

2017

ANNUAL

SECURITY

REFRESHER

BRIEFING



U.S. DEPARTMENT OF
ENERGY

Integrated
Support
Center

Welcome!



The purpose of the Annual Security Refresher Briefing is to remind you of your safeguards and security responsibilities and to promote continuing awareness of good security practices.

Per DOE Order 470.4B, Attachment 3, Section 3:

Individuals who possess DOE access authorizations are required to complete refresher briefings. These mandatory refresher briefings are implemented each calendar year at approximately 12-month intervals.



About the Briefing



The content of this Annual Security Refresher Briefing is organized into eight sections.

Section 1: Security Badges and Identification of Prohibited & Controlled Articles

Section 2: Classified Matter Protection and Control (CMPC)

Section 3: Controlled Unclassified Information (CUI)

Section 4: Classification

Section 5: Incidents of Security Concern

Section 6: Technical Surveillance Countermeasures (TSCM) & Operations Security (OPSEC)

Section 7: Personnel Security

Section 8: Counterintelligence

You will see references to a [Resource Library](#) that provides an acronym list and links to documents and web sites referenced throughout this briefing. Select the link at any time during the briefing to view and/or print useful information.

Section 1

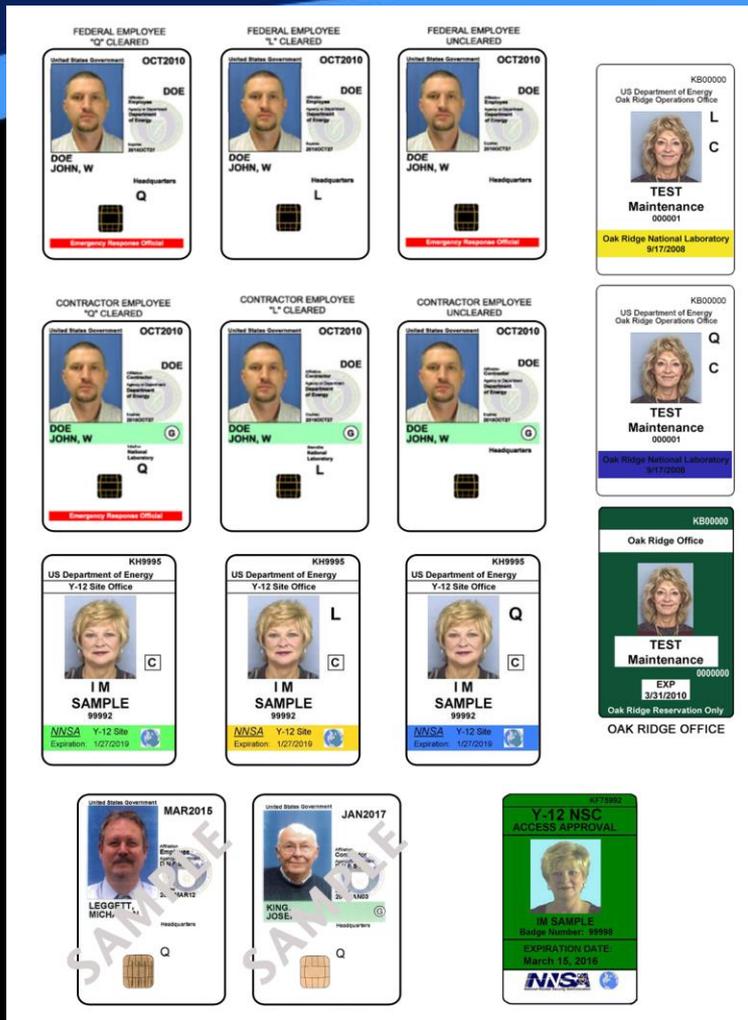
In Section 1, “Security Badges and Identification of Prohibited and Controlled Articles,” you will:

- Recall important responsibilities regarding your security badge
- Recognize “Prohibited Articles” on a DOE site
- Identify Controlled Articles and limits placed on them

What will I learn?

Security Badges and Identification of Prohibited and Controlled Articles

Security Badges control Access



SECURITY BADGES should be:

- Worn at all times while on site
- Conspicuously
- Photo Side Forward
- Above the Waist
- On the Front Side of the Body

Contact information for Badging may be found in
the
[Resource Library](#).

Badge Reminders



Remember these important points about your security badge:

Your badge must be replaced or reissued in these cases:

- Changes in your name
- Significant changes in your physical appearance
- Your badge becomes faded or damaged

Badge cautions:

- It is illegal to counterfeit, alter, or misuse your badge
- **DO NOT** allow your badge to be photographed or photocopied
- **DO NOT** wear the badge in public places
- **DO NOT** use your badge as identification for non-governmental activities

Other badge reminders:

- Protect your badge, report loss or theft of your badge within 24 hours
- Your badge is the property of DOE and must be returned to the Badge Office when:
 - the badge has expired
 - the badge is no longer required, or
 - you are terminating employment

Prohibited Articles



Based on federal laws, regulations, and DOE directives, certain articles are prohibited on DOE property (including facilities, parking lots, roads, and grounds).

The following articles are prohibited:

- Dangerous weapons and explosives (instruments or materials likely to cause substantial injury to people or damage property)
- Non-government-owned firearms (even if you have a gun carry permit)
- Alcoholic beverages (authorization for special events and celebrations is required)
- Controlled substances such as illegal drugs and associated paraphernalia (lawfully prescribed medicine is permitted)
- All items that are prohibited by law and/or regulations



Controlled Articles



To guard against the potential for loss or compromise of classified information, certain items are NOT ALLOWED in Security Areas (i.e. Limited Areas, Vault Type Rooms, Protected Areas, Material Access Areas, or other designated sensitive areas) without authorization from the cognizant security office.

The following are such *Controlled Articles*:

- Laptop or tablet computers
- BlackBerry devices
- Two-way pagers
- Cell phones
- Cameras of all kinds
- Recording equipment
- Digital audio players (iPod, Zune)
- Wearable electronic devices such as Bluetooth, FitBit, Jawbone and “smart” watches



Check signs in controlled areas for additional information.

Controlled Articles (continued)



You may be able to use a controlled item outside of a building but not take it into the building. If you are uncertain, then do not introduce the item into the facility. Remember, introduction of any controlled article into security areas could trigger an Incident of Security Concern (IOSC) which could result in the issuance of a Security Infraction or Violation.

Authorization for use of such devices in one security area does not apply to all other security areas.



Section 2

Classified Matter Protection and Control (CMPC)

- To protect and control classified information/documents
- Prevent unauthorized access
- Provide an audit trail for such documents, where required.

What will I learn?

Identification Of Classified Matter



CLASSIFIED INFORMATION Any knowledge that can be communicated or documentary information/material, regardless of its physical form or characteristics that has been determined pursuant to executive order, regulation or statute to meet classification requirements. (DOE O 471.6) Any information that has been determined pursuant to Executive Order 13526, or successor Orders, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and that is so designated.

CLASSIFIED MATERIAL is defined as a chemical compound, metal, fabricated or processed item, machinery, electronic equipment and other equipment or any combination thereof containing or revealing classified information.

CLASSIFIED MATTER is defined as any combination of documents (paper or electronic) and materials.

CMPC – Levels of Classified Information



Classified information is designated by both a classification level and a category.

The classification level is based on how much our national security could be damaged if the information were to be released to unauthorized person(s).

