

# HQ-111DE, Comprehensive Security Briefing

## 1. Introduction

### 1.1 Accessibility Statement

#### **ACCESSIBILITY**

This course has been optimized for accessibility.

If you are using a screen reader due to visual impairments, or if you use the computer keyboard instead of a mouse due to motor impairments, we recommend reviewing the [Accessible Navigation Instructions](#) to fully understand how to navigate the course with a screen reader and keyboard.

[Select here to continue.](#)

## 1.2 Intro Slide



Notes:

## 1.3 Navigation Instructions



Notes:

## 1.4 Course Instructions

### Course Instructions

| Length                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Credit                                                                                                                                                                                  | Completion                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>This course contains four chapters. It takes approximately 70 minutes to complete the course.</p> <p>If you need to stop before finishing, close the browser window.</p> <p>The Learning Management System (LMS) will:</p> <ul style="list-style-type: none"><li>• Report that the course is "In Progress" and bookmark your place.</li><li>• When you return, select the "Resume" option and the course will open at your last completed page.</li></ul> | <p>You must meet the following requirements to receive credit for the course:</p> <p>View all pages.</p> <p>Complete all activities.</p> <p>Complete the NTC Student Feedback Form.</p> | <p>When you have satisfied the requirements of this course, the LMS will automatically:</p> <ul style="list-style-type: none"><li>• Log your completion and add the completed course to your transcript.</li><li>• You can access your certificate from the LMS Transcript tab and print it or email it to your training point-of-contact or supervisor.</li></ul> |

Previous   Continue

Notes:

## 1.5 Main Menu



The screenshot shows a main menu titled "HQ Comprehensive Security Briefing". It lists four chapters, each with a chapter number in a circle, the chapter title, and a status icon on the right. Chapter 1 is highlighted in purple and has an unlocked icon (a circle with a dot). Chapters 2, 3, and 4 are in grey and have locked icons (a circle with a padlock). At the bottom, there are three buttons: "Previous" (with a left arrow), a document icon, and "Continue" (with a right arrow).

# HQ Comprehensive Security Briefing

- 1** Chapter 1  
Access to Unclassified and Classified Information (Unlocked)
- 2** Chapter 2  
Physical Security (Locked)
- 3** Chapter 3  
Classified Matter Protection and Control (CMPC) (Locked)
- 4** Chapter 4  
Personnel Security, Counterintelligence, and Legal Sanctions (Locked)

Previous [Document Icon] Continue

Notes:

## 1.6 Objectives



The screenshot shows a slide titled "Objectives:". Below the title, it says "In this briefing you will learn the following:" followed by a bulleted list of seven objectives. At the bottom, there are three buttons: "Previous" (with a left arrow), a document icon, and "Continue" (with a right arrow).

## Objectives:

In this briefing you will learn the following:

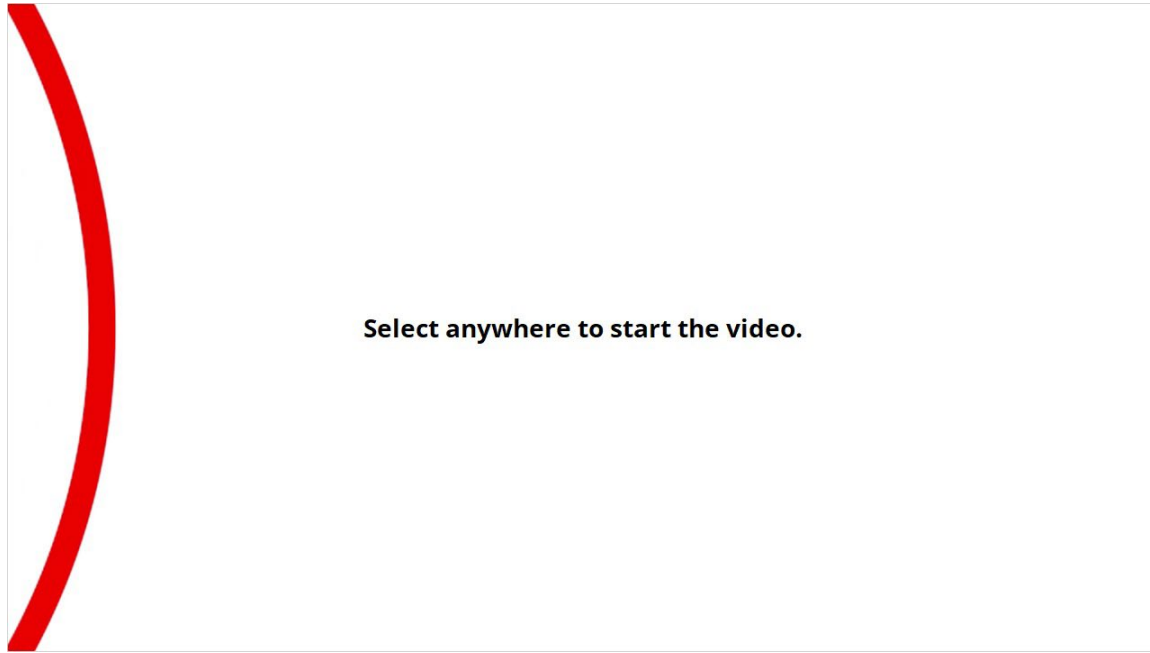
- The purpose of the DOE security program, specifically, basic classification security policies and principles.
- Classified information or matter protection elements.
- Personnel security elements.
- Counterintelligence threats and requirements.
- Individual responsibilities, to include what and when to report subjects impacting your ability to maintain a security clearance.
- Legal aspects for security clearance holders.

