

# Welcome to the CNS Annual Security Refresher Briefing

## **Motivator:**

Congratulations! You have been granted a Department of Energy (DOE) security clearance! DOE requires the completion of a annual security briefing upon receipt of a security clearance and before receiving initial access to classified information or matter, or special nuclear material (SNM).

As a cleared individual that has been granted a security clearance, it is important that you are reminded of your security responsibilities. The annual security refresher briefing's intent is to remind you of those responsibilities.

## **Terminal Objective:**

Upon completion of this course, attendees will identify basic classification policies and procedures, classified information or matter protection elements, personnel security elements and counterintelligence reporting requirements at Y-12 and Pantex as outlined in this annual security briefing.

# BASIC CLASSIFICATION SECURITY POLICIES AND PRINCIPLES

## EO1:

IDENTIFY THE PURPOSE OF THE CLASSIFICATION  
PROGRAM

Throughout history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our institutions, our homeland security and our interactions with foreign nations.

The purpose of the CNS Classification Program is to identify information that is classified under the Atomic Energy Act or Executive Order 13526 so that it can be protected against unauthorized dissemination.

The Classification Office has overall authority and responsibility for classification issues. Some specific responsibilities are:

- **Classification Officer:** An individual who has been appointed to manage a classification program.
- **Derivative Classifier:** An individual authorized to confirm that an unmarked document or material is unclassified or determine that it is classified as allowed by his or her description of authority. A DC may also upgrade a document or material. There are several DCs at CNS. For a complete listing of these, refer to the classification web-site.
- **Reviewing Official:** An individual authorized to confirm that an unmarked document or material contains sensitive unclassified information (i.e. Unclassified Controlled Nuclear Information or Official Use Only), as allowed by his or her description of authority.
- **Derivative Declassifier:** An individual authorized to declassify or downgrade documents or material in specified areas as allowed by his or her description of authority.

# EO2:

DEFINE CLASSIFIED INFORMATION OR MATTER

- **Classified information** is defined as any knowledge that can be communicated or documentary material regardless of its physical form or characteristics, which has been determined pursuant to executive order, regulation, or statute to meet classification requirements. It includes:
  - Restricted Data (RD) classified by the Atomic Energy Act or 10 CFR part 1045
  - Transclassified Foreign Nuclear Information (TFNI) classified by the Atomic Energy Act
  - National Security Information (NSI) classified by Executive Order 13526 or prior Executive Orders
- **Classified Matter** is defined as anything in physical form that contains or reveals classified information.

# EO3:

IDENTIFY THE LEVELS AND CATEGORIES ALONG WITH  
THE DAMAGE CRITERIA ASSOCIATED WITH CLASSIFIED  
INFORMATION OR MATTER

Information and matter are classified based on Levels and Categories. Information and matter vary in their importance to national security. The greater the risk of damage to national security if disclosed to unauthorized sources, the more sensitive the information is considered to be, and the higher the level of classification it has.

**CLASSIFICATION LEVELS** (indicates the level or degree of damage that could occur should that information or matter be compromised):

- **Top Secret (TS):** Information whose unauthorized disclosure could reasonably be expected to cause exceptionally GRAVE damage to the national security that the appropriate official is able to identify or describe.
- **Secret (S):** Information whose unauthorized disclosure could reasonably be expected to cause SERIOUS damage to the national security that the appropriate official is able to identify or describe.
- **Confidential (C):** Applies to information whose unauthorized disclosure could reasonably be expected to cause either UNDUE RISK to the common defense and security (if RD or FRD information) or DAMAGE to the national security (if NSI) that the appropriate official is able to identify or describe.



## **CLASSIFICATION CATEGORIES** (specify the type of information or material):

- **Restricted Data (RD):** All data concerning the design, manufacture, or use of nuclear weapons; production of special nuclear material; or use of special nuclear material in the production of energy except for data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act.
- **Formerly Restricted Data (FRD):** Classified information that the Department of Energy (DOE) or its predecessor agencies and the Department of Defense have jointly determined (1) to be related primarily to the military utilization of atomic weapons and (2) can be adequately safeguarded in a manner similar to NSI. It is also subject to the restrictions on transmission to other countries and regional defense organizations that apply to RD.
- **National Security Information (NSI):** Information that has been determined, pursuant to Executive Order 13526 or any predecessor order, to require protection against unauthorized disclosure and that is so designated.
- **Transclassified Foreign Nuclear Information (TFNI):** Classified information concerning the nuclear energy programs of other nations (including subnational entities) removed from the RD category under section 142 of the Atomic Energy Act after the DOE and the Director of National Intelligence jointly determine that it is necessary to carry out intelligence-related activities under the provisions of the National Security Act of 1947, as amended, and that it can be adequately safeguarded as National Security Information.

This includes information removed from the RD category by past joint determination between DOE and the CIA.

**TFNI DOES NOT** include information transferred to the United States under an Agreement of Cooperation under the Atomic Energy Act or any other agreement or treaty in which the United States agrees to protect classified information.

EO4:

IDENTIFY CLASSIFICATION AWARENESS REQUIREMENTS

## CLASSIFICATION REVIEWS

A document or material potentially containing classified information must be reviewed for classification to ensure that such information is identified for protection. In the following situations, the document or material must be reviewed by a **Derivative Classifier**:

- A newly generated document (in hard copy or electronic format) or material in a classified subject area that potentially contains classified information
- An existing, unmarked document or material that you believe may contain classified information
- An existing, marked document or material that you believe may contain information classified at a higher classification level or more restrictive category
- A document or material generated in a classified subject area intended for public release (e.g., for a publicly available webpage, for news organizations), including documents provided to or testimony given to Congress, must be reviewed by the Classification Officer or a Derivative Classifier who has been delegated this authority in writing
- Printed output from a classified information system must be reviewed to determine the appropriate classification **unless**:
  - The output is a final document that has already been reviewed and is appropriately marked
  - The printed output is a working paper that is:
    - Properly marked at the highest potential level and category or
      - a. Marked and protected at the highest level and category of information resident on the system; or
  - The program verified to produce consistent output and the Classification Officer has determined that the output is consistently classified at a particular level and category or is unclassified. When the Classification Officer documents the classification determination, all printed output from the system using the fields or elements reviewed can use that determination as the basis for its classification. If any fields or elements are added or revised, a new classification review is required.
- Extracts. A newly generated document that consists of a complete section must be:
  - marked as classified if the extracts are from a classified document;
  - must be reviewed by a DC if it is intended to be a stand-alone classified document; or
  - must be reviewed for declassification if it is intended to be a stand-alone unclassified document

If the complete section that is marked UNCLASSIFIED is removed from a classified document for use as a stand-alone document, a review is NOT required.

## CHALLENGES

CNS Personnel are encouraged and expected to challenge the classification of information, documents, or material that he or she believes is improperly classified.

Challenges may be submitted to the CNS Classification Office, however, any employee may submit a classification challenge in writing directly to the Director, Office of Classification. Information concerning the contact with the DOE Office of Classification can be located in DOE O 475.2B, *Identifying Classified Information*.

UNDER NO CIRCUMSTANCE ARE EMPLOYEES SUBJECT TO RETRIBUTION FOR MAKING A CHALLENGE.

While the classification review is being processed, the information, document, or material that is the subject of the challenge, must be protected at the current classification level and category or the classification level and category proposed by the challenge, whichever is higher, until a final decision has been made.

## **NO COMMENT POLICY**

Gen-16, Revision 2, "No Comment" policy provides guidance to DOE Federal and contractor personnel on appropriate actions on classified information and documents that appear in the open literature. This policy is found in 10 CFR 1045.22.

A comment is any activity that would allow a person who is not authorized access to classified information to locate the information or confirm the classified nature or technical accuracy of the information.

An authorized person must not comment (either verbally or in writing), to a person who is not authorized access to classified information on the classification status of any classified information in the open literature (including the fact that a document is being reviewed for classification or the results of such as review, which may be disclosed only to the person who submitted the document for review).

In today's information environment, it is likely that persons who are authorized access to classified information will encounter classified information online in the open literature or in various other literature sources (i.e., books, magazines, films, etc.). Commenting on classified information in the open literature can cause risk of greater damage to the national security by confirming its location, classified nature, or technical accuracy.

## **CLASSIFIED APPEARING IN THE PUBLIC DOMAIN DOES NOT MAKE THE INFORMATION UNCLASSIFIED.**

Identifying the location of specified online sites, titles of books, magazine articles, or other sources of information that reveal classified information is itself classified at the level and category of the information revealed.

Authorized holders of RD and FRD shall not confirm or expand upon the classification status or technical accuracy of classified information in the public domain. Unauthorized disclosure of classified information does not automatically result in the declassification of that information.

## **DECLASSIFICATION**

- **Declassification:** A determination by an appropriate authority (Derivative Declassifier) that information no longer warrants classification or that documents or material no longer contain classified information.

Examples of documents that may require a declassification review:

- Documents requested as part of the Freedom of Information Act (FOIA)
- NSI documents required to be reviewed for declassification should be referred to the Classification Officer for assistance
- **Declassification Proposals:** Each employee is encouraged and expected to submit proposals to declassify information he or she believes no longer requires protection. These proposals should be submitted in writing and must include a description of the information concerned and as reason for the request.
- **Who to Contact for Declassification Proposals:** Declassification proposals may be submitted to the proposer's Classification Officer or Program Classification Officer or to the Director, Office of Classification, who will coordinate the declassification proposals with the appropriate officials.

## CLASSIFIED INFORMATION OR MATTER PROTECTION ELEMENTS

# EO5:

IDENTIFY PROCEDURES FOR PROTECTION AND CONTROL  
OF CLASSIFIED INFORMATION AND MATTER



As a newly cleared individual, you should be familiar with the "cradle-to-grave" concept used in the Classified Matter Protection and Control (CMPC) program. If your work responsibilities involve handling classified matter, you must receive additional training beyond this security briefing. Not every CNS employee works with or comes in contact with classified matter.

Classified information in all forms must be protected in accordance with applicable laws, regulations, policies, directives, and other requirements.