There are three classification levels:

- **Top Secret** - Information which, if disclosed to unauthorized persons, could cause exceptionally **grave damage** to national security.
- **Secret** – Information, which, if disclosed to unauthorized persons, could cause **serious damage** to national security.
- **Confidential** - Information which, if disclosed to unauthorized persons, **could cause damage** to national security.



CLASSIFICATION LEVELS
CONFIDENTIAL SECRET TOP SECRET

CMPC

Categories of Classified Information

The classification **category** describes the type of information contained in the material.

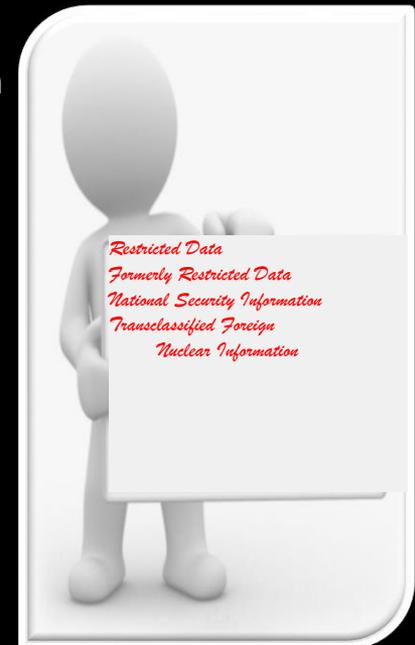
There are four classification categories:

Restricted Data (RD)- Information that is related to the design, manufacturing, and utilization of atomic weapons; production of special nuclear material; or use of special nuclear material in the production of energy.

Formerly Restricted Data (FRD) - Information that pertains to the military utilization of atomic weapons and has been removed by DOE from the Restricted Data category.

Transclassified Foreign Nuclear Information (TFNI) - Information concerning the atomic energy programs of other nations that has been removed from the Restricted Data category for use by the intelligence community and is safeguarded as NSI under Executive Order 13526. *Contact your site Classification Officer if you have information that is or may be TFNI.

National Security Information (NSI) - Information that requires protection in the interest of national defense or foreign relations of the United States that is not related to nuclear weapon design, manufacturing, testing, or utilization.



CMPC – Access to Classified Matter



Access to Classified Matter must be limited to persons who possess appropriate access authorization, have a need to know for the performance of official duties, and have signed an SF-312.

Access is not obtained or granted by position only.

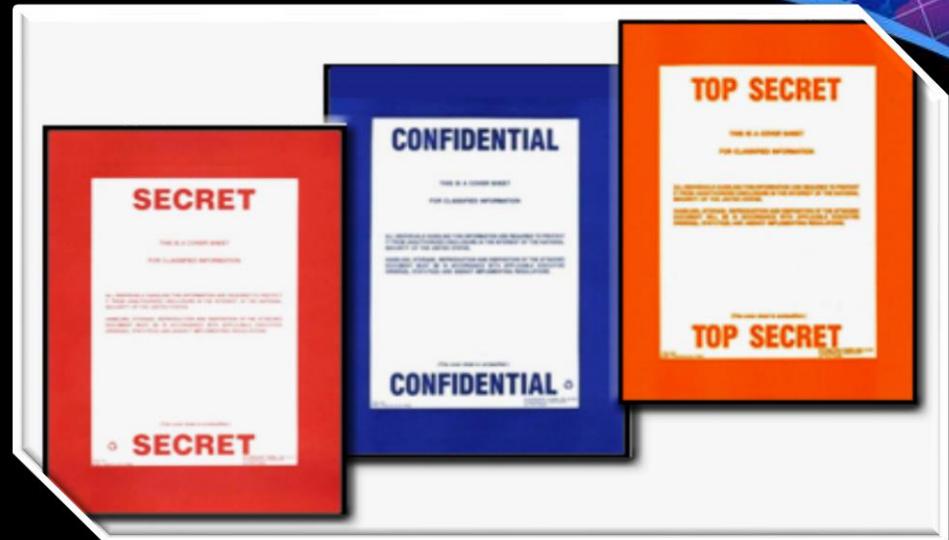
The level and category of classified matter to which a person has a need for access determines the access authorization, “Q” or “L”, that is granted to a person based on their duties. These relationships are summarized by the table below:

	Restricted Data	Formerly Restricted Data	National Security Information/TFNI
Top Secret	Q	Q	Q
Secret	Q	Q or L	Q or L
Confidential	Q or L	Q or L	Q or L

CMPC

WHAT DOES CLASSIFIED LOOK LIKE?

Cover sheets (pictured) must be used any time a classified document is removed from a security container/repository/safe (includes a security area such as a vault, or vault-type room). The purpose of a classified cover sheet is to prevent unauthorized visual access, serve as an immediate identifier that the attached document or material is classified, and to identify the classification level of the document.



Contact information for Classified Matter Protection and Control may be found in the [Resource Library](#).

WHAT DOES CLASSIFIED LOOK LIKE?

COMPACT DISCS



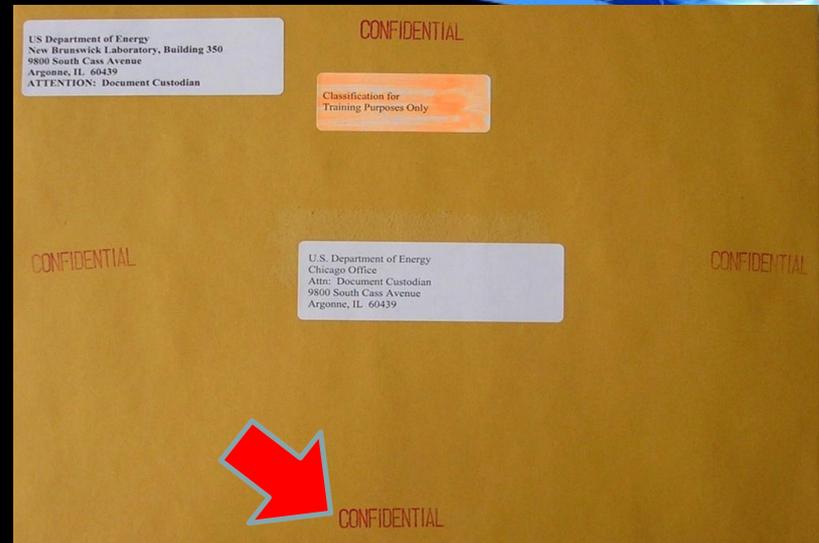
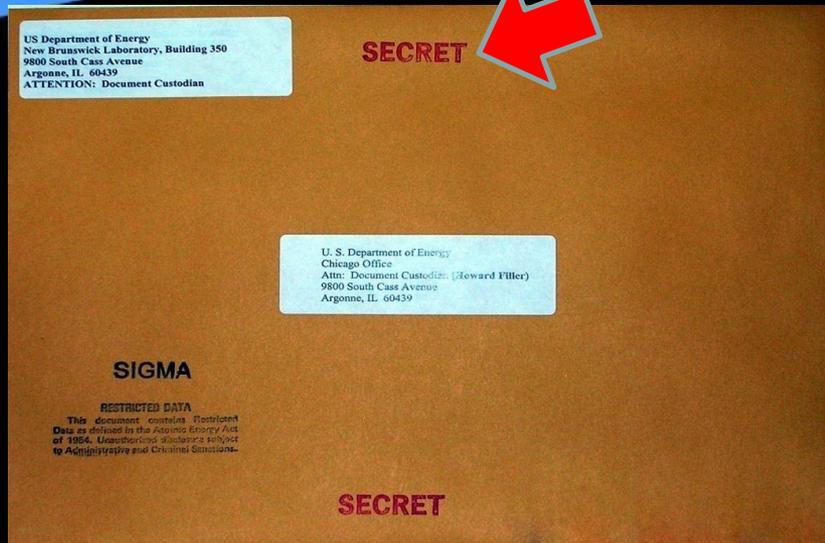
MEDIA LABELS



Examples of "Electronic Media"

- Compact Disks
- Tape Drives
- Hard Drives

TRANSMITTAL ENVELOPES



If you receive or find a package or letter through normal channels and discover an interior envelope marked like the examples

DON'T OPEN IT!