Previous [Document Icon] Continue



**Notes:**

## ***1.7 Responsibilities***

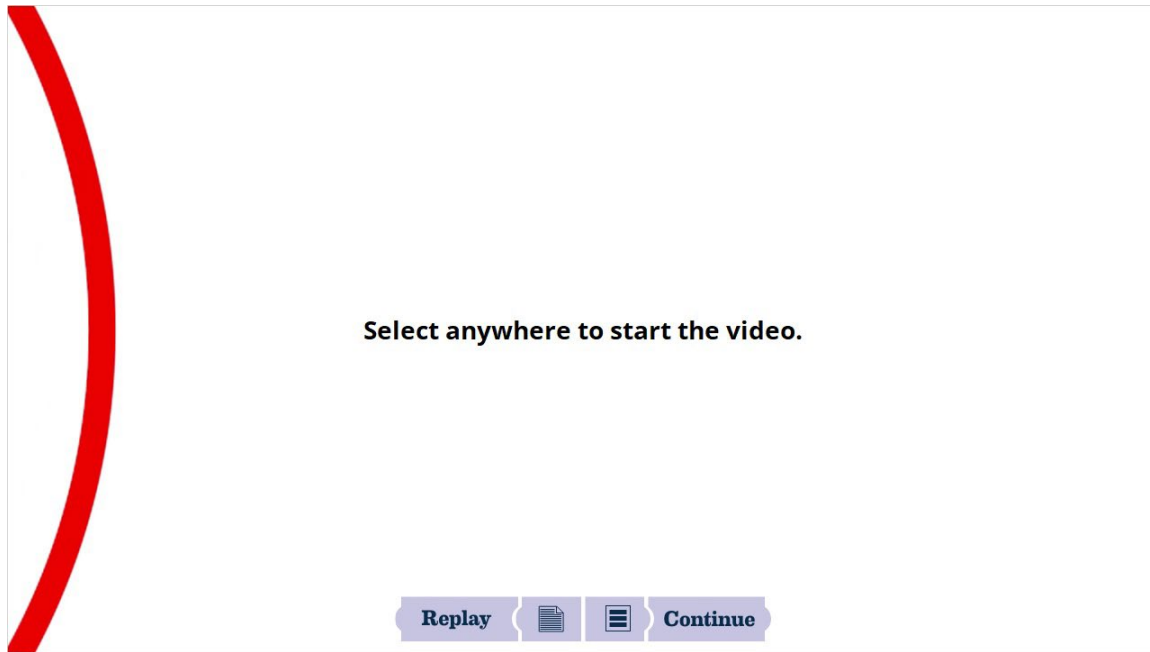


**Notes:**

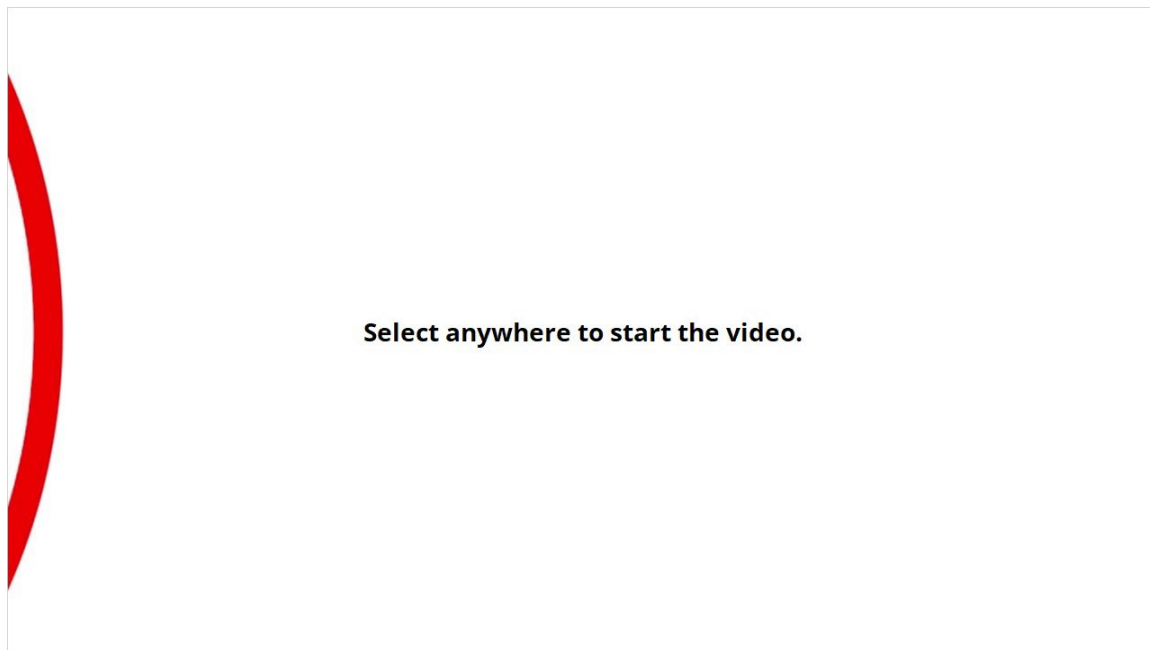
### **RESPONSIBILITIES**

As a Federal or contractor employee who has been granted a DOE security clearance, you're personally responsible for the proper use, handling, storage, and protection of Controlled Unclassified Information, or CUI, and Unclassified Controlled Nuclear Information (UCNI) in your possession. Keep in mind, a security clearance is not necessary for access to CUI or UCNI. The Head of Element is responsible for implementing a security program consistent with both DOE security directives and the requirements contained in the Headquarters Facility