It is important for all employees to understand the following concepts:

- **Creating Classified Matter**

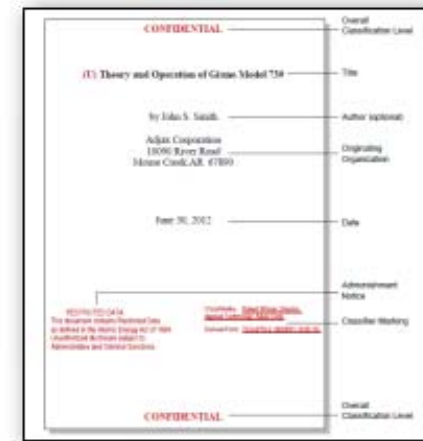
Classified "matter" can be any combination of documents and/or matter containing classified information. Examples include explosives whose shape is classified, classified parts, classified documents, or even classified conversations. Regardless of the type of classified matter, the individual creating it must use equipment that has been approved to process classified. The only exception to this rule is when the individual is creating classified by hand-writing notes or documents. Hand-written classified information must be protected and controlled the same as equipment-generated classified matter. Before a classification review, matter that may be classified must be protected at the highest classification level and category. The originator is responsible for obtaining a classification review.



- **Marking Classified Matter**

Classified matter must be marked to clearly identify it as classified. The highest level (Top Secret, Secret or Confidential) of classified information in the document must be placed on the top and bottom of the following:

- The cover page, if any
- The title, cover, or first page and
- The outside back of the last page.



Each interior page of a classified document must be marked:

- At the top and bottom with the highest classification level of page (or with an unclassified designation) or
- With the overall highest classification of the document.

Refer to MNL-352178, *Classified Matter Protection and Control Security Manual*, Section 4.4.3 for marking requirements (Pantex) or Y19-203, *Manual for the Protection and Control of Classified Matter* (Y-12).

- **In-Use Protection**

When not in approved storage, all classified information must be under the direct control of an individual who possesses the proper security clearance, access authorization, and need to know for the level and category of information being protected. All users of classified information must prevent unauthorized physical, visual, aural, cyber, and other access. Classified information must only be processed on information systems that have received approval to operate at the appropriate classification for the information according to DOE directives.

Classified matter must NOT be discussed, reproduced, destroyed, or processed in Property Protection Areas.

- **Storage of Classified**

Classified matter must be stored under conditions designed to deter and detect unauthorized access to the matter, to include securing it in a General Services Administration (GSA) approved container. Classified matter not under the personal control of an authorized person must be stored in the following methods:

<b>Top Secret</b>	<p>In a locked General Services Administration (GSA) –Approved Security Container with one of the following supplemental controls:</p> <ul style="list-style-type: none"> <li>• Under intrusion detection system (IDS) protection and by Protective Force (ProForce) personnel responding within 15 minutes of alarm annunciation</li> <li>• Inspections by ProForce personnel no less frequently than every two hours.</li> <li>• In a locked vault or vault-type room (VTR) within a limited area (LA), exclusion area (EA), protected area (PA) or material access area (MAA). <ul style="list-style-type: none"> <li>• The vault or VTR must be equipped with IDS equipment</li> <li>• ProForce personnel must respond within 15 minutes of alarm annunciation.</li> </ul> </li> </ul>
<b>Secret</b>	<p>Must be stored in any manner authorized for TS matter;</p> <ul style="list-style-type: none"> <li>• In a locked vault or in a locked GSA-approved security container within a LA or higher</li> <li>• In a locked VTR with the following supplemental controls,</li> <li>• Inspections by ProForce personnel no less frequently than every 4 hours; or</li> <li>• For a VTR located within a PA or higher security area, the ProForce personnel must respond within 30 minutes of the VTR's IDS alarm.</li> </ul>
<b>Confidential</b>	<p>Must be stored in the same manner prescribed for secret or TS matter. However, the supplemental controls are not required.</p>

- **Reproducing Classified**

Procedures for the reproduction of classified matter must be established to:

- Limit production of classified matter to the minimum number of copies consistent with operational requirements and any other pertinent reproduction limitations.
- Identify equipment authorized in accordance with CNS procedures and cyber security policy.

Classified documents, including those from other agencies, may be reproduced without approval of the originator, except where documents contain caveats limiting reproduction. Classified reproduction must not be performed in the presence of inappropriately cleared individuals. Reproduction of classified documents must be kept to the minimum number of copies for operational necessity and any further reproduction limitations shown on the document. Reproduction of all accountable documents must be coordinated through the Control Station (Y-12/Pantex). Classified documents may be copied only on approved copy machines located in security areas. These machines will have a sign indicating they are approved for classified reproduction. Reproduced copies are subject to the same protection and control requirements as the original matter.

- **Copy Machines**

Copy Machines used for classified reproduction must be approved by the CMPC office and located in approved areas(Limited, Exclusion, Material Access or Protected Areas). Copy machines must be designated and posted as approved for the reproduction of classified matter.

- **Clearing Copy Machines**

Copy machines must be cleared after classified documents have been reproduced. To clear a copy machine, three blank sheets must be run through the copier at the end of the process. The blank sheets run through the copier must be destroyed as classified waste.

- **Transmission of Classified**

Transmission of classified matter includes, mailing, hand carrying, transporting, and electronically transmitting (e.g., facsimile and e-mail) within and outside of CNS. Such transmissions must only be carried out in the performance of official and contractual duties.

- **Electronic Transmission**

Classified electronic transmissions must NOT take place over unclassified, non-secure telephone lines, computer lines, facsimile machines, or other similar electronic means. Approved methods of classified electronic transmission are as follows:

- Secure Telephone Equipment (STE), OMNI (Y-12), VIPER (PANTEX) telephone systems,
- Classified facsimile
- SecureNet

Individuals transmitting classified information via facsimile systems must confirm receipt (verbally or in writing) with the intended recipient. A log of incoming and outgoing classified facsimile activity is required, PX-1173B (Pantex). A classified document transmitted by an approved classified facsimile machine must be marked, if possible, as a final document before transmission. DOE F 1325.7A, *Telecommunication Message*, may be used as the first page of the facsimile.

When classified drafts are transmitted by facsimile, they must be marked at the highest potential overall classification level and category.

- **Mailing Classified Matter (Within Pantex/Y-12)**

Classified mail is transported by appropriately cleared individuals who maintain physical control of the matter at all times. Processing of classified mail by Mail Services personnel will be in accordance with approved Classified Mail Services desktop instructions.

Mail Services carriers/Transportation personnel must not under any circumstances open classified mail packages.

All packages used to transport classified matter must be appropriately addressed with the sender's and recipient's names and the classified mail stop(s).



- **Mailing Classified Matter (Outside Pantex/Y-12)**

All classified mail packages must enter the postal system or express delivery services from Classified Mail Services. All classified matter physically transmitted outside of Pantex must be enclosed in two layers, both of which provide appropriate protection and reasonable evidence of tampering and which conceal the contents.

When envelopes are used for packaging, the classified information must be protected from direct contact with the inner envelope. This is accomplished by having a cover sheet on the front of the document and a sheet of paper or cover sheet to protect the back of the document if the document has information on the back page.

Refer to MNL-352178, *Classified Matter Protection and Control Security Manual* (Pantex) or Y19-203, *Manual for the Protection and Control of Classified Matter* (Y-12) for additional mailing requirements.



- **Hand Carrying Classified Matter (Within Pantex/Y-12)**

Any individual who hand carries classified matter on site must:

- Be a cleared employee possessing the need to know
- Have a security clearance commensurate with the classification of the matter being hand carried
- Maintain positive control to prevent unauthorized access to the classified matter at all times
- Be trained in the appropriate CMPC module
- Appropriately stabilize classified prior to setting off for destination
  - Complete an Accountable Receipt, PX-925-1 (Pantex), when hand transferring accountable classified matter to another individual

- **Hand Carrying Classified Matter (Outside Pantex/Y-12)**

Hand carrying classified matter outside CNS (Pantex/Y-12) is highly discouraged and should only be used as a last resort method of transmission.

The following procedures and criteria must be met to hand carry classified information outside CNS (the Oak Ridge Complex/Pantex) and must be approved by the ODSA:

- An unusual situation warrants such action.
- The classified matter is not available at the destination.
- Time does not permit transmission by other authorized methods.
- The classified matter can be properly handled and protected during hand carrying transmission.
- The hand carrying transmission must be expected and/or scheduled to be completed on the same day, and the classified matter can be appropriately stored upon reaching the destination.

Personnel/traveler hand carrying classified matter outside CNS (the Oak Ridge Complex/Pantex) must complete a PX 956(Pantex) (approved by the ODSA) and:

- Possess the NTK,
- Have a security clearance appropriate with the classification of the matter being hand carried,
- Be traveling in the course of official company business,
- Maintain positive control to prevent unauthorized access to the classified matter at all times,
- Be trained in the appropriate CMPC module,
- Be approved in writing by the CNS Information Security Manager;
- Coordinate with Classified Mail Services for classified matter being hand carried,
- Have a Contingency Plan in place as delineated in PX-956(Pantex) and approved by the ODSA (See Section 2.1, Pantex, Section C6, Y-12),
- Make prior arrangements for storage of classified matter through the host security office.
- Obtain written authorization when traveling outside the United States, from the cognizant Departmental Element, who must arrange for nonprofessional diplomatic courier status from the U. S. Department of State.

Additionally, classified matter:

- Is prohibited from being taken to private residences or other unapproved places (e.g., hotel or motel rooms).
- Must remain within the physical custody of the traveler at all times during the trip. The briefcase must be of solid construction with lockable hardware.

- **Destruction of Classified Matter**

**Destruction Methods at Pantex**

Classified matter must be destroyed beyond recognition or re-composition. NOTE: Pantex does not currently utilize shredders for destroying classified documents. Destroy classified matter in accordance with current MNL-352178.

Use destruction methods that are approved to ensure classified matter is physically altered, demolished, or reduced to a useless form in such a way that no classified information can be obtained from it.

**Destruction Methods at Y-12**

Classified matter must be destroyed beyond recognition to preclude reconstruction, using one of the following approved methods:

- Shredding
- Burning
- Melting
- Chemical decomposition
- Pulverization
- Disassembly
- Mutilation
- Pulping

Deconstruction must remove the possibility of recognition, reproduction, or reconstruction of the matter.

## Discussion of Classified Information

Discussion of classified information shall take place only in approved security areas. If you are unsure if you are in an approved area, do not discuss classified information. Telephones are one of the greatest tools at our disposal, but they can also be one of our greatest vulnerabilities to the protection of classified resources. Classified information must never be discussed on a conventional telephone. Secure Telephone Units (STU) have been placed in various locations around the Plant and must be used for classified telephone discussions.

### References:

- DOE O 471.6, *Information Security*
- Y19-203, *Manual for the Protection and Control of Classified Matter* (Y-12)
- MNL-352178, *Classified Matter Protection and Control Security Manual* (Pantex)
- U.S. Title Code 18, Subsection 798, *Disclosure of Classified Information*

# EO6:

DEFINE UNAUTHORIZED DISCLOSURE

- **Unauthorized disclosure:** a communication or physical transfer of classified information to an unauthorized recipient.