Protect the envelope/document and call your local Security Office

Protection and Control Measures (continued)



Handling and Marking of Draft documents or Working Papers

Classified working papers and drafts are considered to be interim production stages toward the generation of a final document. Hard copies of working papers and drafts must contain the following markings:

- Date created.
- Highest potential overall classification level of the draft or working paper at the top and bottom of the outside of the cover page (if any), on the title page (if any), on the first page of text, and on the outside of the back cover or last page. Each interior page of a classified document must be marked at the top and bottom with the highest potential classification level of that page (including unclassified) or the overall classification of the document.
- The overall category (if RD or FRD) of the draft or working paper must be marked on the cover page (if any), title page (if any), or the first page of text. The category marking is not required on draft and working paper interior pages that contain RD or FRD information.
- Annotation “Draft” or “Working Paper” must be marked on the front cover along with the date created and/or modified.
- Any applicable caveats or special markings must be annotated on the cover page (if any), title page (if any), or the first page of text.

CMPC – Protection and Control Measures (continued)



Security markings for a final (finished) document must be applied when a draft or working paper or draft meets any of the following requirements:

- Released by the originator outside the activity, office, etc.
- Top Secret retained for more than 30 days from the date of origin.
- Secret or Confidential retained for more than 180 days (i.e., 6 months) from the date of origin.
- It will no longer be revised

CMPC – Protection and Control Measures (continued)



- Classified information may only be shared or communicated in a location approved for classified discussions and only by approved secure/classified means (e.g., secure telephone or secure fax).
- Ensure that electronic documents are properly marked, protected and reviewed for classification prior to distribution.
- Any document, report, presentation, briefing, etc. regarding a potentially classified subject area must be reviewed for classification by a Derivative Classifier.

For additional protection and control measures, including training/briefing, contact your site CMPC Point of Contact (POC) or Classification Officer *listed in the [Resource Library](#).*

CMPC – Protection and Control Measures **(continued)**



Printed output from a classified information system must be reviewed by a Derivative Classifier to determine the appropriate classification unless:

1. The output is a final document that has already been reviewed and is appropriately marked;
2. The printed output is a working paper that is:
 - A. properly marked at the highest potential level and category or
 - B. marked and protected at the highest level and category of information resident on the system; or
3. The program is 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.

WHAT ARE MY RESPONSIBILITIES?



As an individual with a security clearance, the following incidents regarding CMPC need to be reported:

- ✓ Any classified media/matter outside of a Security Area.
- ✓ Any unauthorized disclosure of classified information/matter to an individual without a security clearance and need-to-know.
- ✓ Any discussion/reproduction/ transmission/generation/destruction of classified documents/matter outside of an approved Security Area or by unauthorized individuals (no security clearance or need-to-know).

CMPC

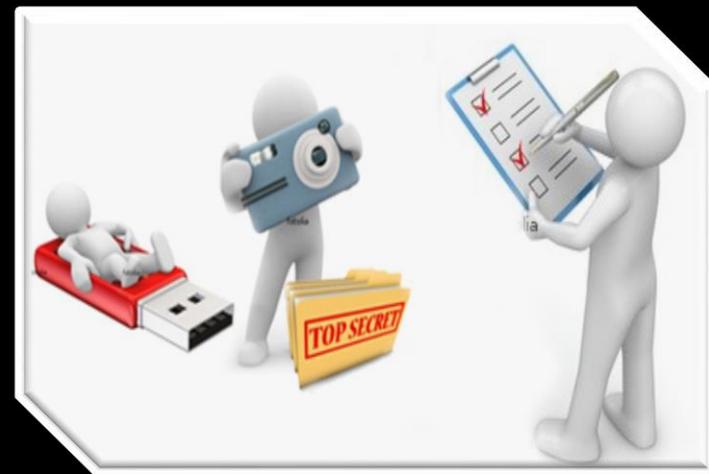
Accountable Classified Matter



Certain Classified Matter (i.e., paper, electronics, parts) requires stricter controls to prevent unauthorized access to or removal of it. These controls include a system of procedures that provide an audit trail and a chain of custody that is referred to as “accountability.”

Accountable classified documents include:

- North Atlantic Treaty Organization documents
- United Kingdom documents
- Certain “Special Access Required” documents
- Sensitive Compartmented Information
- Other documents as directed by program managers or as stipulated in contracts.



Section 3

In Section 3, “Controlled Unclassified Information,” you will:

- Define types of Controlled Unclassified Information (CUI)
- Recognize controls for protecting CUI from unauthorized disclosure
- Describe appropriate methods for transmittal of CUI

What will I learn?

Controlled Unclassified Information

Controlled Unclassified Information



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

Many other Statutes and Executive Orders govern the protection of information (e.g., FOIA, Privacy Act, etc.)

CUI includes, but is not limited to

- **Official Use Only (OUO)**
 - Personally Identifiable Information (PII)
 - Export Control Information (ECI)
- **Unclassified Controlled Nuclear Information (UCNI)**

Information (UCNI)

- Unclassified Controlled Nuclear

Protecting Controlled Unclassified Information



ACCESS—A person granted routine access to CUI must have a **need to know** the specific information in the performance of official or contractual duties. Because CUI is unclassified, **an access authorization (L or Q) is not required**; however, recipients must be **advised of the protection requirements**. Unless specifically authorized, foreign nationals are not allowed access to ECI and UCNI.

STORAGE—CUI must be protected at all times from unauthorized disclosure or unauthorized access by individuals without a need to know. Consult the site Classification Officer for CUI storage requirements.

MARKING—CUI must be marked in compliance with DOE and site directives prior to dissemination. Consult the site Classification Officer for CUI marking requirements.

REPRODUCTION—CUI may be reproduced without permission of the originator. Reproduction shall be limited to the minimum number of copies necessary consistent with the need to carry out official duties. Reproduced copies shall be marked and protected in the same manner as the original document. A copy machine malfunction must be cleared, and all paper paths must be checked for CUI material.



Transmission of Controlled Unclassified Information



Email:

CUI must be protected when transmitted electronically. Requirements and means to accomplish this protection vary site to site. Generally speaking, protection will involve encryption or the use of a document password. DOE uses *Entrust* for encryption. Consult the site Classification Officer for CUI electronic protection requirements.

Fax:

When faxing CUI, the sender must contact the recipient prior to faxing the document and make a follow-up call to confirm that the entire document was received. UCNI must be sent via a secure telephone facsimile.

