and requires two person integrity for Top Secret material.
Roles and Responsibilities

EPA Key Management

**Administrator, Environmental Protection Agency**
- Original Classification Authority
- Responsible for successful implementation of the NSI program

**Assistant Administrator, OARM**
- Designated Senior Agency Official
- Responsible for ensuring that EPA’s NSI program is in compliance with E.O. 13526

**Director, OA**
- Oversees the direction and management of EPA’s Security Management Division

**Director, Security Management Division**
- Focal point for all EPA security matters
OARM’s NSI Program Team

Responsible for developing and implementing EPA’s NSI policies, procedures, guidelines, and security training and education programs

National Security Information Handbook

NSI Representatives

Responsible for implementation and management of NSI Program in assigned area, all aspects of classified information handling and processing, and also for formulating/issuing local standard operating procedures
 Roles and Responsibilities

EPA Cleared Personnel

• It’s your responsibility to:
  - Comply with security regulations
  - Limit access (prevent unauthorized disclosure)
  - Complete annual security refresher training
  - Report security incidents immediately or within 24 hours to your supervisor, NSI Representative or NSI Program Team
  - For Top Secret security clearances, report changes in marital status, same sex and opposite sex cohabitation. A spousal NAC is required on the Subject's spouse or cohabitant (same or opposite sex). Contact PSB on (202) 564-7912 for additional information
  - Notify the NSI Program Team if duties change in current position, you are promoted, you change positions or you go on a detail inside or outside EPA. A new justification may be required to maintain your security clearance
All employees with security clearances must have their duties included in their PARS.

- The mandatory element addresses the ongoing responsibility to safeguard and protect classified information regardless of how frequently the clearance holder accesses or handles classified information.
- Employees who choose not to include the critical element in their PARS will have their clearance administratively withdrawn.
General Schedule Critical Element for Agency Security Clearance Holders

- **Critical Element**: Results Driven (Accountability)
  - **Strategic Plan elements supported by this CE**: This work is an enabling and support function that supports the outcome of the agency’s strategic goals (1, 2, 3, 4, and 5).

- Compliance with Policies and Standards Related to National Security Information (Agency Security Clearance Holders). Complies with all applicable personnel security and National Security Information requirements. Safeguards and protects classified information in the manner prescribed by regulation, directive and agency guidelines. Reports incidents involving the improper handling or unauthorized or inadvertent disclosure of classified information and violations of the security regulations.
General Schedule Critical Element for Agency Security Clearance Holders

- **Critical Element**: Results Driven (Accountability)
  - **Strategic Plan elements supported by this CE**: This work is an enabling and support function that supports the outcome of the agency’s strategic goals (1, 2, 3, 4, and 5).

- Compliance with Policies and Standards Related to National Security Information (Agency Security Clearance Holders). Complies with all applicable personnel security and National Security Information requirements. Safeguards and protects classified information in the manner prescribed by regulation, directive and agency guidelines. Reports incidents involving the improper handling or unauthorized or inadvertent disclosure of classified information and violations of the security regulations.
Roles and Responsibilities

EPA Cleared Personnel

**Violations**
- Knowingly disclosing classified information to unauthorized persons
- Loss, compromise, or suspected compromise of classified information
- Purposefully violating security regulations

**Infractions**
- Unintentional violation of security regulations
- Does not involve the loss, compromise, or suspected compromise of classified information
- Infractions are documented and kept on file

**Preliminary Inquiry**

**Administrative Sanctions**
- The severity of any sanction for a violation or infraction is based on:
  - The seriousness of the violation or infraction; the number of previous violations or infractions; the time span between violations

- Typical administrative actions are as follows:
  - Written or oral admonition; suspension; revocation of access; termination of employment or affiliation; imprisonment or fined

- The imposition of administrative action does not prohibit or limit action under civil or criminal statutes
The primary purpose of the SF 312 is to inform the employee of:

- Responsibilities to protect information
- Consequences of unauthorized or negligent handling
Revision of the SF 312

Paragraph 10 on the SF 312 has been revised due to statutory requirements. The following is a list of “Executive Orders and statutory provisions,” which are controlling in the case of any conflict with an agency’s NDA:

• Executive Order No. 13526;
• Section 7211 of Title 5, United States Code (governing disclosures to Congress);
• Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military);
• Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act of 1989 (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats);
• Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents);
• The statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, and 952 of title 18, United States Code; and
• Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)).
AN AGREEMENT BETWEEN

[Name of Individual - Print or type]

AND THE UNITED STATES

(Remainder of agreement text printed, but obfuscated due to nature of content.)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of the granting of access to classified information. As used in this Agreement, classified information is marked or unmarked classified information including oral communications. This is classified in accordance with the standards of Executive Order 13526, or under any other Executive order or statute that prohibits the unauthorized disclosure of information about the national security and causes such information to be classified.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information including the procedures to be followed in associating those persons to whom I will disclose this information who have been approved for access to it, and that I understand these procedures.

3. I have been advised that all authorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or adverse injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will not divulge classified information to anyone unless (a) I have officially verified that the recipient has been properly authorized by the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted; (b) I am responsible for confirming that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b) above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearance I hold, removal from any position of special confidence and trust requiring such clearance, or termination of my employment or other relationship with the Department or Agency that granted me my security clearance or clearance. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation or violation of United States criminal laws, including the provisions of sections 641, 703, 704, 708, 1022 and 1024, title 18, United States Code, "the provisions of section 703(b), title 50 United States Code, and the provisions of the Intelligence Identities Protection Act of 1976. I recognize that nothing in this Agreement creates a waiver by the United States Government from the rights of a third party or from any judgment of a court which may determine that any restriction contained in this Agreement is not valid.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce the Agreement, including, but not limited to, application for a court order precluding disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is new and will not be destroyed or returned to the United States Government until such time as authorized by an authorized official or by final ruling of a court of law. I understand that I may not disclose classified information to another person unless I am responsible for the protection of that information.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that the United States Government may, at any time, request or require the return of any classified information.

9. Each provision of this Agreement is severable. If any court should find any provision of this Agreement to be unenforceable, other provisions of this Agreement shall remain in full force and effect.

10. These provisions are consistent with and do not supersede, conflict with, or otherwise infringe or violate the obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, communications to Congress, (2) the reporting to an Inspector General of a violation of any law, rule, or regulation, or management, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (3) any other whistleblower protection. The definitions, rights, obligations, and liabilities created by existing statute or Executive order are incorporated into this Agreement and are controlling.
Questions

The NSI Program Team at EPA Headquarters is always available for questions, comments, or concerns.

- Phone: 202-564-1983
- Fax: 202-565-2028
- Email: NSI_ProgramTeam@epa.gov
- Intranet Web: http://intranet.epa.gov/oaintran/smd/nationalsec.htm