EO7:

IDENTIFY PENALTIES FOR UNAUTHORIZED DISCLOSURE



- Unauthorized disclosure of classified information is subject to criminal and/or civil penalties, as provided by the Atomic Energy Act of 1954; the Espionage Act; and other security directives. Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States **ANY** classified information shall be fined under U.S. Title Code 18, Subsection 798, *Disclosure of Classified Information* or imprisoned not more than ten years, or both (imprisonment/fines).

# EO8:

IDENTIFY CONDITIONS AND RESTRICTIONS FOR ACCESS  
TO CLASSIFIED INFORMATION OR MATTER

Personnel requiring access to classified information and/or matter must meet the following requirements:

- Possess a DOE Access Authorization/Security Clearance ("L" or "Q")
- Must have the Need-to-know (NTK)
- Sign Standard Form 312 (SF312), Classified Information Nondisclosure Agreement
- Complete the appropriate training

Classification Level	Classified Matter Category			
	Restricted Data (RD)	Formerly Restricted Data (FRD)	National Security Information (NSI)	Transclassified Foreign Nuclear Information (TFNI)
Top Secret	Q	Q	Q	Q
Secret	Q	Q & L	Q & L	Q
Confidential	Q & L	Q & L	Q & L	Q & L

# EO9:

IDENTIFY INDIVIDUALS' SAFEGUARDS & SECURITY  
REPORTING REQUIREMENTS

Any person who determines classified matter has been or may have been lost or compromised or is otherwise unaccounted for, must take immediate action to preclude any further or potential compromise.

This information must be immediately reported in person or via a secured communication to the Plant Shift Superintendent 865.574.7172 (Y-12) or the Operations Center at 806.477.5000 (Pantex).

# EO10:

IDENTIFY LEGAL AND ADMINISTRATIVE SANCTIONS FOR  
SECURITY INFRACTIONS AND VIOLATIONS OF LAW

A security infraction is any knowing, willful, or negligent action contrary to the requirement of Executive Order 13526, *Classified National Security Information*. If security personnel find these actions were intentional or caused by gross negligence, the action may constitute a violation resulting in criminal prosecution or other administrative action(s).

Committing a security infraction may result in administrative discipline including loss of access authorization.

#### Examples of Security Infractions:

- Leaving classified documents or material exposed and unattended or unsecured, to include leaving a classified repository open and unattended
- Failure to properly safeguard classified documents or combinations to repositories
- Changing a document's classification marking without proper authority
- Failure to provide for a document classification review, as required
- Destruction of classified documents in other than the prescribed manner
- Improper transmission of classified documents or material
- Failure to escort uncleared personnel within security areas
- Unauthorized possession of prohibited articles in CNS facilities

A security violation is any knowing, willful or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information. Suspected or a known violation of U.S. criminal statutes, Federal statutes, or Federal laws pertaining to the unauthorized disclosure of classified matter are referred to Federal Law Enforcement for further action.

Incidents of security concern, infractions, and violations are all subject to legal and administrative sanctions, to include disciplinary action, possible termination of employment, and possible prosecution in a court of law.

Unauthorized disclosure of classified information is subject to criminal and/or civil penalties, as provided by the Atomic Energy Act of 1954; the Espionage Act; and other security directives. The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations (CFR), Part 824, "Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations."



# EO11:

IDENTIFY PROTECTION AND CONTROL PROCEDURES FOR  
CONTROLLED UNCLASSIFIED INFORMATION

## Controlled Unclassified Information (CUI)

CUI is information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or governmental interests, commercial interests, or personal privacy. CUI is broadly defined as unclassified information that may be exempt from public release under the Freedom of Information Act (FOIA).

At CNS there are two types of CUI:

- **Official Use Only (OUO):**

Certain unclassified information that meets the following two criteria:

- **Damage.** In the opinion of the person making the determination, the information has the potential to damage governmental, commercial, or private interests if released to persons who do not need it to do their jobs or other DOE-authorized activity..
- **Potentially falls under a Freedom of Information Act (FOIA) Exemption:** In the opinion of the person making the determination, the information may fall under at least one of the FOIA exemptions (3-9).

OUO includes the following:

- Personally Identifiable Information (PII)
- Privacy Act Information
- Proprietary Information
- Export Controlled Information
- Patent Information
- Sensitive Nuclear Technology
- Applied Technology
- Source Selection Technology

## **When must a document be reviewed for OOU?**

An unclassified document originated within a program element must be evaluated to determine whether it contains OOU information:

- If the originator believes the document contains sensitive information, it should be reviewed prior to being finalized, released by the originator outside of the activity or office, or filed.
- Documents originated prior to April 9, 2003, (when the OOU program was established) must be reviewed if they are going to be publicly released if the possessor believes there is a potential for the document to contain sensitive information.

## **Who has authority to identify OOU?**

- Any employee, Federal or contractor, from an office with cognizance over the information may make OOU determinations for unclassified documents
  - Originated within his/her office
  - Produced for his/her office
  - Under the control of his/her office
  - No special authority or designation is required
  - Training is not required, but is highly recommended
  - Some Program Offices may have additional requirements (training, specific personnel to make determinations, etc.)

## **OUO and the FOIA Exemptions**

### **Exemption 3-Statutory Exemption**

- Disclosure of information is prohibited by statute
- Not OUO if information is otherwise classified or controlled (e.g., RD, FRD, TFNI, UCNI)

### **Examples of Exemption 3**

- **Espionage Act**-Information pertaining to communication intelligence and cryptographic devices
- **National Security Act of 1947**-Intelligence sources and methods
- **Internal Revenue Code**-Taxpayer Identification numbers

## **OUO and the FOIA Exemptions**

### **Exemption 4-Commercial/Proprietary**

- Trade Secrets
- Commercial or financial information whose release would:
  - Impair the Government's ability to obtain information in the future, or
  - Cause competitive harm to submitter

### **Examples of Exemption 4**

- Trade Secret Information (e.g. Coca-Cola formula)
- Financial Information, such as income, profits, losses, costs
- Contract proposal, solicited or unsolicited
- Customer/supplier lists
- Government credit card numbers
- Security measures for commercial entities performing work for the Government

## **OUO and the FOIA Exemptions**

### **Exemption 5-Privileged Information**

Three primary privileges:

- Deliberative process (a.k.a. "predecisional")
- Attorney-Work Product
- Attorney-Client

### **Examples of Exemption 5**

- Documents concerning budget cuts
- Documents concerning cancellation of a program
- Documents concerning DOE property purchases

## **OUO and the FOIA Exemptions**

### **Exemption 6-Personal Privacy**

- Constitutes a "clearly unwarranted invasion of personal privacy"
- Personal information that might cause distress or embarrassment or risk identity theft

### **Examples of Exemption 6**

- Personally Identifiable Information (PII)
  - Examples (when associated with an individual)
    - Social security number (even when not associated with an individual)
    - Place/Date of Birth
    - Mother's maiden name
    - Medical history
    - Financial history

## **OUO and the FOIA Exemptions**

### **Exemption 7-Law Enforcement**

Includes but is not limited to:

- Information whose release could reasonably be expected to endanger the life or physical safety of any individual or
- Information would disclose techniques and procedures for law enforcement investigations or prosecutions

### **Examples of Exemption 7**

- Investigative Information
- Civil, criminal investigations
- Personnel investigations
- National Security/Terrorism investigations
- Security measures to protect Federal officials
- Security measures to protect Federal buildings
- Security manuals
- Classification guides



## **OUO and the FOIA Exemptions**

### **Exemption 8-Financial Institutions**

- Evaluations of a financial institution's stability prepared by, on behalf of, or for use of an agency responsible for regulation of financial institutions (FDIC, etc.)

### **Exemption 9-Wells**

- Technical and scientific information about any type of well

### **Examples of Exemption 9**

- Geothermal well BTU production
- Ground water inventories and well yields in gallons per minute
- Natural gas reserves

## How is OOU Marked?

Front Marking-Determination Based on Guidance (Classification/Control Guides)

### Front Marking – Determination based on Guidance (Classification/Control Guides)

The diagram shows a form titled "OFFICIAL USE ONLY" with the following text: "May be exempt from public release under the Freedom of Information (5 U.S.C. 552), exemption number and category: 7, Law Enforcement". Below this is a section titled "Department of Energy review required before public release" with fields for "Name/Org: John Smithson, NA-121", "Date: 4/11/14", and "Guidance (if applicable): EG-SS-4". Red arrows point from labels to specific fields: "Name AND Organization" points to the "Name/Org" field; "Exemption Number" points to the "7" in the exemption category; "Exemption Name" points to "Law Enforcement"; "Date of Determination" points to the "Date" field; and "Short Name of Guide" points to the "Guidance" field.

**OFFICIAL USE ONLY**

May be exempt from public release under the Freedom of Information (5 U.S.C. 552), exemption number and category: 7, Law Enforcement

**Department of Energy review required before public release**

Name/Org: John Smithson, NA-121 Date: 4/11/14

Guidance (if applicable): EG-SS-4

**Name AND Organization**

**Exemption Number**

**Exemption Name**

**Date of Determination**

**Short Name of Guide**

**Markings are for example purposes only**

38

**Page Marking**

OFFICIAL USE ONLY:

- On bottom of ALL pages OR
- On bottom of only those pages containing OUO information.

XXXXX XX X XXXXXX XXX  
XX XXXXXXXXXXXX XXXXXXXX  
XXXXXXXXXX.

XX XXXXXXXX X|XXXX XXXX  
XXXXXXXXXX XX XXXXXX. XX  
XXXX XXXXXXXX X XXXXX  
XXXXXX XXXX XXXX.

OFFICIAL USE ONLY

## **Mandatory Supplemental Markings**

- Markings required by law, regulation, or other DOE directives that convey additional advice on handling or access restrictions
- Used in addition to, not in place of OOU markings (both types of markings must appear on the document)
- OOU Markings ensure consistent protection and handling throughout DOE

## **Examples of information with supplemental markings:**

- Protected Cooperative Research and Development Agreements (CRADA) information
- Export Controlled Information
- Applied Technology Information
- Source Selection Information

SAMPLE OF OOU DOCUMENT WITH  
SUPPLEMENTAL MARKING (CRADA)

XXX XXXXXX XX XXXXXXXX  
XXXXX XXXXXXXXXXXXXXX XXXXXXX

XXXXXXXX. XXXX XXXXXX XXXXXXXXXXX XXX XXXXXXX XXXX XXXXXXX XXXXXXXXXXX XXX XXXXXXXXXXXXXXX,  
XXXXXXXX, XXX XXXXXXXXXXX XXXXXXX XXX XXXX (XXX) XXXXXXXXXXX. XXXX XXXXXXX XXXXXXX  
XXXXXXXX XXXXXXXXXXX XXX XXXXXXXXXXX XXXXXXX. XXXXXXX X XXXXXXX XXX XXXXXXXXXXXXXXX  
XXX XXXXXXXXXXX XXX XXXXXXX XXX XXXXXXXXXXX; XXXXXXX XX XXXXXXXXXXX XXXXXXXXXXX XXX  
XXXXXXXXXXXX. XXX XXXXXXXXXXX XXXXXXXXXXX XXXXXXX (XXX), XXXXXXXXXXX X, XXX XXXXX  
XXXXXXXXXXXX XXX XXX XXXXX XXX XXXX XX XXX/XXXXXXXX XXXXXXXXXXX XXXXXXXXXXX.

