



# National Security Information Program

## **Initial NSI Orientation**

December 13, 2013



# Objectives

---

After completion of this training session, you will:

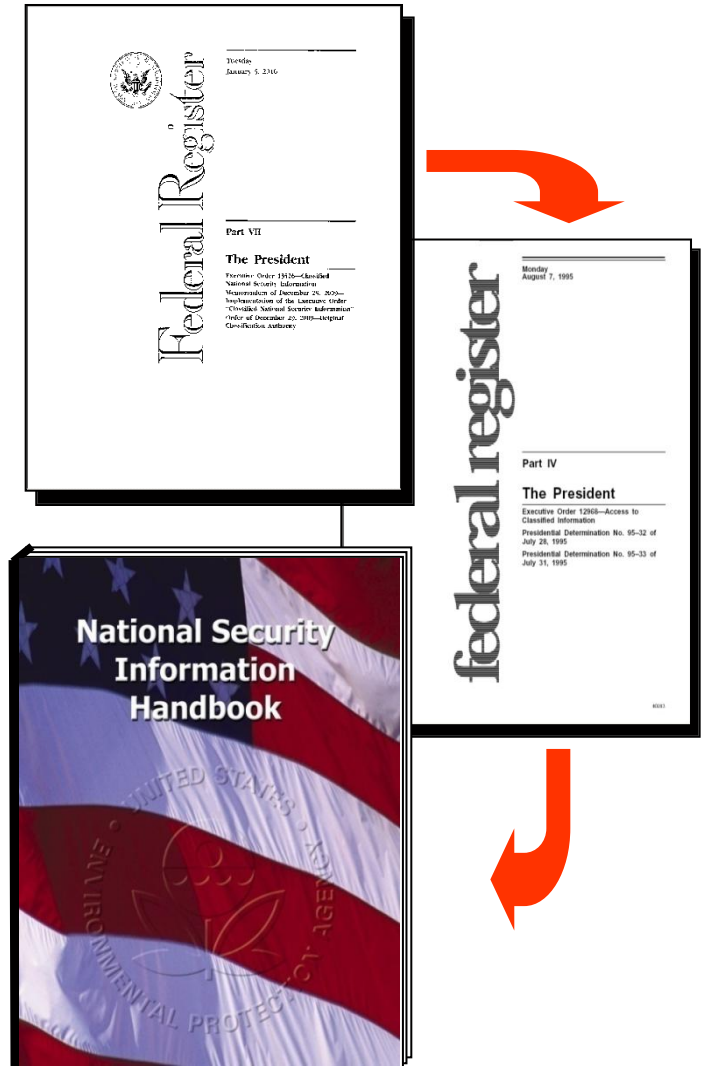
- Be familiar with the National Security Information (NSI) Program
- Understand the basic security clearance process
- Know how to identify and properly mark classified documents
- Understand the classification process
- Know the proper procedures to safeguard classified information
- Understand your 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



# National Security Information Program

---

## 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





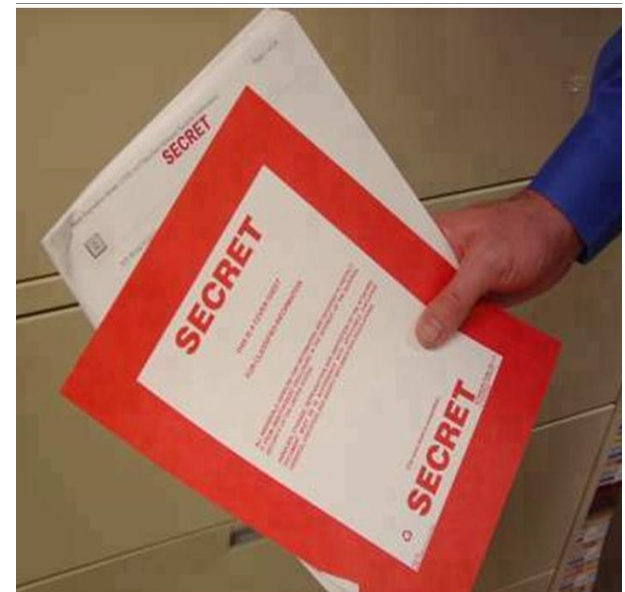


# Classification Levels and Marking

---

## 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





# Classification Levels and Marking

## Classification Markings



**SECRET**

July 15, 2012

**Environmental  
Protection Agency**

**(U) Special Report  
ANX-128**

Classified by: Gina McCarthy, EPA Administrator  
Reason: 1.4(g)  
Declassify on: July 15, 2022

**SECRET**  
For training purposes only

**SECRET**

July 15, 2012

Subject: **(U)** Special Report ANX-128

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.