Mail:

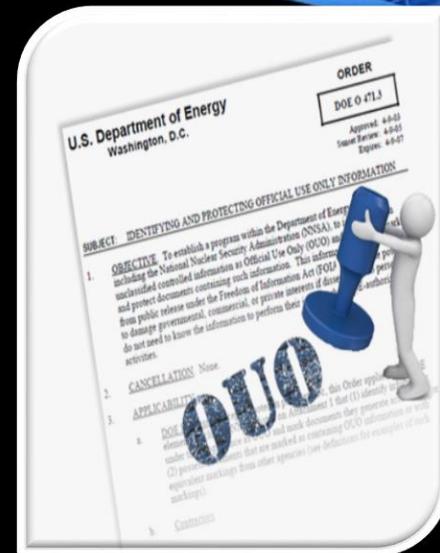
Place documents in a sealed opaque envelope or wrapping marked with "To Be Opened by Addressee Only." The document may be mailed off site using first class, express, certified, or registered mail, or sent via any commercial carrier.



Official Use Only

To be identified as **Official Use Only (OUO)**, information must be unclassified and must meet the following criteria:

- ✓ No clearance required
- ✓ Reasonable precautions to prevent unauthorized access
- ✓ Mailed in a sealed opaque envelope marked
- ✓ **“To Be Opened by Addressee Only”**
- ✓ Copies kept to a minimum
- ✓ Destroy with strip-cut shredder (1/4” or less)
- ✓ Transmit electronically by secure means when possible
- ✓ The use of this coversheet is optional but good business practice



OUO has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not "need to know" the information to perform their jobs or other DOE-authorized activities.

OUO falls under at least one Freedom of Information Act (FOIA) exemption.

Requirements for identification, protection, and control of OUO are found in the DOE O 471.3 Admin Chg 1, Identifying and Protecting Official Use Only Information

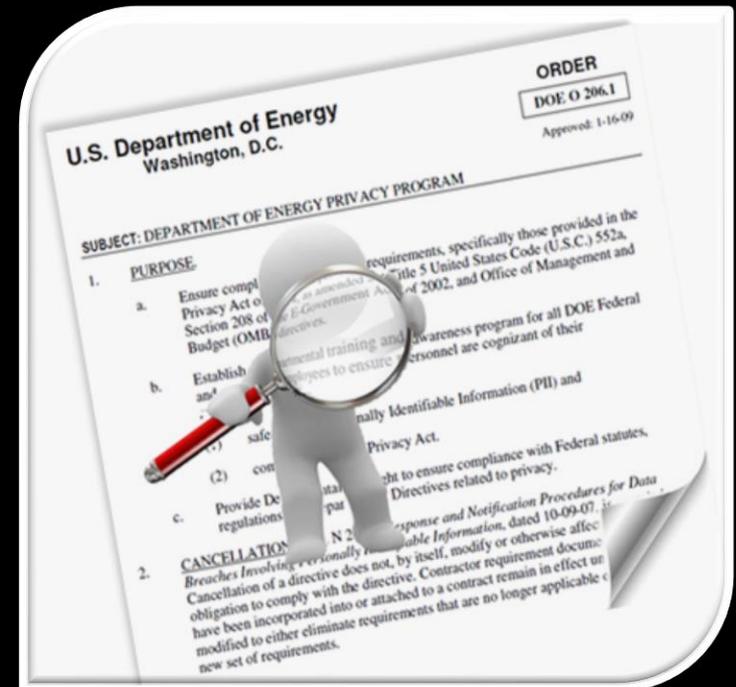
Personally Identifiable Information



One type of OUO information you may encounter is **Personally Identifiable Information (PII)**. (PII is marked and protected as OUO, Exemption 6, Personal Privacy)

PII is any information maintained by DOE, contractors, or subcontractors about an individual, including but not limited to:

- Education
- Financial transactions
- Medical history
- Criminal or employment history
- Information that can be used to distinguish or trace an individual's identity, such as his/her name, social security number, date of birth, place of birth, mother's maiden name, biometric data



Export Control Information

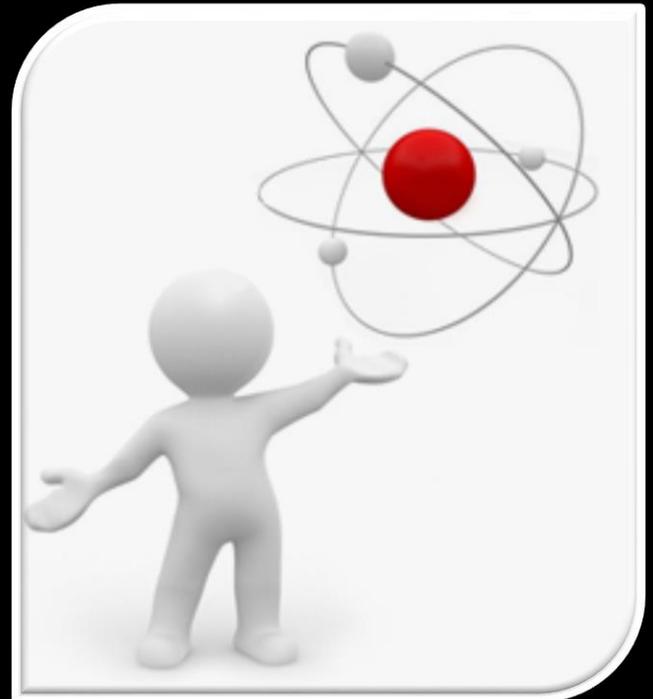


Another type of OUO information is **Export Control Information (ECI)**.

ECI is defined as unclassified technical information whose export is subject to export control and whose unrestricted public dissemination could help potential adversaries of the United States.

All nuclear technologies and most other technologies are controlled by the United States with respect to foreign nationals—both those in and out of the United States.

ECI is marked and protected as OUO, Exemption 3, Statutory Exemption. The ECI marking must appear adjacent to the OUO marking on the first page of documents.



Section 4

Classification Program

Classification is the identification of information that needs to be protected in the interest of national security.

All classified matter is protected according to federal statutes and presidential Executive Orders. DOE is responsible, under the Atomic Energy Act of 1954, for classifying information and material relating to atomic energy and its use in weapons and under executive orders for other aspects of national security.

Classifying establishes protective barriers that ensure that classified information and material do not fall into unauthorized hands. Through the process of classification, we protect important information from adversaries, yet allow the same information to be used by scientists, statesmen, military planners, and others with applicable access authorization and who meet the need-to-know criterion.



What will I learn?

Classification

CLASSIFICATION



CAN I CLASSIFY DOCUMENTS? NO!!

Employees called Derivative Classifiers (DCs) have a security clearance, the proper training, and have been formally granted authority by the delegated Classification Officer to make classification determinations.

The classifier (DC) derives his or her determination based on written classification guidance.

These guides enable the DC to correctly identify what information requires protection.

Who is the Program Point of Contact?

The *Classification Office* telephone number is listed in the [Resource Library](#).



ORIGINAL CLASSIFICATION AUTHORITY



An original determination occurs when information is classified by an original classifier in accordance with **NATIONAL SECURITY INFORMATION EXECUTIVE ORDER 13526**, when there are no source documents or guides to cite as a basis for classification.

Original classification authority resides within the government because the original decision sets policy.

Contractor employees can not make original classification determinations.

Classification – Responsibilities



Documents or material potentially containing classified information must be reviewed for classification to ensure that such information is identified for protection.

Obtain DC review of these documents:

- ✓ Newly generated documents or material in a classified subject area that may contain classified information
- ✓ Existing unmarked documents or material that may contain classified information
- ✓ Existing documents or material believed to contain information that should be classified at a higher level or more restrictive category
- ✓ Newly generated documents that contain extracts from an existing classified document (e.g., a chapter or an appendix)



Documents or material in a classified subject area intended for public release (e.g., for a webpage, Congress, etc.) require review by your site Classification Officer.