Master Security Plan (HQFMSP). However, as a matter of practice, these security responsibilities are delegated from each Head of Element to their Headquarters Security Officer (HSO). HSOs are security representatives who serve as points-of-contact for security-related matters within their organizations. It is imperative you know who your HSO personnel are.

## Replay (Slide Layer)



## 1.8 Congratulations Slide



### Notes:

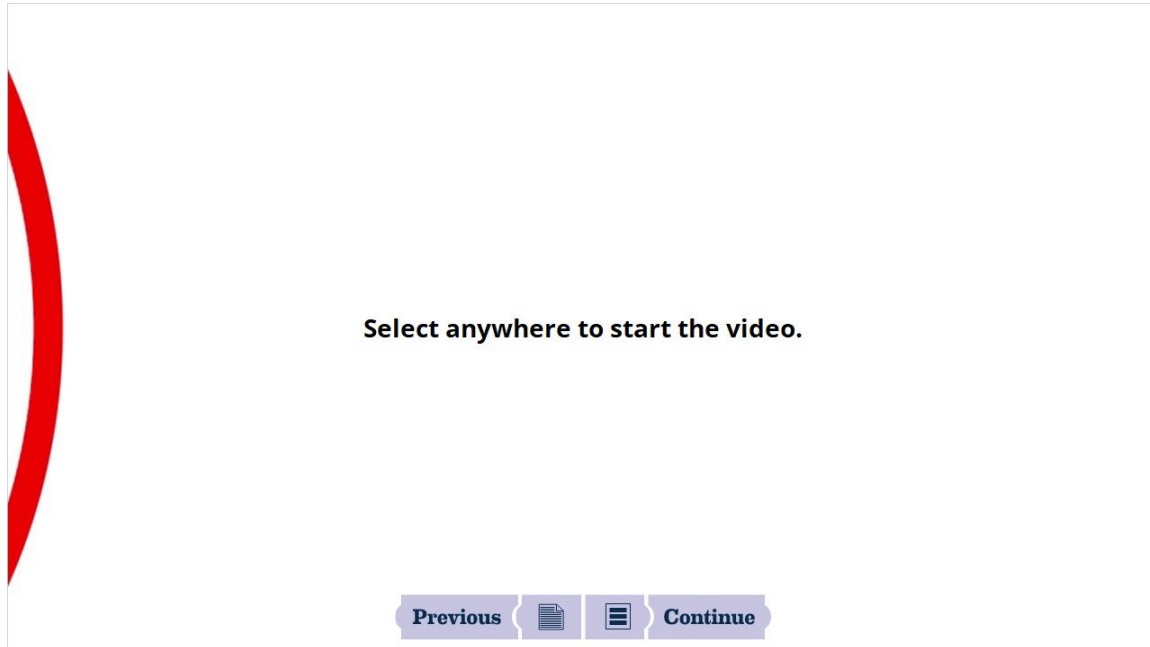
Congratulations. You've been issued a Department of Energy, or DOE, security clearance. Upon receipt of a Headquarters-issued security clearance and before you're granted initial access to classified information, you're required to complete a Comprehensive Security Briefing.