XXXXXXXX. XXXXXXX XXXXXXXXXXX XXXX XXXXX XXXXXX XX XXXXXXXXXXX XXX XXXXXXXXXXX  
XXXXXXXXXXXXXXXX XXX XXXXXXX XXXXXXX XX XXX-XXXX-XXXX.

Protected CRADA Information

This product contains Protected CRADA Information which was  
produced on 11/6/06 under CRADA No. 12345 and is not to be  
further disclosed for a period of five years from the date it was  
produced except as expressly provided for in the CRADA.

OFFICIAL USE ONLY

May be exempt from public release under the Freedom of Information Act  
(5 U.S.C. 552), exemption number and category: 3, Statutory  
Exemption  
Department of Energy review required before public release  
Name/Org: Curtis Gonzales, BWXT-Pantex Date: 4/15/03  
Guidance (if applicable): Pantex Plant OOU Topical Guide

OFFICIAL USE ONLY

**Markings are for example purposes only**

## HOW IS A DOCUMENT CONTAINING OUO AND NATIONAL SECURITY INFORMATION MARKED?

Do not apply OUO front and page markings

Do apply

- title marking
- portion marking

The diagram shows a rectangular box representing a document template. At the top center is the word "SECRET". Below it is the text "(OUO) Title" followed by three horizontal lines. Below this is the text "(S)" followed by three horizontal lines. Below that is the text "(OUO)" followed by three horizontal lines. Below that is the text "(U)" followed by three horizontal lines. At the bottom center is the word "SECRET". Two red arrows originate from the text on the left: one points from "title marking" to the "(OUO) Title" section, and the other points from "portion marking" to the "(OUO)" section.

SECRET

(OUO) Title

(S)

(OUO)

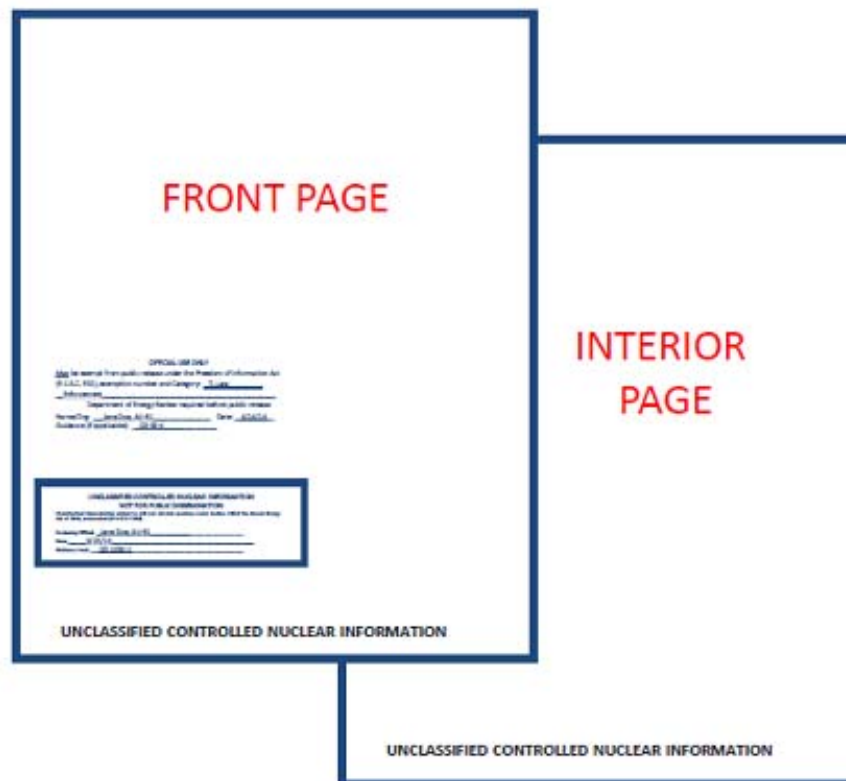
(U)

SECRET

**Markings are for example purposes only**

## HOW IS A DOCUMENT CONTAINING OUO AND UCNI MARKED?

- Apply OOU front marking to a document containing both OOU and UCNI to alert holder to the presence of OOU information
- For interior pages may use the highest category of information in the document (UCNI) on every page or the actual category of information (UCNI or OOU) found on each page



**Markings are for example purposes only**



## HOW IS A DOCUMENT TRANSMITTING OUO MARKED?

Document transmitted  
contains OUO information

- Required if transmittal document itself does not contain classified or controlled information
- Calls attention to presence of OUO information in attachment



## SAMPLE MARKING OF DOCUMENT TRANSMITTING OUO:



Attachment contains  
OUO; transmitting  
document does not  
contain classified or  
controlled information

## HOW IS AN e-MAIL CONTAINING OUO MARKED?

- First line of message
  - Insert "OUO" before text
  - If attachment to message is OUO:
    - Message must indicate attachment contains OUO
    - Attachment must be marked correctly

## HOW IS OOU PROTECTED?

### Who may have access to OOU?

- Anyone needing the information to perform his/her job or other DOE-authorized activity
  - No security clearance required
  - Not limited to DOE employees
  - No requirement for U.S. citizenship
- Some OOU may have additional restrictions (Export Controlled Information, Source Selection Information, etc.)
- Determination made by **person possessing** document-**not person wanting** the document

### In-Use

- Take reasonable precautions to prevent access by persons who don't need the information to do their jobs.
- For example, don't read an OOU document in a public place.

### Storing OOU

- With internal building security during non-duty hours-unlocked file cabinet, desk, briefcase, etc.
- No internal building security during non-duty hours-locked room or locked file cabinet, desk, briefcase, etc.

## **HOW IS OUO PROTECTED?**

### **Copying OUO**

- No permission from originator needed
- Make minimum number of copies
- Make sure copies are marked and protected

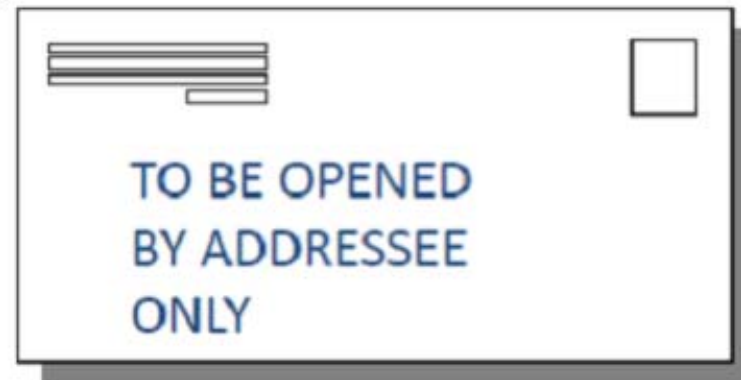
### **Destruction of OUO**

- Strip-cut shredder with strips no more than ¼ inch wide and 2 inches long
- May also use method approved for classified
- Any other method approved by Classification Office

## Transmission of OUO

### Transmitting by mail-Inside Facility

- Place in sealed, opaque envelope or wrapping with recipients address and "TO BE OPENED BY ADDRESSEE ONLY" on outside



### Transmitting by Mail-Outside Facility

- Place in sealed, opaque envelope or wrapping with recipient's address, return address, and "TO BE OPENED BY ADDRESSEE ONLY" on outside (same requirements as inside facility, but must include return address)
- U.S. mail-First Class, Express, Certified, Registered
- Any commercial carrier

### **Transmitting by Hand Between Facilities or Within a Facility**

- May be hand-carried
- Must control access to document

### **Transmission by Fax or e-Mail**

- Use encryption methods (e.g., Entrust) whenever possible
- Emailing OUC outside of the CNS firewall WITHOUT encryption will result in an Incident of Security Concern (IOSC)

### **Transmission Over Voice Circuits**

- Use encryption when possible
- If unavailable and other encrypted means are not a feasible alternative, regular voice circuits allowed

## **Penalties for Misuse of OUO**

Penalties may be imposed if individual:

- Intentionally releases OUO information from document marked OUO
- Intentionally or negligently releases OUO document
- Intentionally does not mark a document known to contain OUO information
- Intentionally marks a document OUO known not to contain OUO information

### **Examples of Penalties**

- Verbal admonishment
- Written reprimand
- Suspension
- Termination

## **Where Can You Obtain Additional Information About OUO?**

- DOE O 471.3, Administrative Change 1
- DOE Manual 471.3-1, Administrative Change 1

**Unclassified Controlled Nuclear Information:** Certain unclassified design and security information concerning nuclear facilities, material, and weapons that can be controlled under section 148 of the Atomic Energy Act.

## **Why Is UCNI Controlled?**

Because its release would significantly increase the likelihood of the illegal production of a nuclear weapon or the theft, diversion, or sabotage of nuclear material, equipment, or facilities.

## **What Information Could be UCNI?**

- Unclassified Government information that concerns atomic energy defense programs
- Three subject areas:
  - Design of production or utilization facilities
  - Security measures for the physical protection of production or utilization facilities or nuclear material contained in these facilities or in transit
  - Declassified RD

**What are Your Responsibilities for UCNI?** All CNS employees and non-employees have a responsibility to protect the confidentiality of personal and other sensitive information from unauthorized disclosures and intentional or negligent misuse.

CNS employees and non-employees with access to UCNl:

- Must refer documents that may require UCNl to an UCNl Reviewing Official with appropriate authority
- Must protect UCNl in accordance with 10 CFR 1017, DOE directives and CNS policies and procedures

### **How Do You Know if a Document Should Be Reviewed for UCNl?**

If the document is an UCNl subject area, it may contain UCNl.