Classification – Declassification and Downgrading



Declassification is the determination that classified information (document or material) no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure. The classification designation is removed or cancelled with this determination.

If you believe currently marked classified matter should be declassified or downgraded (i.e., you believe the information belongs in a lower classification level or category), DOE encourages and expects you to contact your site Classification Officer (CO) to begin the declassification/downgrading process.

Only appropriately trained/approved Derivative Declassifiers may remove markings from a classified document.

Classification – “No Comment” Policy



Authorized holders of classified information shall not confirm, deny, or expand upon 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.

Public Domain

- In newspapers, magazines, websites, books, speeches, TV, etc.
- No comment on accuracy, classification, or technical merit of **classified information**.
- Fact of appearance of classified information is classified at same level and category as the information.



Examples of Comments

- Statement of an opinion on the status of the information.
- Confirmation of the classification status.
- Disseminating of a public domain source by email.
- Discussing the information on the telephone.
- Anything that lends credibility to the status of the information.

Classification – Challenges to Classification

Although authority for making classification determinations rests with a DC, each employee is encouraged and expected to challenge the classification of information, document, or material that he or she believes is improperly classified. Under no circumstance is the employee subject to retribution for making a challenge. Challenges should be directed to the classification Point-of-contact in the [Resource Library](#)

However, employee must be advised he or she may submit a formal challenge directly to the Director, Office of Classification (OC) at any time and there will be no retribution

Director, OC coordinates formal challenges with cognizant CO, Program Classification Officer (PCO) and responds within 60 days

NSI Appeals

Director, OC responds within 60 days or notifies challenger if the response will be after 60 days. If no response is received within 120 days, challenger may forward challenge to ISCAP

If challenger is not satisfied, appeals to AU-1 who coordinates with NNSA, Chief of Defense Nuclear Security, when appropriate

If AU-1 does not respond within 90 days or employee is not satisfied, employee may forward challenge to Interagency Security Classification Appeals Panel (ISCAP)

RD/FRD

If employee not satisfied, appeals to AU-1 who coordinates with NNSA, Chief of Defense Nuclear Security, when appropriate

No appeal to ISCAP



Section 5

Incidents of Security Concern (IOSC)

Per DOE Order 470.4B, Attachment 5, you are required to report IOSCs immediately. An IOSC occurs any time there is a potential or actual loss or compromise of Classified Matter or Controlled Unclassified Information (CUI) or when a security rule is violated. Examples include:

- An e-mail may contain classified information
- Improper storage of unclassified controlled information
- Theft or vandalism of government property

IOSCs should be reported to your site security office personnel either in person or by phone.

What will I learn?



More about Incidents of Concern

Upon discovery of a potential IOSC, take immediate action to report it to your site security office personnel in person or by secure means (e.g., secure phone) and take reasonable steps to contain the incident, protect the scene, and secure any classified or CUI matter, as appropriate.

In most cases, an inquiry is conducted into an IOSC to establish the pertinent facts and circumstances, determine root cause, identify corrective actions, and take administrative actions, as appropriate. Administrative actions can result in the issuance of a security infraction or disciplinary action in accordance with DOE or an employer's personnel practices.



Reporting Incidents of Security Concern



You are also required to report IOSCs immediately, upon discovery, to prompt a graded response, which includes an assessment of the potential impacts, appropriate notification, extent of condition, and corrective actions. An IOSC occurs any time there is a potential or actual loss or compromise of Classified Matter or Controlled Unclassified Information (CUI) or when a security rule is violated.

ISOCs should be reported to your site security office personnel either in person or by secure phone.



The telephone number for reporting IOSC is listed in the [Resource Library](#).

Section 6

TSCM & OPSEC

In this section, you will:

- Become familiar with the Technical Surveillance Countermeasures (TSCM) Program
- Read the appropriate response to discovery of a technical surveillance device
- Recall how the principles of Operations Security are applied
- Identify ways you can support Operations Security

What will I learn?

Technical Surveillance Countermeasures



Technical Surveillance Countermeasures (TSCM) is a counterintelligence program that is designed to detect, deter, isolate, and nullify technologies that are intended to obtain unauthorized access to classified information and CUI.

The technologies range from simple, mechanical means to sophisticated electronic and fiber-optic techniques. The more common techniques include:

- Hidden audio and radio-frequency transmitting devices (microphones),
- Telephone bugging equipment, and
- Visual tools such as binoculars, telescopes, mini cams, and fiber-optic cameras.

The sale of these devices is not restricted. They are readily available to anyone on the commercial market.



Technical Surveillance Countermeasures (continued)



If you discover what you consider to be a technical surveillance device,

- Do not voice the discovery within the immediate area, which includes the suspect room and all other rooms that are above, below, and adjacent to it
- Immediately **cease all activity in the area** (as discreetly as possible)
- **Secure the room and do not touch or remove the device**
- Immediately **notify your TSCM POC** using secure communications outside the area where the suspected device has been found. During off-shift hours, notify the site security office personnel.



NOTE: Information pertaining to an actual or suspected technical penetration is classified. Notifications must be made in person or by secure means.

The TSCM points of contact are listed in the [Resource Library](#).

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM)



The TSCM Program helps to protect information from:

**FOREIGN
GOVERNMENTS**



**INDUSTRIAL
COMPETITORS**



**DISGRUNTLED
EMPLOYEES**



ACTIVISTS



INSIDERS



TERRORISTS



Operations Security (OPSEC)

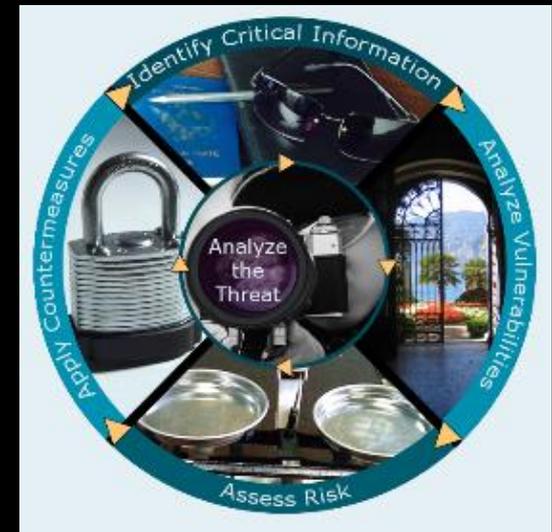


OPSEC is an analytical process used to deny an adversary's access to sensitive (generally unclassified) information and to prevent unauthorized disclosure.

The process consists of five basic questions.

1. What is my critical information?
2. What are the threats to my information?
3. How is my information vulnerable?
4. What is the risk involved, considering threats and vulnerabilities from an adversary?
5. How can I apply countermeasures to protect my Information?

The OPSEC process is cyclical and tailored to the specific organization and activity being analyzed. It allows viewing from a friendly and adversary perspective.



**OPSEC doesn't replace "traditional" security programs...
it supplements them.**



OPSEC Begins With You

- Use encryption and virtual private network connections to transmit CUI
- Use appropriate markings on CUI and classified correspondence
- Watch for ways in which an adversary can collect information in an open environment (e.g. overheard conversations, notes left in plain sight)
- Guard against phone calls, emails, and text messages seeking personal or sensitive information
- Do not discuss CUI or classified information in public
- Limit distribution of CUI to those with a need to know
- Destroy CUI using approved methods

**See ISC OPSEC SharePoint site for further information:
<https://intranet.osc.doe.gov/sites/ISCOPSEC/Pages/Home.aspx>**

Section 7

PERSONNEL SECURITY

- The Adjudicative Process
- Legal Authority
- Security Clearance Process
- Security Concerns
- Reporting requirements

What Will I Learn?