**SECRET**  
For training purposes only



# Classification Levels and Marking

## Derivative Classification

**SECRET**

Memorandum July 15, 2012

From:  
To:

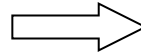
Subject: (U) Water Tables of the U.S.

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

**SECRET**  
For training purposes only

**Source Document**



**SECRET**

Memorandum July 15, 2012

From:  
To:

Subject: (U) Water Amount used in 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: John Smith, Research Specialist, NHSRC  
Derived From: Memo, (U) "Water Tables of the U.S."  
July 15, 2022  
Declassify On: July 15 2022

**SECRET**  
For training purposes only

**Derivative Document**

# 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





# Safeguarding Classified Information

## Storage Container Check Sheet (SF 702)

SECURITY CONTAINER CHECK SHEET								
TO (if required)				THRU (if required)				
CERTIFICATION								
I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.								
MONTH/YEAR								
DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME
6/6	VV	930	VV	935	AW	500		



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

 United States Environmental Protection Agency Washington, DC 20460				Container Number Office/Room Number	
Drawer Inventory Log					
Control Number / Date of Receipt	Copy Number / Date of Material	Media Type	Item Description (unclassified title, # of pages, originator)	Point of Contact	Destroyed / Transferred
Control Number:	Copy Number:	<input type="checkbox"/> Paper <input type="checkbox"/> Diskette <input type="checkbox"/> CD <input type="checkbox"/> Hard Drive <input type="checkbox"/> Other		Name:	<input type="checkbox"/> Destroyed <input type="checkbox"/> Transferred
Date of Receipt:	Date of Material:	Class Level: <input type="checkbox"/> TS <input type="checkbox"/> S <input type="checkbox"/> C <input type="checkbox"/> SCI		Phone:	Date:
Control Number:	Copy Number:	<input type="checkbox"/> Paper <input type="checkbox"/> Diskette <input type="checkbox"/> CD <input type="checkbox"/> Hard Drive <input type="checkbox"/> Other		Name:	<input type="checkbox"/> Destroyed <input type="checkbox"/> Transferred
Date of Receipt:	Date of Material:	Class Level: <input type="checkbox"/> TS <input type="checkbox"/> S <input type="checkbox"/> C <input type="checkbox"/> SCI		Phone:	Date:
Control Number:	Copy Number:	<input type="checkbox"/> Paper <input type="checkbox"/> Diskette <input type="checkbox"/> CD <input type="checkbox"/> Hard Drive <input type="checkbox"/> Other		Name:	<input type="checkbox"/> Destroyed <input type="checkbox"/> Transferred
Date of Receipt:	Date of Material:	Class Level: <input type="checkbox"/> TS <input type="checkbox"/> S <input type="checkbox"/> C <input type="checkbox"/> SCI		Phone:	Date:
Control Number:	Copy Number:	<input type="checkbox"/> Paper <input type="checkbox"/> Diskette <input type="checkbox"/> CD <input type="checkbox"/> Hard Drive <input type="checkbox"/> Other		Name:	<input type="checkbox"/> Destroyed <input type="checkbox"/> Transferred
Date of Receipt:	Date of Material:	Class Level: <input type="checkbox"/> TS <input type="checkbox"/> S <input type="checkbox"/> C <input type="checkbox"/> SCI		Phone:	Date:
Control Number:	Copy Number:	<input type="checkbox"/> Paper <input type="checkbox"/> Diskette <input type="checkbox"/> CD <input type="checkbox"/> Hard Drive <input type="checkbox"/> Other		Name:	<input type="checkbox"/> Destroyed <input type="checkbox"/> Transferred
Date of Receipt:	Date of Material:	Class Level: <input type="checkbox"/> TS <input type="checkbox"/> S <input type="checkbox"/> C <input type="checkbox"/> SCI		Phone:	Date:
Control Number:	Copy Number:	<input type="checkbox"/> Paper <input type="checkbox"/> Diskette <input type="checkbox"/> CD <input type="checkbox"/> Hard Drive <input type="checkbox"/> Other		Name:	<input type="checkbox"/> Destroyed <input type="checkbox"/> Transferred
Date of Receipt:	Date of Material:	Class Level: <input type="checkbox"/> TS <input type="checkbox"/> S <input type="checkbox"/> C <input type="checkbox"/> SCI		Phone:	Date:





# 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

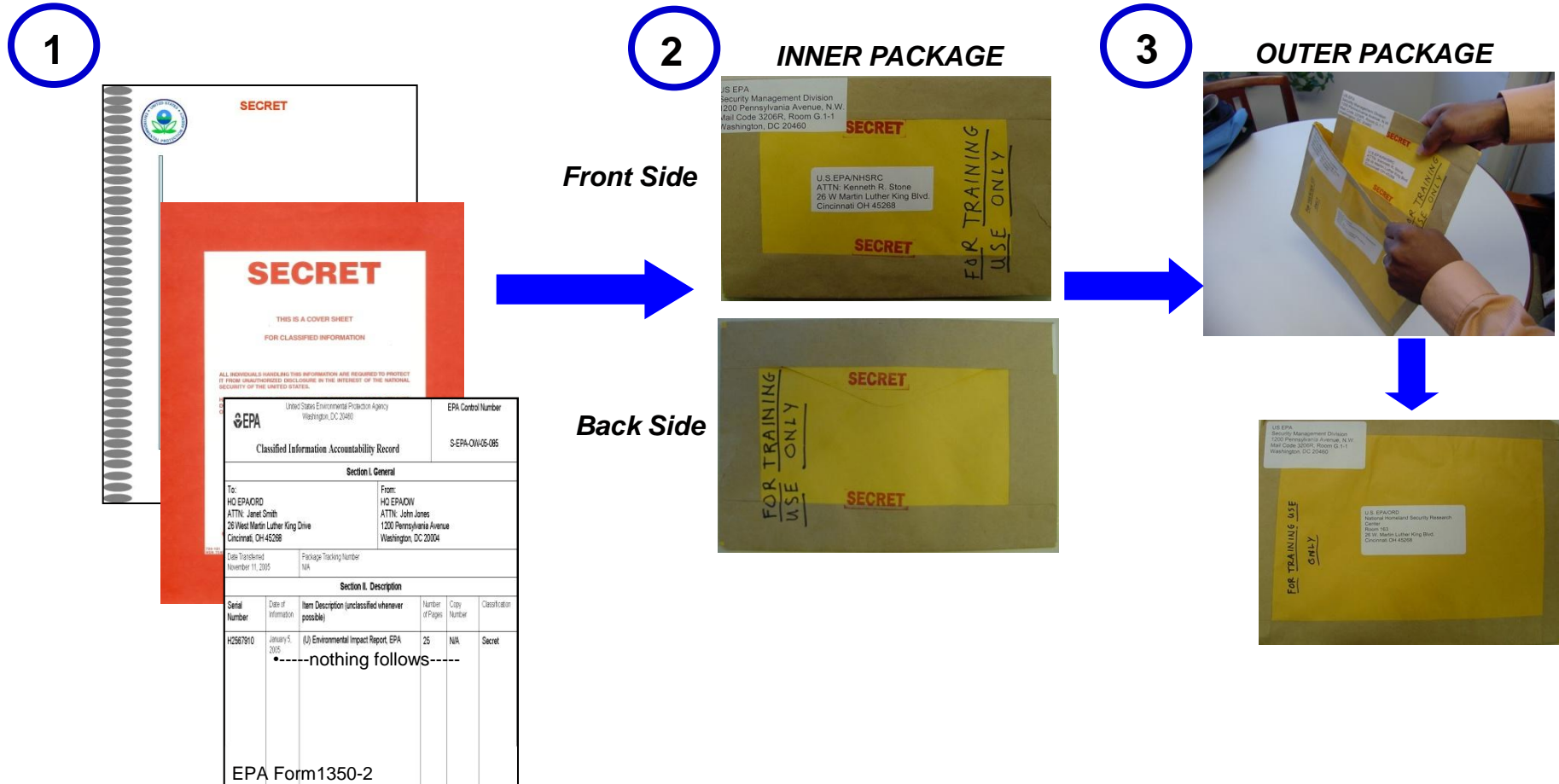
- Process classified information only on designated computers
- Systems will be clearly marked to indicate the level of information that can be processed
- Media will be clearly marked to indicate the level of information contained on them