Guarding the national security of the U.S. is an integral requirement of the mission of DOE. Critical to this endeavor is the

---

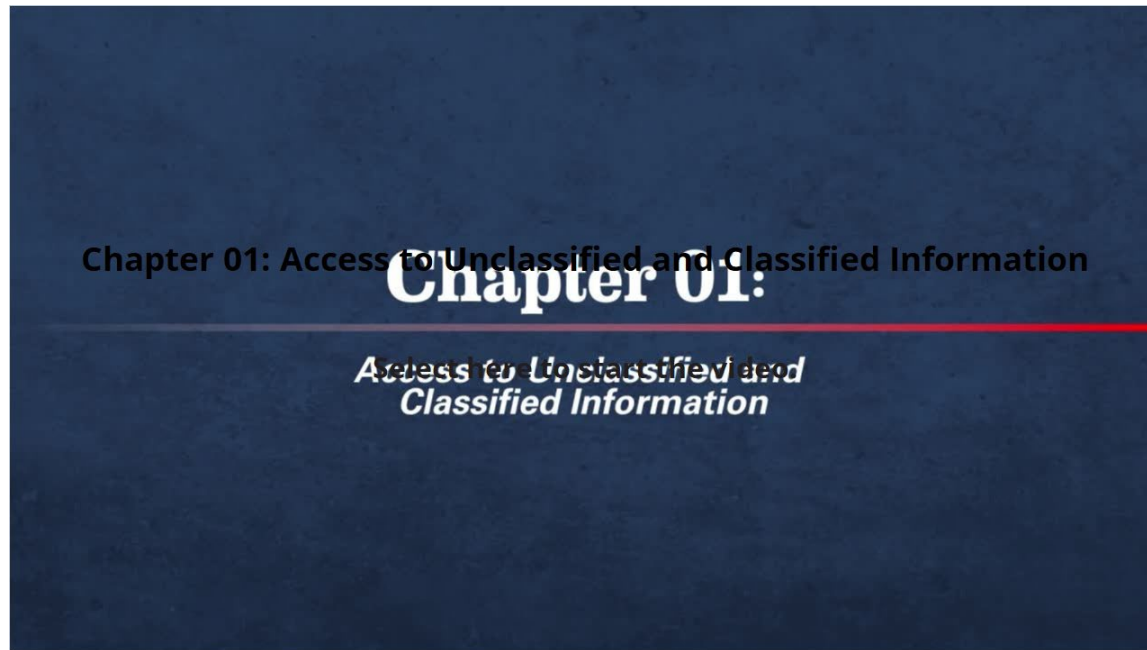
protection of sensitive information. These requirements are established under the Atomic Energy Act of 1954, Executive Orders, Federal statutes, regulations, and DOE directives.

### nav buttons (Slide Layer)



## 2. Access to Unclassified and Classified Information

### 2.1 Responsibilities



#### Notes:

##### **ACCESS TO CLASSIFIED MATTER**

Four requirements must be met before you can access classified information.

##### **Security Clearance**

As an employee of the Federal Government or one of its contractors, you've been subject to a personnel security investigation. The purpose of this investigation was to determine your trustworthiness to access classified information. When the investigation was completed, DOE granted you a "Q", "L", Top Secret (TS), Secret (S) or Confidential (C) security clearance based on a favorable determination of the investigation results.