U.S. DEPARTMENT OF
ENERGY

Integrated
Service
Center



THE ADJUDICATIVE PROCESS



The adjudicative process is an examination of a sufficient period of a person's life or "Whole-Person Concept" to make a determination that the person is an acceptable security risk.

Congress has set forth the criteria Personnel Security Specialists look at when weighing the risks of granting someone access to National Security Information. The criteria was developed by analyzing the history of persons who have done serious harm to the National Security of the United States.

Adjudicative Guidelines were also developed to help Specialists address security concerns or help to mitigating these concerns. These guidelines include topics such as foreign preference or influence, drug use, alcohol consumption, emotional, mental, and personality disorders, and financial considerations to name a few.

Another important consideration is a person's honesty, judgment, and reliability. While some security concerns can be mitigated over time and with professional treatment, falsification or lying by omission on a security form or during an interview with a security professional is seen as a concern that is hard to mitigate.

Legal Authority



Legal Authority to collect information and to adjudicate access authority (security clearances) comes from Federal Statutes, Regulations, Executive Orders and DOE Directives and Orders:

Federal Statutes

“Atomic Energy Act of 1954”

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)

Federal Regulations

“Criteria and Procedures for Determining Eligibility for access to Classified Matter or Special Nuclear Material” (10 CFR 710)

Executive Orders

EO 12968

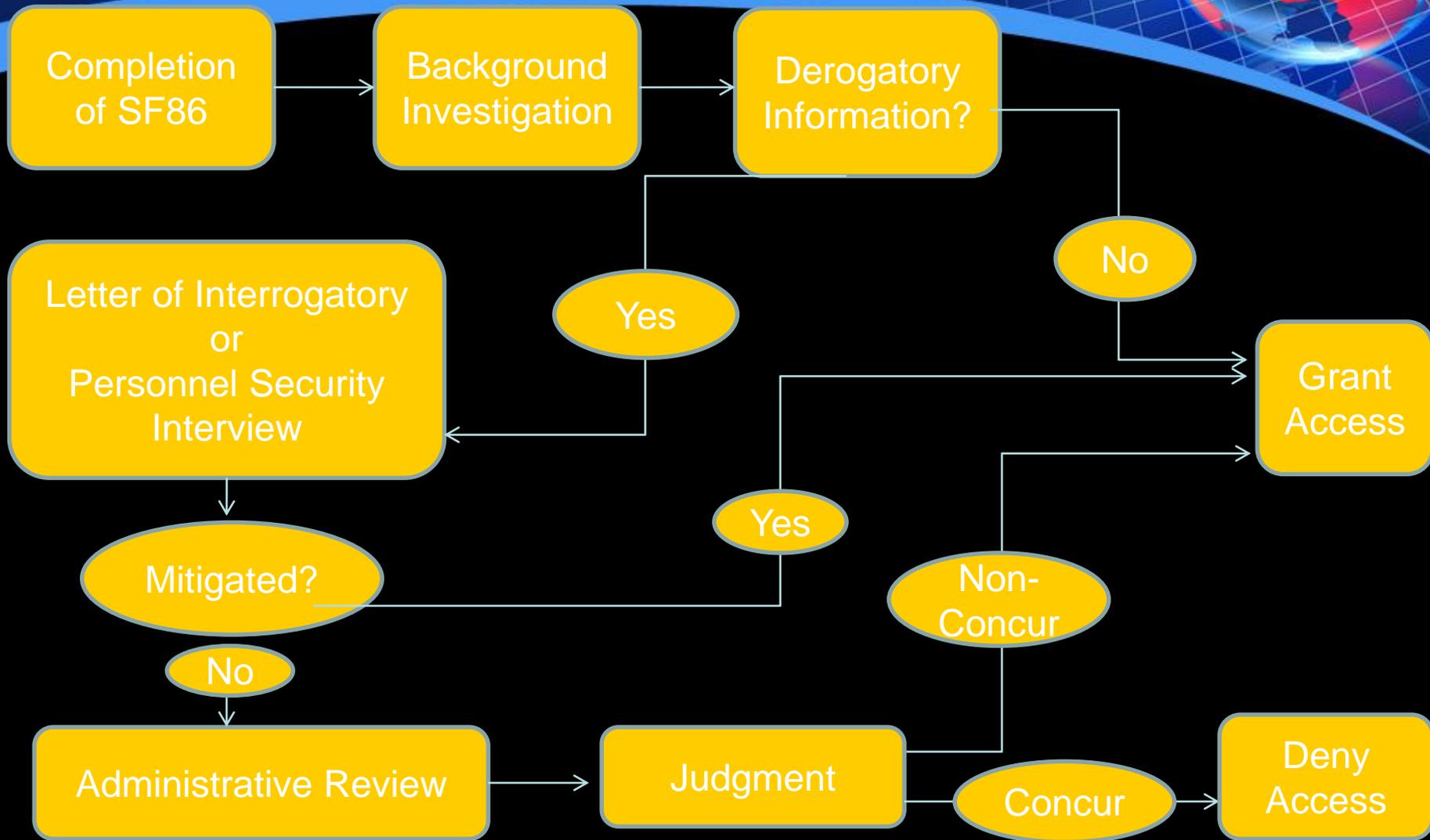
DOE Directives/Orders

DOE Order 470.4B Admin Chg. 1, Safeguards and Security Program

DOE Order 472.2 Chg. 1, Personnel Security

Adjudicative Guidelines 2014

SECURITY CLEARANCE PROCESS



SECURITY CLEARANCE PROCESS



Security Clearances or Access Authorization will not be granted and should not be requested or maintained for following reasons:

- ✓ To avoid the use of access controls or physical barriers.
- ✓ To alleviate individual or management responsibilities for properly protecting classified information or SNM.
- ✓ Establish a pool of employees with pre-existing security clearances.
- ✓ Accommodate an individual's personal convenience, expedience, gain or advantage.
- ✓ Anticipate unspecified classified work.
- ✓ Determine suitability for Federal employment or fitness for contractor employment.

Reporting Personal Information



Once you hold a security clearance or access authorization, you are required to **IMMEDIATELY** notify your local Security Office of following:

- ✓ Any information that raises doubts about another employee's continued eligibility for access to classified matter.
- ✓ Any approaches or contacts by anyone attempting to obtain unauthorized access to classified matter or Special Nuclear Material.
- ✓ Any classified matter which has or may have been lost or compromised.



Reporting Personal Information



When you completed your original Questionnaire for National Security Positions (QNSP) or Electronic Questionnaire for Investigative Process (e-QIP), and when a renewal of your clearance was requested, you were made aware of your responsibility to report certain personal information. Those reporting responsibilities are **ONGOING**.

An individual (e.g., employee, contractor, subcontractor) who holds a clearance or is in the process of obtaining a clearance is **required** to report certain personal information (contained in next slide).

This personal information must be reported within **2 days by phone and 3 days by written notification**, unless noted otherwise, to your Personnel Security Office.

The Personnel Security points of contact are listed in the [Resource Library](#).



Reporting Personal Information

Report these Occurrences/Changes:

Criminal Charges

All criminal charges, including felony, misdemeanor, public, and petty offenses as defined in the statutes of any state

Traffic Violations

Any traffic violations for which you receive a fine of \$300 or more, or **any traffic violation that is alcohol or drug-related regardless of the amount**

Hospitalization

Hospitalization for treatment of mental illness or other mental condition; treatment for alcohol or drug abuse; any condition that may cause a significant impairment in judgment or reliability.