#### **What Are UCNl Subject Areas?**

- Safeguard & Security
- Arms Control & Verification
- Intra-Site Secure Transport Vehicle
- Transportation Safeguards and Security
- Radiological Emergency Response
- High Explosives in Nuclear Weapons
- Nuclear Nonproliferation
- Uranium Atomic Vapor Laser Isotope Separation (AVLIS)
- Plutonium AVLIS
- Gaseous Diffusion
- Plutonium Processing



## What If You Are Not Sure if a Document May Contain UCNi?

If you are not sure if a document may contain UCNi, contact:

- An UCNi Reviewing Official
- Your Supervisor
- Your Program Classification Officer (PCO) or Classification Representative

## How Do You Identify a Document That Contains UCNi?

If a determination has been made that a document contains UCNi, it will have page markings and an UCNi front marking

### UCNi Front Page Marking

<p style="text-align: center;"><b>UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION</b> <b>NOT FOR PUBLIC DISSEMINATION</b></p> <p>Unauthorized dissemination subject to civil and criminal sanctions under Section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168).</p> <p>Reviewing Official: _____</p> <p>Date: _____ (Name/Organization)</p> <p>Guidance Used: _____</p>
--

### **UCNI PAGE MARKINGS (EXAMPLE PURPOSES ONLY)**


The following markings will be located on the bottom of the page and on the back cover  
(Reference 1017.16(a)(1) and (2))

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

UCNI

*(only if space is limited)*

## SAMPLE DOCUMENT CONTAINING UCNI



**DEPARTMENT OF ENERGY**  
Washington, D.C. 20585

This is a sample of the front page of a document with the required UCNI markings:

1. The words "Unclassified Controlled Nuclear Information" are on the bottom of the first page.
2. The front marking, which identifies the Reviewing Official with his or her organization, the date the UCNI determination was made, and the guidance used to make the determination, is on front of the document.

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION  
NOT FOR PUBLIC DISSEMINATION  
Information is controlled pursuant to DOE and (where  
applicable) under section 105 of the Atomic Energy Act of 1954,  
as amended (42 U.S.C. 2161).

Reviewing Official: John Smith, CTM  
(Name/ Organization)  
Date: 11/1/19  
Guidance Used: DOE PDR

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

## SAMPLE UNCLASSIFIED DOCUMENT TRANSMITTING UCNi

- Attachment instructions are placed on the transmittal
- Calls attention to the presence of UCNi in the attachment and indicates how the transmittal is handled when separated from the attachment

XXX XXXXX XX XXXXXX  
XXXX XXXXXXXXXXXXXXX XXXXXX

XXXXXXXX. XXX XXXXX XXXXXXXX XXX XXXXXXX XXX XXXXXXX XXXXXXXX XXX  
XXXXXXXXXX, XXXXXX, XXX XXXXXXXX XXXXXXXX XXX XXX (XXX)  
XXXXXXXXXX. XXXXX XXXXXXXX XXXXXXX XXXXXXXX XXXXXXXX XXX XXXXXXXX  
XXXXXXXX. XXXXXX X XXXXXXX XXX XXXXXXXX XXX XXXXXXXX XXX  
XXXXXX XXX XXXXXXXX; XXXXXX XX XXXXXXXX XXXXXXXX XXX  
XXXXXXXXXX. XXX XXXXXXXX XXXXXXXX XXXXXXXX (XXX), XXXXXXXX X,  
XXXX XXXXX XXXXXXXX XXX XXX XXXXX XXX XXX XX XXX/XXXXXXXX  
XXXXXXXXXX XXXXXXXX.

XXXXXXXX. XXXXXXX XXXXXXXX XXX XXXXX XXXXX XX XXXXXXX XXX  
XXXXXXXXXX XXXXXXXX XXX XXXXXXX XXXXX XXX XXX-XXX-XXXX.

Document transmitted contains  
Unclassified Controlled Nuclear  
Information. When separated  
from enclosures, this transmittal  
document does not contain UCNi.

### **SAMPLE e-MAIL CONTAINING UCNI**

First line will have "UCNI" and Reviewing Official's name and organization, and guidance used to make the determination.

**From:** Martinez, Paul  
**Sent:** Friday, June 5, 2009 3:15 PM  
**To:** Puits, Clair  
**Cc:**  
**Subject:** UCNI Markings on E-Mail Messages  
**Attachments:**

**UCNI; Paul Martinez, CTI-61; CG-PUN-1** – When the e-mail contains UCNI, the first line must have this information.

## What Markings Does a Document Have to Indicate it No Longer Contains UCNi?

- A Reviewing Official may determine, based on guidance, that an unclassified document or material marked as containing UCNi no longer contains UCNi.
- In such as case, the Reviewing Official:
  - Ensures that all UCNi markings are removed or crossed out and
  - The front of the document or material is marked with :

DOES NOT CONTAIN  
UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION  
Reviewing/Denying Official: Michael Kieszowski, CTI-61  
(Name/Organization)  
Date: 4/30/16

## **Access to UCNl**

### **Who Can Have Access to UCNl?**

#### **Routine Access**

- Authorized person
  - No security clearance required
  - Must meet criteria in 10 CFR 1017, Subpart D
- Need to Know

### **Who Can Have Routine Access to UCNl?**

- **U.S. Citizen**
  - Federal Government (military or civilian) employee
  - Employee of a Federal Government contractor or subcontractor
  - Employee of state, local, and tribal governments
  - Emergency Responders
  - Government Consultant
- **Non-U.S. Citizens**
  - Federal Government (military or civilian employee)
  - Employee of a Federal Government Contractor or subcontractor
  - Employee of state, local and tribal governments
  - Persons who need to know the UCNl in conjunction with activity approved by the DOE Program Secretarial Officer or NNSA Deputy or Associate Administrator with cognizance of the UCNl.
  - For others, refer to 10 CFR 1017, Subpart D

## If They Do Not Meet the Criteria For Routine Access, Can an Individual Have Access to UCNI?

Maybe.

- Check **ALL** criteria in Subpart D of 10 CFR 1017 to verify they do not meet the criteria for routine access
- If they do not meet the criteria for routine access, they may be eligible for limited access.
- **For limited access:**
  - Must have a need to know the information
  - Must submit a request for limited access to the appropriate approving authority in accordance with 1017.21
  - Further dissemination is not permitted

### Limited Access

This type of access is for persons not eligible for Routine Access.

### How is UCNI Stored?

- Must be stored to preclude unauthorized disclosure
- When not in use, documents or material containing UCNI must be:
  - Stored in a locked receptacle (e.g., file cabinet, desk drawer) or
  - If in a secured area or facility, in a manner that would prevent inadvertent access by an unauthorized individual



## How are Documents Containing UCNi Transmitted?

- A document or material marked as containing UCNi may be transmitted by:
  - U.S. First Class, Express, Certified or Registered Mail
  - Any means approved for transmission of classified documents or material
  - An authorized individual or person granted limited access as long as physical control of the package is maintained
  - Internal mail services
- The document or material must be packaged to conceal the presence of the UCNi from someone who is not authorized access. A single, opaque envelope or wrapping is sufficient for this purpose.
- The address of the recipient and the sender must be indicated on the outside of the envelope or wrapping along with the words "TO BE OPENED BY ADDRESSEE ONLY"
- **Encryption is REQUIRED** over telecommunication circuits (e.g. e-mail, telephone, fax, internet)

### **Are There Limits to Copying Documents Containing UCNI?**

- Minimum extent necessary
- Originator permission NOT required
- Ensure UCNI markings are on all copies

### **How IS UCNI Disposed Of?**

- Plain brown burn bags
- Cross-cut shredder that produces particles no larger than ¼ inch wide and 2 inches long
- Any classified method of destruction
- Sensitive Unclassified Data Boxes (Pantex)

## **DO NOT DISPOSE OF UCNI IN RECYCLE BINS OR OFFICE TRASH CANS!**

### **What Are the Penalties for Infractions and Violations?**

#### **Infractions:**

- Administrative Penalty

#### **Violations:**

- Civil penalty of up to \$150,000
- Criminal penalty of:
  - 2 Years (without intent to harm the Nation)
  - 20 Years (with intent to harm the Nation)

#### **If You Have Questions About UCNI, Refer to:**

- 10 CFR Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*, Revision Effective 12/08/08
- DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*
- CNS Classification Office:
  - 865.576.0134 (Y-12)
  - (806)477.6152 (Pantex)
- CNS Controlled Unclassified Information Point of Contacts:
  - Prescott Griggs (Y-12) 865.574.4891
  - Blake Villanueva (Pantex) 806.477.5291
- Your Classification Representative
- DOE Office of Classification Outreach 301.903.7567 or outreach@hq.doe.gov

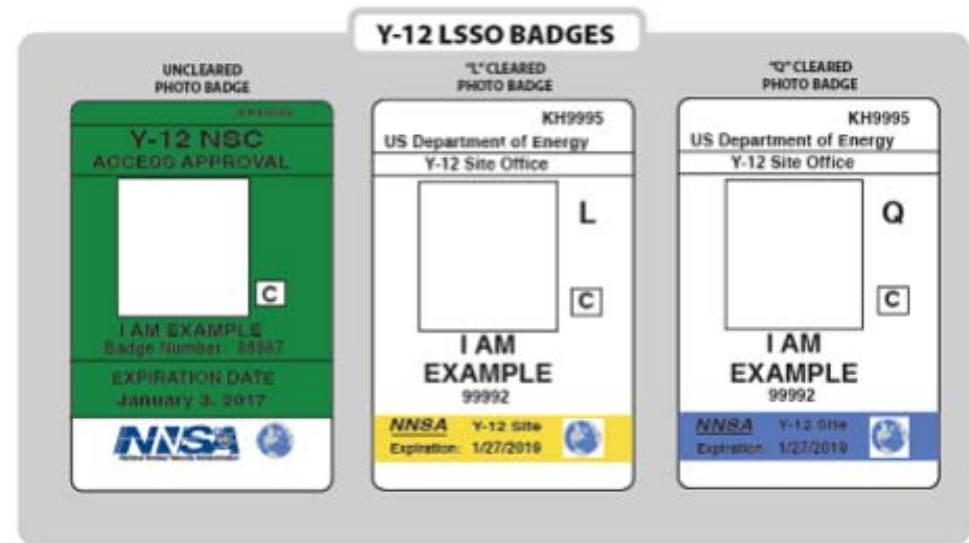
# EO12:

IDENTIFY INFORMATION PERTAINING TO SECURITY  
BADGES, SECURITY CLEARANCE LEVELS AND ACCESS  
CONTROLS

There are currently two types of badges utilized at CNS:

- Local Site Specific Only (LSSO)

### Y-12 LSSO Badges:



The LSSO badge uses a letter and a color-coded background or stripe to indicate the access authorization level, or security clearance.