# Safeguarding Classified Information

## Packaging Procedures



**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



# Safeguarding Classified Information

---

## 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

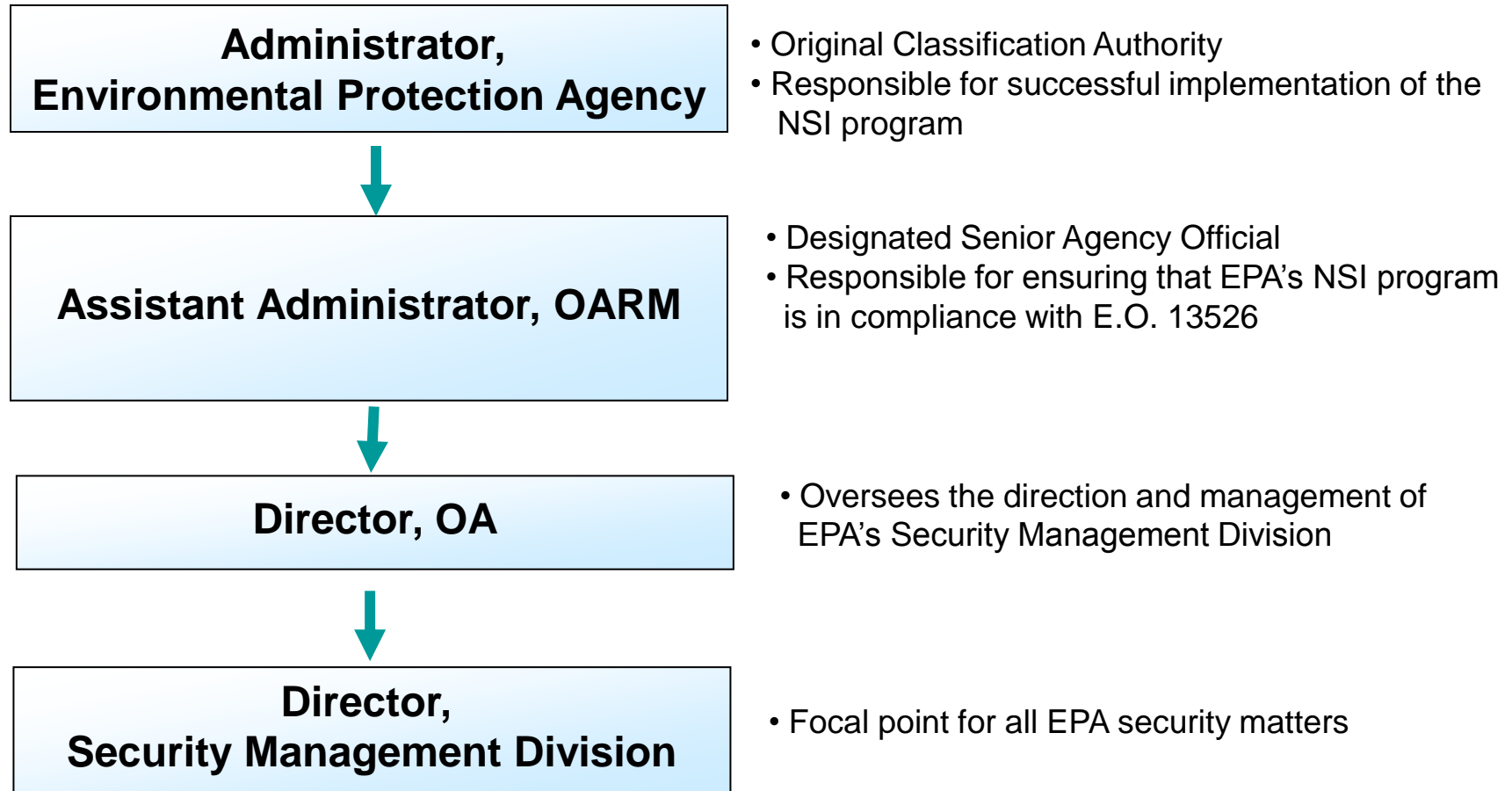




# Roles and Responsibilities

---

## EPA Key Management

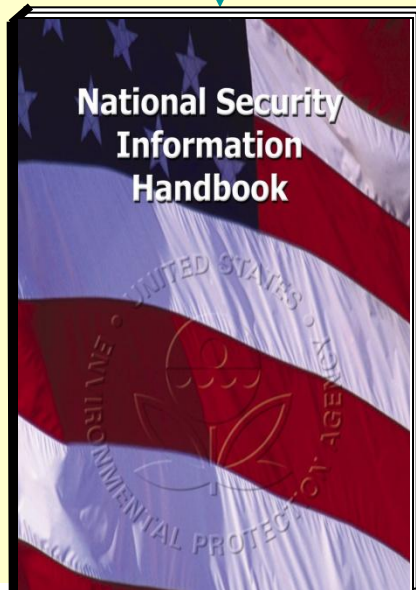




# Roles and Responsibilities

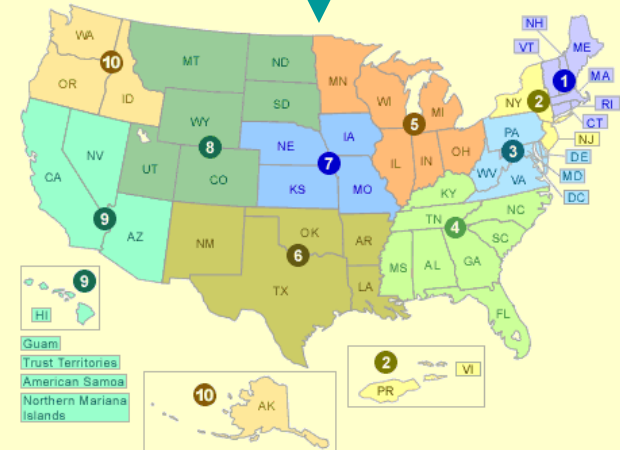
## OARM's NSI Program Team

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



## 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



# Performance Appraisal and Recognition System

---

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.



# PARS for Senior Executive Service Employees

---

## 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.



# PARS For General Schedule Employees

---

## 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

**Preliminary Inquiry**

### *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

### *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





# SF 312 Nondisclosure Agreement

---

- 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)).

# SF 312 Nondisclosure Agreement



## CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN [REDACTED] AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 13526, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 13526, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

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 ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from 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. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official 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 clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of sections 641, 793, 794, 798, \*952 and 1924, title 18, United States Code; the provisions of section 783(b), title 50, United States Code; and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

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 this Agreement including, but not limited to, application for a court order prohibiting 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 now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of sections 793 and/or 1924, title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all 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 alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