##### **Comprehensive Security Briefing**

The second requirement prior to initial access to classified information is that you've completed a Comprehensive Security Briefing upon receipt of a security clearance. Completing this briefing satisfies this requirement.

##### **Classified Information Nondisclosure Agreement**

The third obligation prior to your initial access to classified information is to sign the "Classified Information Nondisclosure Agreement," Standard Form 312. The SF 312 is a contractual agreement between you, as a cleared employee, and the U. S. Government, in which you agree never to disclose classified information to an unauthorized person.

After completing this briefing, and prior to receiving your DOE security badge from the HQ badge office, you will be asked to read and sign a copy of the SF 312.

##### **"Need-to-Know"**

The fourth and final requirement for access to classified information is the "Need-to-Know" principle. You must have a valid Need-to-Know the information in order to perform your official duties or assist in a lawful and authorized Governmental function. The holder of classified information to which you seek access is responsible for confirming your identity, your security clearance level, and your Need-to-Know. As a holder of classified information, you're responsible for making these same determinations with respect to any individual to whom you may disclose it. Check with your supervisor if you have any doubt as to an individual's Need-to-Know.

No person may have access to classified information unless he or she has been granted a security clearance equal to, or higher than, the classification level and category of the information, and the requisite Need-to-Know. Additionally, no person is entitled to access classified information solely by virtue of their rank, office, position or security clearance.

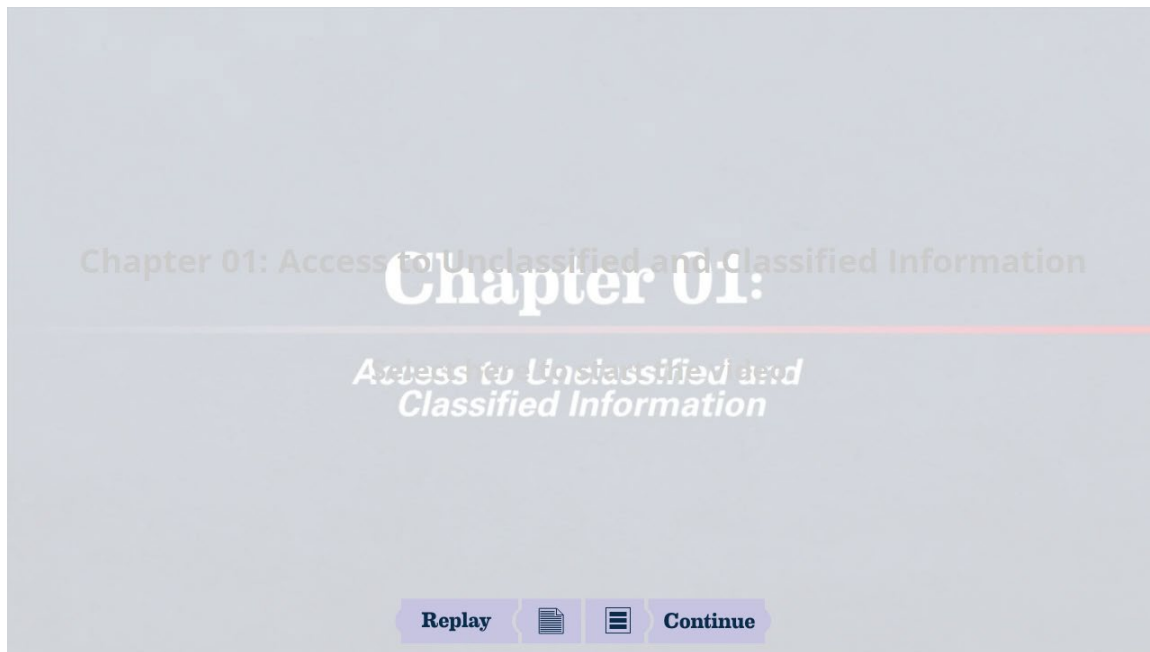


### PERSONNEL SECURITY CLEARANCE

Prior to receiving your security clearance, you've been subject to a personnel security investigation. The purpose of this investigation was to determine your trustworthiness to access classified information. When the investigation was completed, DOE granted you a security clearance.

An employee's security clearance is determined by the work they will perform, their position description (if a Federal employee), or the terms of the contract (if a contractor employee).

### Replay (Slide Layer)



## 2.2 Classification and categories

# Classification and Categories

Q, TS, L, S, or C security clearance indicators are visible on Federal and contractor security badges and may be used to identify an individual's security clearance.