The appropriate letter opposite the picture indicates the clearance level in addition to the following:

**GREEN:** Indicates the individual is **UNCLEARED**

**YELLOW STRIPE:** Indicates an "L" access authorization has been granted.

**BLUE STRIPE:** Indicates a "Q" access authorization has been granted.

## Pantex LSSO Badges:



**LSSO** badge uses a letter and a color-coded background to indicate the access authorization level, or clearance.

The appropriate letter opposite the picture indicates the clearance level in addition to the following colors:

- At Pantex, the security badge with a **WHITE** background and **RED "V"** indicates that an individual is UNCLEARED and at Pantex on a temporary basis.
- The security badge with a **GREEN** background indicates that an individual is UNCLEARED.
- The security badge with a **YELLOW** background indicates an "L" access authorization has been granted.
- The security badge with a **BLUE** background indicates that a "Q" access authorization has been granted.

NOTE: The LSSO badge **MUST** be worn at Pantex in addition to the HSPD-12.

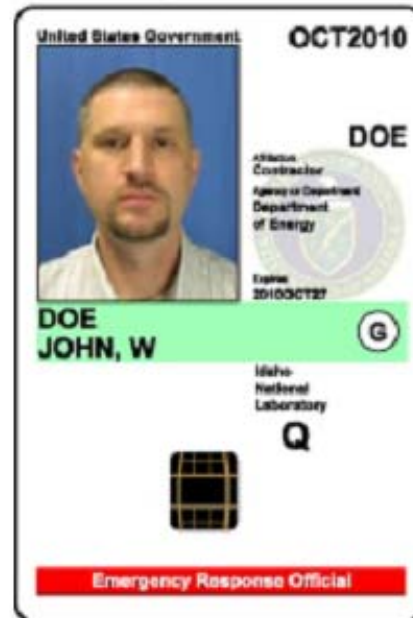


## Pantex LSSO Human Reliability Program (HRP) Designations

HRP is a security and safety reliability program designed to assure that individuals who occupy positions affording access to certain materials, nuclear explosive devices, facilities and programs meet the highest standards of reliability as well as physical and mental suitability.



- DOE Security Badge (HSPD-12)



Homeland Security sponsored a Presidential Directive signed in 2004 that requires all employees of the federal government, all prime contractors, and all sub-contractors to process through a basic background check and possess a federal credential. The HSPD12 is the result of that directive.



## **BADGE RESPONSIBILITIES:**

- **ALWAYS** wear badge(s) on CNS sites
- The HRP indicator LSSO badge must also be worn with the HSPD12 at Pantex
- Ensure badge is visible on upper body
- When not on DOE owned or leased property, badge should be removed or obscured from visual access
- Do NOT alter, photocopy, scan, reproduce, or photograph/video badge
- Do not post badge information to any social media sites
- Do NOT share your badge or let anyone use your badge
- Do NOT leave badge unattended or in plain view(Y-12)
- Do NOT leave badge visible in vehicle(Pantex)
- Do NOT wear LSSO badge off-site
- Do NOT wear HSPD-12 badge outside of CNS sites unless it is for an official government purpose
- Keep the HSPD-12 badge in the approved holder provided by the badge office when not in use

## **Reporting Lost Badges**

To report a lost badge during normal business hours, contact the following;

Y-12 Badge Office-865.574.3285

Pantex Access Control-806.477.3908 or 806.477.3909

To report a lost badge after business hours, contact the following:

Y-12 Plant Shift Superintendent's Office-865.574.7172

Pantex Operations Center-806.477.5000

## **Reporting Stolen Badges**

To report a stolen badge during normal business hours contact the following:

Y-12 Badge Office-865.574.3285

Pantex Access Control-806.477.3908 or 806.477.3909

To report a stolen badge after normal business hours contact the following:

Y-12 Plant Shift Superintendent's Office-865.574.7172

Pantex Operations Center-806.477.5000

A report must also be made with local police department to report the stolen badge. Ensure the police department files a report, obtain a copy of the report and submit it to the Y-12 Badge office Personnel (Y-12) or Pantex Access Control (Pantex).

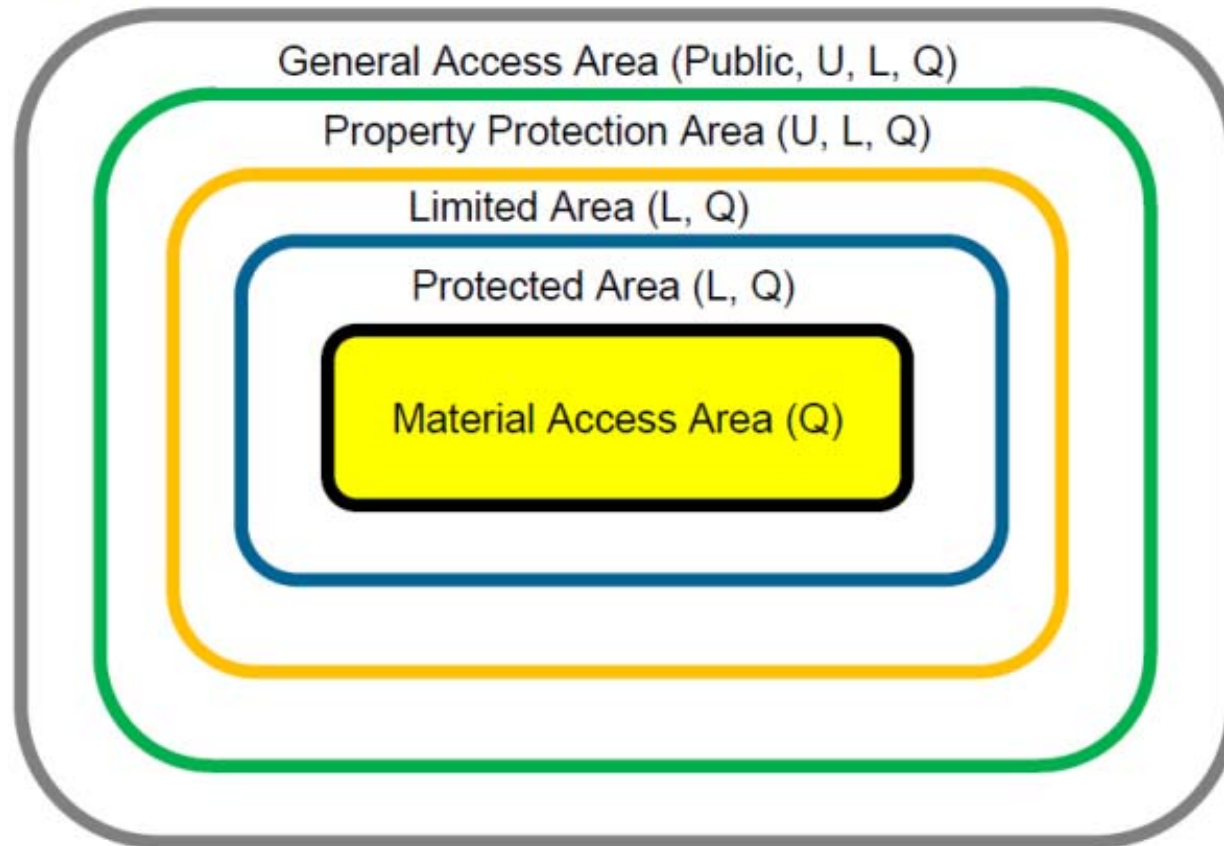
There are also other forms you will complete at the Y-12 badge office or Pantex Access Control Office.

## **Badge Surrendering**

- Security Police Officer/Supervisor Direction
- Resignation/Termination
- Expired or No Longer Valid/Required
- Any Leave of Absence >30 days or if unknown duration

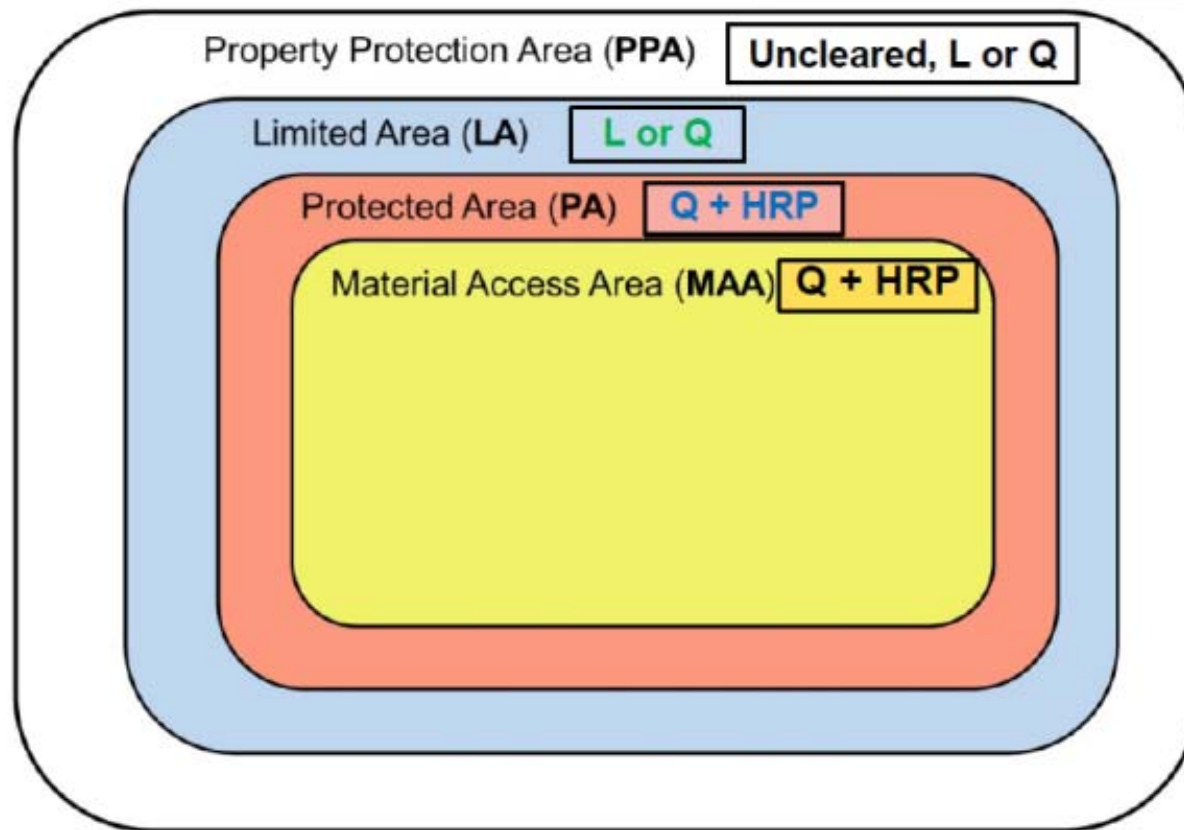
## Access Controls

**Y-12**



## Access Controls

### PANTEX



Layers of security requirements, beginning with the least restrictive and moving inward to the most restrictive, must be implemented for protecting S&S interests at CNS. Personnel requiring access to these facilities that are not General Access Areas, must have a security badge for entry.