(Continue on reverse.)

NSN 7540-01-280-5499  
Previous edition not usable.

STANDARD FORM 312 (Rev. 7-2013)  
Prescribed by ODNI  
32 CFR PART 2001.80 E.O. 13526

11. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 13526 (75 Fed. Reg. 707), or any successor thereto 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); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); sections 7(c) and 8H of the Inspector General Act of 1978 (5 U.S.C. App.) (relating to disclosures to an inspector general, the inspectors general of the Intelligence Community, and Congress); section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 403-3h)(g)(3) (relating to disclosures to the inspector general of the Intelligence Community); sections 17(d)(5) and 17(e)(3) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403g(d)(5) and 403q(e)(3)) (relating to disclosures to the Inspector General of the Central Intelligence Agency and Congress); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, \*952 and 1924 of title 18, United States Code, and \*section 4 (b) of the Subversive Activities Control Act of 1950 (50 U.S.C. section 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

12. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Part 2001, section 2001.80(d)(2)) so that I may read them at this time, if I so choose.

\* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

SIGNATURE [REDACTED]	DATE [REDACTED]	SOCIAL SECURITY NUMBER (See Notice below) [REDACTED]
-------------------------	--------------------	---

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)  
[REDACTED]

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS (Type or print)		NAME AND ADDRESS (Type or print)	

### SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Public Law 104-134 (April 26, 1996). Your SSN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above or to determine that your access to the information indicated has been terminated. Furnishing your Social Security Number, as well as other data, is voluntary, but failure to do so may delay or prevent you being granted access to classified information.

STANDARD FORM 312 BACK (Rev. 7-2013)



# 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](mailto:NSI_ProgramTeam@epa.gov)
- Intranet Web: <http://intranet.epa.gov/oaintran/smd/nationalsec.htm>