Select the Clearance buttons to view applicable Categories

Q

L



Previous   Continue

Notes:

### Q (Slide Layer)

# Classification and Categories

## Q Clearance

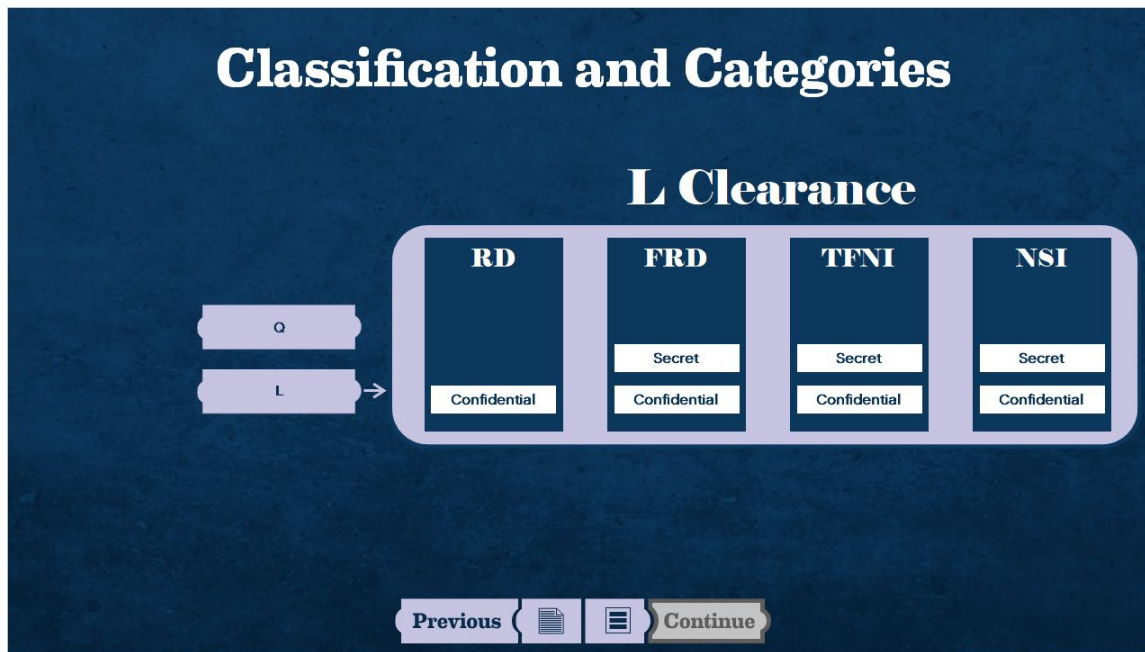
Q

L

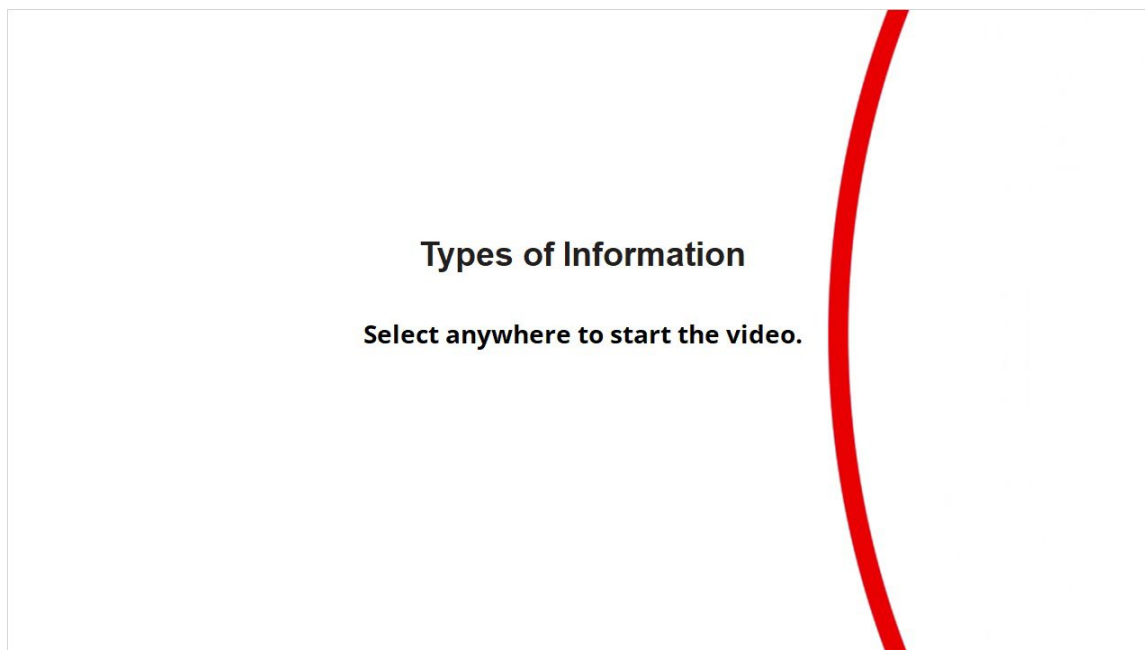
| RD           | FRD          | TFNI         | NSI          |
|--------------|--------------|--------------|--------------|
| Top Secret   | Top Secret   | Top Secret   | Top Secret   |
| Secret       | Secret       | Secret       | Secret       |
| Confidential | Confidential | Confidential | Confidential |