Badges are verified by either a security police officer (SPO) or an automated access control system. These security areas are physically defined by permanent barriers. Access to these security areas must be based on the individual's need-to-know to perform official duties, validation of the individual's access authorization, and the presentation of a valid badge.

- **General Access Area (GAA)**

This type of area may be established to allow access to certain areas with minimum security requirements. GAAs are accessible to all personnel, including the public. Example: Y-12 History Center located at New Hope.

- **Property Protection Area (PPA)**

This type of area has been established to protect government-owned property and equipment against damage, destruction or theft and must provide a means to control public access. A DOE security badge (HSPD-12) or a LSSO badge (for that site) will grant access to the property protection areas. Employees and non-employees that have been issued an uncleared, "L" or "Q" badge may be granted access to the PPA.

- **Limited Area (LA)**

This security area has been established to protect classified matter and Category III/IV material to serve as a concentric layer of protection. An individual must have a DOE "L" or "Q" clearance to access this area unescorted. Individuals not possessing the proper security clearance must be escorted by an authorized "L" or "Q" cleared person who ensures measures are taken to prevent the compromise of classified matter.

- **Protected Area (PA)**

This security area has been established to protect up to Category II quantities or greater of Special Nuclear Material (SNM). The PA provides concentric layers of security of the MAA. Only authorized personnel are permitted to enter and exit. Unescorted access must be controlled to limit entry to individuals with an appropriate security clearance and the need-to-know. Individuals without the appropriate security clearance must be escorted. The escort must ensure measures are taken to prevent compromise of classified matter or access to SNM. At PANTEX, access to the PA requires a badge with "Q" security clearance **AND HRP** designator for unescorted access.

- **Material Access Area (MAA)**

This security area has been established to protect Category I quantities of SNM. Access must be controlled to limit entry to individuals with an appropriate security clearance and who have been authorized for entry consistent with need-to-know and operations. Individuals without appropriate security clearance must be escorted.

At PANTEX, access to the MAA requires a badge with "Q" security clearance **AND HRP** designator for unescorted access

- **Exclusion Area**

This security area has been established to protect information or material where an individual's mere presence may result in access to classified matter.

At PANTEX, access to the exclusion area requires a badge with "Q" clearance **AND HRP** designator for unescorted access.



# EO13:

## IDENTIFY ESCORTING RESPONSIBILITIES

**Escort:** An authorized individual who has the responsibility of accompanying personnel who lack the access authorization within a security area to ensure adherence to security measures.

**General Requirements for Escorts:**

- Must be "L" or "Q" cleared (as appropriate for the area)
- Knowledgeable of security interests to be protected
- Ensure measures are taken to prevent unauthorized access (physical, visual, auditory), of classified matter
- Must not be performing work that will distract from escort responsibilities
- Ensure escorted personnel wear badge in plain view above the waist and on the outer clothing
- Maintain visual contact with escorted personnel at all times, and in a position to control their movements/actions
- Report (by secure means) any potential compromises of classified information to the PSS (Y-12) or IOSC (Pantex) as soon as practical.

**Y-12 Escorts:**

May be conducted by Y-12 employees or a trained and qualified subcontractor employee

## **Pantex Escorts:**

There are three different types of escorts at Pantex:

- **Administrative**

- a. Required for uncleared individuals to have access to the LA
- b. Escort completes required training

- **HRP**

- a. Required for "Q" cleared individuals who are not HRP certified requiring access to the PA/MAA
- b. Escort must be "Q" cleared, HRP Certified, Pantex employee
- c. Coordination with access control required

- **Security Police Officer**

- a. For uncleared performing work in LA/PA/MAA
- b. For "Q" cleared, non-HRP performing work in the PA/MAA
- c. For uncleared or "L" cleared persons requiring PA/MAA access
- d. For visitor group, regardless of clearance level, that will be cocooned" into the PA/MAA
- e. Coordination with Access Control required
- f. Coordination with Construction Management required

Pantex escorts CANNOT be related to those being escorted.

# EO14:

IDENTIFY SPECIAL NUCLEAR MATERIAL PROTECTION  
REQUIREMENTS

CNS is required to account for the nuclear material under its control. The Nuclear Materials Control and Accountability (NMC&A) department is responsible for tracking and controlling these materials through complex-level policies and procedures.

### **Methods of Control**

There are various methods of material control or surveillance methods used to maintain the accountability of special nuclear material. The methods are designed to detect unauthorized activities that could result in diversion or theft.

Some examples are: vaults, security cameras, tamper-indicating devices, daily administrative checks and the two-person rule. Process monitoring is also being introduced in selected areas to allow immediate discovery of errors that could contribute to the inventory difference.

# EO15:

IDENTIFY THE PURPOSE AND RESPONSIBILITY OF THE  
SF-312, CLASSIFIED INFORMATION NONDISCLOSURE  
AGREEMENT

The SF312 is a contractual agreement between the U.S. Government and you, a cleared employee, in which you agree to never to disclose classified information to an unauthorized person.

The primary purpose of the SF-312 is to inform you of:

- The trust that is placed in your by providing you access to classified information
- Your responsibilities to protect that information from unauthorized disclosure
- The consequences that may result from your failure to meet those responsibilities

Additionally, by establishing the nature of this trust, your responsibilities, and the potential consequences of noncompliance in the context of a contractual agreement, if you violate that trust, the United States will be better able to prevent an unauthorized disclosure or to discipline you for such a disclosure by initiating a civil or administrative action.

The SF 312 was revised in July 2013 by the Office of the Director of National Intelligence to conform to two new federal statutes:

- The Financial Services and General Government Appropriations Act (Public Law 112-74)
- The Whistleblower Protection Enhancement Act (WPEA) (Public Law 112-119)

## **The Whistleblower Protection Enhancement Act (WPEA)**

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.

### **Your Responsibility**

If you have already signed an SF312, you will not be required to sign another; however, you should be familiar with the Executive Orders and statutory provisions that take precedence in cases of conflict with the nondisclosure agreement.



## PERSONNEL SECURITY ELEMENTS

# EO16:

IDENTIFY THE PURPOSE OF THE PERSONNEL SECURITY PROGRAM

The Department of Energy (DOE) Personnel Security Program establishes requirements that ensure DOE's missions are accomplished in a secured environment by men and women in whom both DOE and the American people may place their complete trust and confidence.

# EO17:

IDENTIFY THE SOURCES OF LEGAL AUTHORITY AND  
GUIDANCE

- Executive Order 13526, Classified National Security Information, dated 12-9-09
- Title 10 Code of Federal Regulations, Part 710, (10 CFR, 710), Criteria and Procedures for Determining Eligibility for Access to Classified Material or Special Nuclear Material
- DOE Order 472.2 Chg 2, *Personnel Security*
- DOE Order 475.1, Counterintelligence Program

# EO18:

DESCRIBE THE ACCESS AUTHORIZATION PROCESS

Processing an applicant for a security clearance involves several steps and personnel security personnel. Security clearances and access authorizations denote an individual's eligibility for access to a particular type of classified information or material, such as National Security Information, Restricted Data, Formerly Restricted Data, or Special Nuclear Material. In determining such eligibility, DOE may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security.

An individual's eligibility is based on the completion of a personnel security investigation conducted for DOE by the Office of Personnel Management (OPM), the Federal Bureau of Investigation (FBI) or Other Government Agency (OGA) authorized to conduct background investigations.

# EO19:

IDENTIFY KEY TERMS ASSOCIATED WITH ADJUDICATIONS

The following adjudicative guidelines are established for all U.S. government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees, and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs, and are to be used by government departments and agencies in all final clearance determinations.

GUIDELINE A: Allegiance to the United States

GUIDELINE B: Foreign Influence

GUIDELINE C: Foreign Preference

GUIDELINE D: Sexual Behavior

GUIDELINE E: Personal Conduct

GUIDELINE F: Financial Considerations

GUIDELINE G: Alcohol Consumption

GUIDELINE H: Drug Involvement

GUIDELINE I: Psychological Conditions

GUIDELINE J: Criminal Conduct

GUIDELINE K: Handling Protected Information

GUIDELINE L: Outside Activities

GUIDELINE M: Use of Information Technology Systems



# EO20:

IDENTIFY THE ADJUDICATION FACTORS

The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the individual is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines.

The adjudication process is the careful weighing of a number of variables known as the whole-person concept. Available, reliable information about the person, past, and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

- The nature, extent, and seriousness of the conduct
- The circumstances surrounding the conduct, to include knowledgeable participation
- The frequency and recentness of the conduct
- The individual's age and maturity at the time of the conduct;
- The extent to which participation is voluntary
- The presence or absence of rehabilitation and other permanent behavioral changes
- The motivation for the conduct
- The potential for pressure, coercion, exploitation, or duress
- The likelihood of continuation or recurrence

Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent recurring pattern of questionable judgement, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole-person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

# EO21:

IDENTIFY DUE PROCESS

When applicants and employees are determined not to meet the standards for access to classified information, the cognizant personnel security office will initiate the Administrative Review process. The Administrative review process is initiated when an individual's eligibility for security his or her security clearance has been suspended or cannot be granted due to unresolved security concerns.

The administrative review process give the individual the opportunity to submit written information and/or to appear before a DOE hearing officer. These procedures are established to ensure that an individual is afforded full due process in a manner consistent with traditional American concepts of justice and fairness.

Title 10 Code of Federal Regulations, Part 710, Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material.

# EO22:

IDENTIFY INDIVIDUAL REPORTING REQUIREMENTS

All individuals applying for or in possession of a DOE security clearance must truthfully provide all information requested for personnel security purposes. All individuals have a specific obligation to report personnel security-related matters as they occur, whether related to themselves or to other individuals applying for in the possession of a DOE security clearance.

The following personnel-security related matters should be reported verbally and directly immediately upon becoming aware of the situation or incident and in no event later than two (2) working days after the event (Y-12). Immediate written and verbal notification must be made within one (1) working day to the Pantex Reporting Official.