Wage Garnishment

All wage garnishments, including, but not limited to, divorce, delinquent debts, or child support

Name Changes

All legal name changes

Emotional or Psychological Issues

Report If treatment is required



Arrests

All arrests, including charges that are dismissed

Detention by Law Enforcement

Any detention by federal, state, or other law enforcement authority for violation of law, except detention for a simple traffic stop

Ongoing Contact with Foreign Nationals

Employment, business, and personal associations with any foreign national or employees/representatives of a foreign-owned interest

Bankruptcy or Excessive Indebtedness

Any personal or business-related bankruptcy

Change in Marital/Cohabitation Status

Report within 45 days

Change in Citizenship

US citizen who changes citizenship or acquires dual citizenship

An immediate family member who assumes residence in a sensitive country

CLARIFICATION ON MEDICAL MARIJUANA



Many people are confused about the legality of medical access to marijuana. The passage of state initiatives in recent years has intensified this confusion and places many people at risk.

Marijuana, for any use, is illegal under federal law. Even if you live in a state that has enacted legislation or passed a ballot initiative that recognizes marijuana's medical utility, use of illegal drugs on or off duty by federal and/or contractor employees in positions with access to sensitive information is not allowed because it may pose a serious risk to national security and is inconsistent with the trust placed in such employees as servants of the public.

The Department of Justice issued guidance making it clear that no state can authorize violations of federal law, including violations of the Controlled Substance Act, which identifies marijuana as a Schedule I controlled drug. Moreover, IRTPA, as amended, specifically prohibits a federal agency from granting or renewing a clearance to an unlawful user of a controlled substance.

Section 8

**In Section 6, “Counterintelligence,”
you will:**

- Describe the foreign intelligence threat
- Recall how intelligence is collected
- Identify counterintelligence information to be reported
- Describe the “insider threat”
- Identify potential indicators of espionage activities

What will I learn?

Counterintelligence

Counterintelligence

The Foreign Intelligence Threat

DOE, the National Nuclear Security Administration (NNSA), and contractors of those agencies are the guardians of some of our nation's most closely held and vital secrets, products, and technology. As such, we are targets of extreme interest by foreign powers seeking to acquire those secrets.

The information you hold as a member of the workforce is valuable to almost any foreign intelligence service in the world. Foreign intelligence services want to know everything about what we are doing and how our facilities function so that they can exploit that information.



Foreign Intelligence Threat to DOE



Foreign governments, foreign intelligence services, and foreign companies – including those based in the U.S. – have the potential to harm DOE's interests through espionage, sabotage, or ...



Intelligence Collection



To obtain needed information from foreign countries, governments maintain professional intelligence and security services.

ALMOST EVERY COUNTRY HAS THESE SERVICES.

Intelligence organizations task their employees, and sometimes private citizens, to collect US information of value in these areas:

- Military/defense (classified information)
- Political
- Economic
- Science/technology (even if later published, to get a head start)
- Business (sensitive, proprietary, intellectual property)

Intelligence Collection (continued)



Traditional collection methods still use foreign agents, traitors, listening devices, and satellite surveillance. However in today's environment, we must also be alert to more overt methods of collection.

Events such as international conferences, conventions, and trade fairs attract foreign scientists and engineers. These venues can provide foreign intelligence collectors a group of specialists on a key topic of interest. In addition to obtaining available literature, intelligence collectors use these opportunities to elicit information and identify personnel who can be targeted for further contact.

Research activities may be exploited during foreign travel, while hosting foreign visitors or assignees, or by other means of international collaboration or joint ventures.

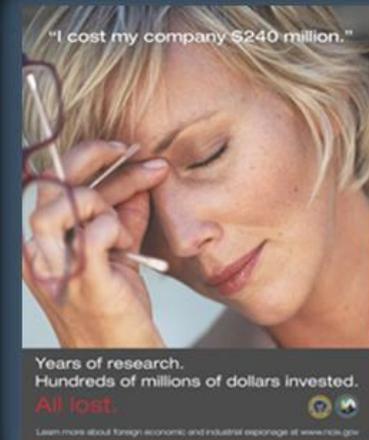


The Threat Is REAL



Factors that increase the possibility that YOU or other DOE employees will be targeted

- ✓ Your access to information, people, or places of interest
- ✓ International or domestic travel where foreign intelligence organizations can gain access to you
- ✓ What you place on your social networking profiles may attract the attention of foreign intelligence organizations



Protecting DOE Sensitive Information and Technology

In the past four years, nearly 100 individual or corporate defendants have been charged by the US Justice Department with **stealing trade secrets or classified information** from private industry and US Government agencies and providing them to foreign entities...

Washington Post Article – March 25, 2013 Peter Finn



The Insider Threat

Risk of betrayal of trust does not depend upon the presence of a foreign adversary. It depends only upon an insider with the opportunity to betray some combination of character weaknesses and situational stresses, and a trigger that sets the betrayal in motion. The insider is a major threat to national security, using his or her access to programs, systems, people, and facilities and knowledge of security protocols to obtain information.

As a general rule, four preconditions must be present before a disaffected or troubled employee commits a serious betrayal of trust such as espionage:

1. **Ability to overcome inhibitions** For example, moral values, fear of being caught, and loyalty to employer or co-workers.
2. **Trigger** - Something that sets the betrayal in motion.
3. **Motive** or a need to be satisfied through the crime.
4. **Opportunity** to commit the crime.



THE INSIDER THREAT
DANGER FROM WITHIN

THE MOM AND POP NUKE SHOP

Leo & Marjorie Mascheroni

In September of 2010, Pedro "Leo" Mascheroni and his wife Marjorie Mascheroni were indicted and charged with conspiracy to communicate and communicating Restricted Data to an individual with the intent to secure an advantage to a foreign nation, as well as conspiracy to convey and conveying classified information. Leo Mascheroni was a Ph.D. physicist who worked at the Los Alamos National Laboratory (LANL) from 1979 to 1988. Marjorie Mascheroni worked at LANL between 1981 and 2010 as a technical writer. Both of the Mascheronis held a security clearance that allowed them access to classified information, including Restricted Data. Leo Mascheroni became frustrated with the United States Government because he believed his scientific ideas were superior to others and felt no one was listening to him. Leo Mascheroni reached out to an individual he believed was a representative of the Venezuelan government who promised him monetary compensation as well as providing him with the ability to conduct research in his way. Leo Mascheroni admitted that he unlawfully communicated Restricted Data with reason to believe the data would be used to secure an advantage for Venezuela. He also admitted to making false statements and unlawfully converting Department of Energy (DOE) information to his own use and selling the information. Marjorie Mascheroni pled guilty to conspiracy, making false statements, and conspiracy to communicate Restricted Data.

The investigation was conducted by the Federal Bureau of Investigation with the assistance of the DOE Counterintelligence Office. Both of the Mascheronis were sentenced to federal prison for their actions. U.S. Attorney Damon Martinez made the statement, "Those who work at our country's national laboratories are charged with safeguarding that sensitive information, and we must and will vigorously prosecute anyone who compromises our nation's nuclear secrets for profit."



The Insider Threat (continued)



There is no established formula for recognizing that someone is involved in espionage; however, certain situational factors or suitability issues can make an individual predisposed to volunteer or vulnerable to exploitation by foreign intelligence officers.