Previous   Continue

## L (Slide Layer)



## 2.3 Types of Information



### Notes:

#### TYPES OF INFORMATION

The DOE originates and receives unclassified information, unclassified controlled nuclear information and controlled unclassified information.

Unclassified is the designation for information, a document, or material that has been determined not to be classified or that

has been declassified by proper authority.

UCNI and CUI are two forms of data you should be familiar with. Although unclassified, this is sensitive material that requires special handling.

### Unclassified Controlled Nuclear Information

UCNI is certain unclassified but sensitive information concerning nuclear material, weapons, and components the distribution of which is controlled under the Atomic Energy Act. You can recognize UCNI documents by the markings. Documents containing UCNI have "Unclassified Controlled Nuclear Information" marked on the front, internal pages, and back. Email containing UCNI will have "Unclassified Controlled Nuclear Information" at the beginning of the email.

UCNI is unclassified data; a security clearance is not required to access this information. However, because it is sensitive information, access is controlled and based on a Need-to-Know for official business. Requirements are contained in 10 CFR Part 1017, and DOE Order 471.1B, Identification and Protection of Unclassified Controlled Nuclear Information.

### Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is information that is identified and safeguarded under Executive Order (E.O.) 13556, Controlled Unclassified Information. Requirements for CUI are contained in Title 32, Code of Federal Regulations Part 2002, Controlled Unclassified Information and DOE Order 471.7, Controlled Unclassified Information.

CUI is based on law, regulation, or Government-wide policy (LRGWP). When the LRGWP contains specific requirements for activities like dissemination, safeguarding, marking, the CUI is Specified CUI and the requirements contained in the LRGWP take precedence over any other CUI requirements. Requirements for the Privacy Program contained in DOE O 206.1 remain in effect.

Prior to the implementation of CUI, DOE controlled unclassified information was identified as Official Use Only, or OUO. DOE Order 471.3 was the driving document for how to handle and maintain OUO. Legacy OUO is still found throughout DOE. Contact your CUI Representative for how to handle legacy OUO.

## 2.4 CUI

# CUI

CUI is information the Government, or an entity on behalf of the Government, creates or possesses that an LRGWP requires or permits an agency to handle using safeguarding or dissemination controls.

All individuals handling CUI are required to protect it from unauthorized disclosure. Handling, storage, reproduction, and dissemination of CUI documents must be in accordance to 32 CFR Part 2002 and DOE O 471.7.

*Refer to DOE O 471.7, Identification and Protection of Unclassified Controlled Nuclear Information for additional information.*

[Previous](#)   [Continue](#)

### Notes:



## 2.5 Access to UCNI

### Access to UCNI

In general, any DOE employee or contractor, which includes non-U.S. citizens, is authorized for routine access to UCNI if the individual has a "need to know" in order to perform official duties.

However, there are restrictions in some circumstances regarding the release of UCNI to persons who are not DOE, government, or contractor employees, to include restrictions for foreign nationals. Such individuals may still request limited access to UCNI under 10 CFR Part 1017.21, Subpart D.

Previous   Continue

Notes:

## 2.6 Legacy OUO

### Legacy OUO

Prior to the implementation of CUI, DOE Controlled Unclassified Information was identified as Official Use Only (OUO). DOE Order 471.3 was the driving document for how to handle and maintain OUO.

Legacy OUO is still found throughout DOE. Contact your CUI Official or CUI Liaison for how to handle legacy OUO.