***NOTE: If the situation being reported involves drugs, alcohol or an alleged violence, notify CNS BEFORE reporting to work.***

- Legal action effected for a name change
- Change in citizenship
- Any arrests, criminal charges (including charges that are dismissed), citations, tickets, summons, or detentions by Federal, State, or other law enforcement authorities for violations of law within or outside of the U.S.

NOTE: Traffic violations for which a fine up to \$300 was imposed DOES NOT have to be reported unless the violation was alcohol or drug related

- An immediate family member assuming residence in a sensitive country
- Hospitalization for mental health reasons or treatment for drug or alcohol abuse
- Employment by, representation of, or other business related association with a foreign or foreign-owned interest or non-U.S. citizen or other individual who is both a U.S. citizen and a citizen of a foreign country
- Personal or business related filing for bankruptcy
- Garnishment of wages
- Any approach by an individual seeking unauthorized access to classified information or SNM, or any other potentially CI related incident, in accordance with DOE O 475.1, *Counterintelligence Program*
- Foreign Travel (Reported to CI)

The following must be reported within 45 days (unless there is a name change. If a name change occurred, then the two day notification applies)

- Marriage/cohabitation (DOE F 5631.34, Data Report on Spouse/Cohabitant form must be completed)

To report at Y-12 during normal business hours:  
Personnel Security 865.574.7196

To report at Y-12 after normal business hours:  
PSS Office 865.574.7172

To report at Pantex during normal business hours:  
Pantex Reporting Official 806.477.7205

To report at Pantex after normal business hours:  
Pantex Operations Center 806.477.5000



## COUNTERINTELLIGENCE REPORTING REQUIREMENTS

# EO23:

IDENTIFY TARGETING AND RECRUITMENT METHODS OF  
FOREIGN INTELLIGENCE SERVICES

## The Recruitment Cycle:

A systematic approach, which can be used as a "social cultivation". The adversary will target individuals of interest using the five step recruitment cycle below:

You, are now an individual of interest because you have access to CNS facilities, which provides you with access to information.

- **Spot:** This could occur at a conference, seminar overseas or here in the U.S.
- **Assess:** They will attempt to learn about you. Your habits, hobbies, political views, or any issues you may have going on at work.
- **Recruit:** You will be asked to help them by providing them with information that you have access to. They may blackmail you, or offer you a sum of money.
- **Handle:** They will use you to provide the desired information that you have access to.
- **Termination:** You may no longer have access to the information or they no longer need that information

This recruitment cycle has been proven very successful for adversaries over the years.

# EO24:

IDENTIFY COUNTERINTELLIGENCE REPORTING  
REQUIREMENTS

All CNS employees and non-employees are required to report the following to counterintelligence:

- Official or unofficial travel outside of the United States
- Travel to countries where you intend to have or have had discussions with sensitive country foreign nationals regarding sensitive subjects. This would include travel known in advance to involve meetings with sensitive country foreign nationals or chance meetings where there are foreign nationals from sensitive countries in attendance.
- Foreign National-anyone who is not a U.S. citizen by birth or naturalization
- Sensitive Countries-Countries may be designated as sensitive based on reasons of national security, nuclear non-proliferation, regional instability, threat to national economic security, or terrorism concerns.

All travel to any country when area determined to be sensitive subjects will be discussed.

- Any substantive professional, substantive personal, or substantive or enduring financial relationships with foreign nationals affiliated with sensitive countries.
  - **Enduring Relationship**-one that has existed or is expected to exist for a substantial period of time (months or years).
  - **Substantive Relationship**-one that is enduring and involves substantive sharing of personal information and/or the formation of emotional bonds.
- Any contacts with foreign nationals who make requests that could be attempts at exploitation or elicitation. Examples are:
  - Requests for documents or information that is viewed by the traveler as unexpected or unrelated to the purpose of the interaction
  - Requests for the traveler to transport back to the U.S. any package(s) or letter(s) for mailing in the U.S.
  - Requests of any kind that cause the traveler to feel uncomfortable or call into question the purpose of the request
  - Professional contacts and relationships with sensitive country foreign nationals, whether they occur at one's worksite or abroad
  - Any foreign travel for which foreign monetary support is provided, whether to a sensitive or non-sensitive country
- Requests for unauthorized access to classified or otherwise sensitive information

## **Who Should You Contact If You Have Counterintelligence Questions?**

### **Y-12**

Edgar (Chip) Myers, Oak Ridge Field Office: [edgar.myers@cns.doe.gov](mailto:edgar.myers@cns.doe.gov) or 865.241.1519

Selin Warnell, Oak Ridge Field Office: [warnells@ornl.gov](mailto:warnells@ornl.gov) or 865.574.6770

### **Pantex**

Michael Lowe 806.477.5361

Amanda Hammer 806.477.5312

Bruce Johnston 806.477.3631

Michelle Abell 806.477.5374

E-mail: [CI@cns.doe.gov](mailto:CI@cns.doe.gov)

## PROHIBITED AND CONTROLLED ARTICLES

# EO25:

## IDENTIFY PROHIBITED ARTICLES

Prohibited articles are not permitted on U.S. Department of Energy (DOE)-controlled property, nor are they allowed to be stored in personally or government-owned vehicles while those vehicles are on the Y-12 National Security Complex (Y-12) or Pantex Plant (Pantex) site.

Prohibited articles include items such as explosives; dangerous weapons, instruments or material likely to produce substantial injury to persons or damage to persons or property; controlled substances (e.g., illegal drugs and associated paraphernalia but NOT prescription medication); and other items prohibited by law.

- **Alcohol**-Includes, but is not limited to beer, liquor, wine, or other intoxicating beverages.
- **Controlled Substances** (e.g., illegal drugs and associated paraphernalia but not prescription medication)-Prescription medication taken under the direction of a medical provider is not considered a prohibited article if it is brought on-site for the sole use of the prescription holder. The individual must be able to produce evidence of the prescription if requested. **(Pantex employees prescribed medication must inform Medical of medication use.)**
- **Dangerous Weapons**-Per Title 18, "Crimes and Criminal Procedures", Section 930, "Possession of firearms and dangerous weapons in Federal facilities", the term "dangerous weapon" means a weapon, device, instrument, material, or substance animated or inanimate, that is used for or is readily capable of, causing death or serious bodily injury. Such instruments include, but are not limited to, switchblade knives, guns, pellet/air guns, blackjacks, brass knuckles, archery equipment, nightsticks, batons, and martial arts weapons and equipment.



Prohibited articles are not permitted on U.S. Department of Energy (DOE)-controlled property, nor are they allowed to be stored in personally or government-owned vehicles while those vehicles are on the Y-12 National Security Complex (Y-12) or Pantex Plant (Pantex) site.

Prohibited articles include items such as explosives; dangerous weapons, instruments or material likely to produce substantial injury to persons or damage to persons or property; controlled substances (e.g., illegal drugs and associated paraphernalia but NOT prescription medication); and other items prohibited by law.

- **Explosives**-an explosive in any chemical compound or mechanical mixture designed to function as an explosive or a chemical compound that functions through self-reaction as an explosive and which, when subjected to heat, impact, friction, shock or other suitable initiation stimulus, undergoes a very rapid chemical change with the evolution of large volumes of highly heated gases that exert pressures in the surrounding medium. The term applies to materials that either detonate or deflagrate, including unauthorized ammunition.
- **Instruments or material likely to produce substantial injury to persons or damage to persons or property**-Such material includes incendiary devices, which are any self-contained devices intended to create an intense fire that can damage normally flame-resistant or flame retardant materials.
- **Road flares**-Over-the-road and heavy-equipment truck drivers or personal vehicles are permitted to possess no more than five road flares as part of a vehicle's emergency inventory.

# EO26:

## IDENTIFY CONTROLLED ARTICLES

Controlled articles are items that are permitted on DOE-controlled property but restricted from use in specified security areas. These items are identified as controlled items as they require conditional restrictions. Items are identified as controlled articles because of the potential for use in recording or transmitting information without authorization.

Examples of controlled items include portable electronic devices (both government and personal owned); recording equipment (e.g. audio, video, optical, infrared, or data); electronic equipment with data exchange port capable of being connected to automated information system equipment; cellular telephones and smart phones (Droid, Blackberry, iPhone, EVO, Rogue); e-readers; MP3-type devices; iPod; iPad; netbooks, laptop computers; radio-frequency transmitting equipment; and other associated media.

While controlled items such as cell phones or portable electronic devices may be permitted at CNS facilities, personnel may not use cell phones or portable electronic devices while operating a motor vehicle under any of the following situations, regardless of whether a hands-free device is used:

- When operating a motor vehicle owned, leased, or rented by the Company/U.S. Government.
- When operating a personal motor vehicle within the Pantex Plan/Y-12 National Security Complex, and/or off-site/leased facilities.
- When the cellular telephone or portable electronic device is Company owned, leased or rented regardless of motor vehicle or location.
- When using a cellular telephone or portable electronic device to conduct Company business regardless of motor vehicle or location.

Use of cellular telephone or portable electronic device is defined as, but is not limited to:

- Answering or making telephone calls
- Engaging in telephone conversations
- Reading, sending, or responding to emails and text messages
- Accessing the Internet

In an emergency, drive to a safe location, pull over, and put the motor vehicle in Park before calling to report an emergency.

Employees who violate this policy will be subject to disciplinary action, up to and including employment termination (E-POL-1021).

## Y-12 Controlled Article Policy

*Use scrollbar to view document.*



**Pantex Controlled Items-The following items are allowed on-site at Pantex but MUST remain in personal vehicles in the Property Protection Area.**

- Cameras –At no time are pictures to be taken anytime on the plant site with any type of personal camera.
- Computers not owned by Pantex (EXCEPTION; given on a case by case basis by the ISSM or his designate)
- Laptops/notebooks
- Media players (iPods)
- Tablets, pads and slates (i.e., iPads)
- Game devices (i.e. PSP, Playstation, Xbox, Nintendo)
- Any other devices with a processor and storage
- Computer components
- Cellular Wireless Cards
- Wireless cards (Exception: wireless cards used for pool laptops in transit between 16-19 and your car)
- Bluetooth cards, devices or adapters
- Any other computer component or peripheral
- Global Positioning System-(e.g., portable transmit/receive)
- On-Star
- Personal software
- Radio frequency devices (exception: key fobs are allowed except in Nuclear Explosive Areas)
- Recording devices (optical, video, audio or data)
- XM or Sirius radio receivers with recording capabilities
- Any privately owned device, electronic or optical, capable of recording, processing, storing or transferring audio, computer data, video or photos. (Only if Bluetooth capability can be disabled).
- Lighters
- Electronic Cigarettes
- Mace/Pepper Spray