Behavioral and Suitability Issues	Socioeconomic Factors	Psychological Factors	Technological Trends
<ul style="list-style-type: none">• Substance abuse or dependence• Hostile, vindictive, or criminal behavior• Extreme, persistent interpersonal difficulties• Unreported foreign interaction• Gambling/lavish spending	<ul style="list-style-type: none">• Global market is expanding• Increased foreign interaction• Vulnerabilities (i.e., financial crisis)• Organizational loyalty is diminishing• Ethnic or religious ties• Moral justification	<ul style="list-style-type: none">• Narcissistic personality—i.e., a grandiose sense of their own importance—a sense of entitlement.• Sociopathic personality—i.e., lacking a sense of moral responsibility or social conscience	<ul style="list-style-type: none">• Developments in information technology make it much harder to control the distribution of information

Counterintelligence Reporting



To ensure that DOE and NNSA assets (people, information, and resources) are protected from foreign intelligence-gathering efforts, employees are required to report all potential espionage or terrorism concerns. Concerns should be promptly reported to the DOE Office of Counterintelligence.

Visit the Office of Counterintelligence web site (See [Resource Library](#)) for specific program information, detailed reporting requirements, and foreign travel and visit information as well as other counterintelligence concerns.

Report the following counterintelligence information:

- **Unusual solicitations**
- **Anomalies**
- **Contact with foreign nationals**
- **Foreign travel**

Counterintelligence Reporting (continued)

To ensure that DOE and NNSA assets (people and information) are protected from foreign intelligence-gathering efforts and potential espionage or terrorism concerns. Contact the DOE Office of Counterintelligence.

Visit the Office of Counterintelligence web site for program information, detailed reporting requirements, and other counterintelligence information as well as other counterintelligence information.

Report the following counterintelligence information:

Unusual solicitations

Anomalies

Contact with foreign nationals

Foreign travel

- Attempts by ANY unauthorized persons to gain access to classified information
- Situations that appear to be attempts by foreign intelligence services to enlist cooperation
- Inquiries regarding sensitive or classified information about your workplace, your official responsibilities, and/or activities and/or identities and activities of coworkers
- Contact with foreign nationals who make requests or statements that could be attempts at exploitation or elicitation
- Indicators of an Insider Threat

• Indicators of an Insider Threat

Counterintelligence Reporting (continued)



To ensure that DOE and NNSA assets (people, information, and resources) are protected from foreign intelligence-gathering efforts, employees are required to report all potential espionage or terrorism concerns. Concerns should be promptly reported to the DOE Office of Counterintelligence.

Visit the Office of Counterintelligence web site (See [Resource Library](#)) for specific program information, detailed reporting requirements, and foreign travel and visit information as well as other counterintelligence concerns.

Report the following counterintelligence

Unusual solicitations

Anomalies

Contact with foreign nationals

Foreign travel

A foreign power activity or knowledge, inconsistent with the expected norm, that suggests foreign knowledge of US national security information, processes, or capabilities

capabilities
information, processes, or

Counterintelligence Reporting (continued)



To ensure that DOE and NNSA assets (people, information, and resources) are protected from foreign intelligence-gathering efforts, employees are required to report all potential espionage or terrorism concerns. Concerns should be promptly reported to the DOE Office of Counterintelligence.

Visit the Office of Counterintelligence web site (See [Resource Library](#)) for program information, detailed reporting requirements, and foreign intelligence information as well as other counterintelligence concerns.



Report the following counterintelligence information:

Unusual solicitations

Anomalies

Contact with foreign nationals

Foreign travel

Professional, personal, and financial relationships with citizens of sensitive countries, including relationships that are maintained via the internet (e.g., email, chat rooms, social networking sites, internet dating)

networking sites, internet dating)

Counterintelligence Reporting (continued)



To ensure that DOE and NNSA assets (people, information, and resources) are protected from foreign intelligence-gathering efforts, employees are required to report all potential espionage or terrorism concerns. Concerns should be promptly reported to the DOE Office of Counterintelligence.

Visit the Office of Counterintelligence web site (See [Resource Library](#)) for specific program information, detailed reporting requirements, and foreign travel and visit information as well as other counterintelligence

Report the following counterintelligence

Unusual solicitations

Anomalies

Contact with foreign nation

Foreign travel



- All personnel (both cleared and uncleared) must attend a Counterintelligence Pre-Travel Briefing prior to traveling to sensitive countries (includes both business and personal travel)
- Travel to nonsensitive countries generally may also require a briefing especially if sensitive subjects or sensitive country nationals are involved

Potential Indicators of Espionage Activities



Your role as an employee is to be aware of potential espionage indicators and to report your concerns to the Office of Counterintelligence. In some cases your concerns might be based on a feeling that "something just isn't right." As a general rule, if something you observe just does not seem right, it probably should be reported. Working together, we can identify issues earlier, render assistance before the situation becomes irreversible, and ultimately protect the security of our mission. Indicators include:

- Disgruntlement
- An "above-the-rules" attitude
- Risk-taking behaviors
- Repeated impulsive behaviors
- Willingness to violate the rights of others to achieve one's own ends
- Conflicting loyalties to the US government
- Willingness to break rules or to violate laws and regulations
- Membership in any group that advocates the use of force or violence to cause political change within the United States



More Potential Indicators of Espionage Activities



- Statements or actions indicating an abnormal fascination with "spy" work
- Attempts to gain unauthorized access to classified or CUI
- Undue curiosity or requests for information about matters not within the scope of the individual's job or need to know
- Unauthorized removal of classified information
- Unusual work schedules
- Unexplained affluence
- Extensive use of copy, facsimile, or computer equipment; use that may exceed job requirements
- Frequent short trips to foreign countries or within the United States to cities with foreign diplomatic facilities for unusual or unexplained reasons
- Unreported foreign travel or foreign contacts
- Joking or bragging about working for a foreign intelligence service
- Behavior indicating concern that one is being investigated or watched, such as actions to detect physical surveillance
- Attempt to conceal any activity covered by one of these counterintelligence indicators



Terrorist Threats – Report Unusual Activity



You can help by being vigilant and aware of activities that could indicate possible domestic or international terrorist activities...



Did you **SEE** something suspicious
Commuting to work or grabbing
some lunch?

Then **SAY** something to appropriate
Authorities to make it right.

REPORT suspicious activity

For DOE related reporting
Contact OROC (865) 576-1005

For additional information contact a
DOE Security Awareness Coordinator
call: (865) 576-0916 or (865) 241-2302

**if you
SEE
something
SAY
something**

 ENERGY



Argonne

PREVENTING **TERRORISM** AT ARGONNE

BE VIGILANT

**Recognize These Indicators of
Potential Terrorist Activities...**

- Surveillance of the site, its employees, and activities
- Unusual and unexplained interest in personnel and technologies
- Attempts to gain site access by using false documentation
- Suspicious behavior such as nervousness or inappropriate clothing for the season
- Attempts to challenge security

**Report
Suspicious
Activities!**

Contact the Security and Counterintelligence Division
838-252-5731 or dial 911 in an Emergency

Terrorism ...The deliberate creation and exploitation of fear for bringing about political change... premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents..."

Congratulations!

You have completed the 2017 DOE Integrated Support Center Annual Security Refresher Briefing.



Remember, you can check out the [Resource Library](#) for additional information.

You may close this browser window. Your completion record will automatically be sent to your training office. Offsite Office personnel and Contractor personnel can print a copy of their completion record to provide to their training point of contact.