Previous   Continue

Notes:

## 2.7 UCNI Requirements

# UCNI Requirements

There are several requirements for handling UCNI and penalties for violations.  
*Select each box for more information.*

1  
Reviewing UCNI

2  
Access to UCNI

3  
Marking UCNI

4  
Protecting UCNI

5  
Penalties

*Refer to 10 CFR 1017 and DOE O 471.1B for complete requirements for UCNI.  
Links to these documents are in the course Resources.*

Previous

Continue

Notes:



## 2.8 PII Information

# Personally Identifiable Information

Personally Identifiable Information (PII) is one type of CUI.

PII consists of any information about an individual maintained by an agency, including but not limited to the following:

- education
- financial history
- medical history
- criminal or employment history

PII is any information which can be used to distinguish or trace an individual's identity, such as their name, associated with the following:

- social security number
- date and place of birth
- mother's maiden name
- biometric records

*PII also includes any other personal information which is linked or linkable to an individual.*

Previous



Continue

Notes:

## 2.9 Disposal of UCNI

# Disposal of UCNI

Paper containing UCNI must be destroyed using a crosscut shredder that results in particles no larger than ¼ inch wide and 2 inches long. Approved shredders can be purchased from the DOE supply store. UCNI may also be destroyed by using the Germantown Centralized Classified Destruction Facility (CCDF).

See UCNI Marking: Additional Information in the course Resources for information on UCNI burn bag marking and access.

Contact your HSO or consult Chapter 13 of the master plan (HQFMSP) for additional information on UCNI destruction.



Previous



Continue

Notes:

## FGI (Slide Layer)

Select here to close

### Foreign Government Information (FGI)

Information that is provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

Information that is produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence; or

Information received and treated as "Foreign Government Information" under the terms of Executive Order 13526 or a predecessor order.

The front page of a document that contains FGI must include the marking "This document contains (indicate country of origin) information." If the identity of the specific government must be concealed, the document must be marked, "This document contains foreign government information."

## 2.10 Reviewing Potential UCNI

# Reviewing Potential UCNI

Getting access to classified matter could increase your chances of generating or encountering unmarked matter that contains UCNI.

UCNI subject areas overlap certain classified subject areas related to the design of production and utilization facilities, the security of those facilities (or nuclear material contained in them or in transit), or *some* declassified information about nuclear weapons that was once RD.

**Examples of UCNI Subject Areas:**

Security information for certain field elements, Radiological Emergency Response, nonproliferation, production/processing of uranium and plutonium, Transportation Safeguards System

If you have questions, talk with your supervisor/HQ Classification Representative, or contact the HQ Office of Classification.

Refer matter that *may* contain UCNI to an UCNI RO for review. See the course Resources for additional information about UCNI.

[Previous](#)   [Continue](#)

Notes:



## FGI (Slide Layer)

Select here to close

### Foreign Government Information (FGI)

Information that is provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

Information that is produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence; or

Information received and treated as "Foreign Government Information" under the terms of Executive Order 13526 or a predecessor order.

The front page of a document that contains FGI must include the marking "This document contains (indicate country of origin) information." If the identity of the specific government must be concealed, the document must be marked, "This document contains foreign government information."

## 2.11 Disposal of CUI: Electronic Media

# Disposal of CUI: Electronic Media

CUI destruction requirements generally require a more involved process of destruction.

Electronic media must be destroyed in accordance with National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, or successor standard and NIST SO 800-88, or successor standard.

It may also be destroyed through any methods of destruction approved for Classified National Security Information (32 CFR 2001.47) or any implementing or successor guidance.

Previous   Continue

Notes:

---

## 2.12 Disposal of CUI: Destroying Paper

# Disposal of CUI: Destroying Paper

### Single-Step Paper Destruction Method:

1. Cross-cut shredders must produce 1 mm x 5 mm (0.04 in. x 0.2 in.) particles or smaller.
2. Equipment that can pulverize/disintegrate paper must use disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen.
3. Equipment must be approved and labeled.

### Multi-Step Paper Destruction Method:

1. Follow guidelines in Information Security Oversight Office (ISOO) CUI Notice 2019-03: *Destroying Controlled Unclassified Information (CUI) in Paper Form*, or successor guidance.
2. The process must result in CUI that is unreadable, indecipherable, and irrecoverable.
3. The multi-step process generally involves storing the paper securely until it is picked up by a service that will destroy it.

*CUI-100DE, Controlled Unclassified Information Overview provides a comprehensive overview of CUI. The course is available on the Learning Nucleus.*

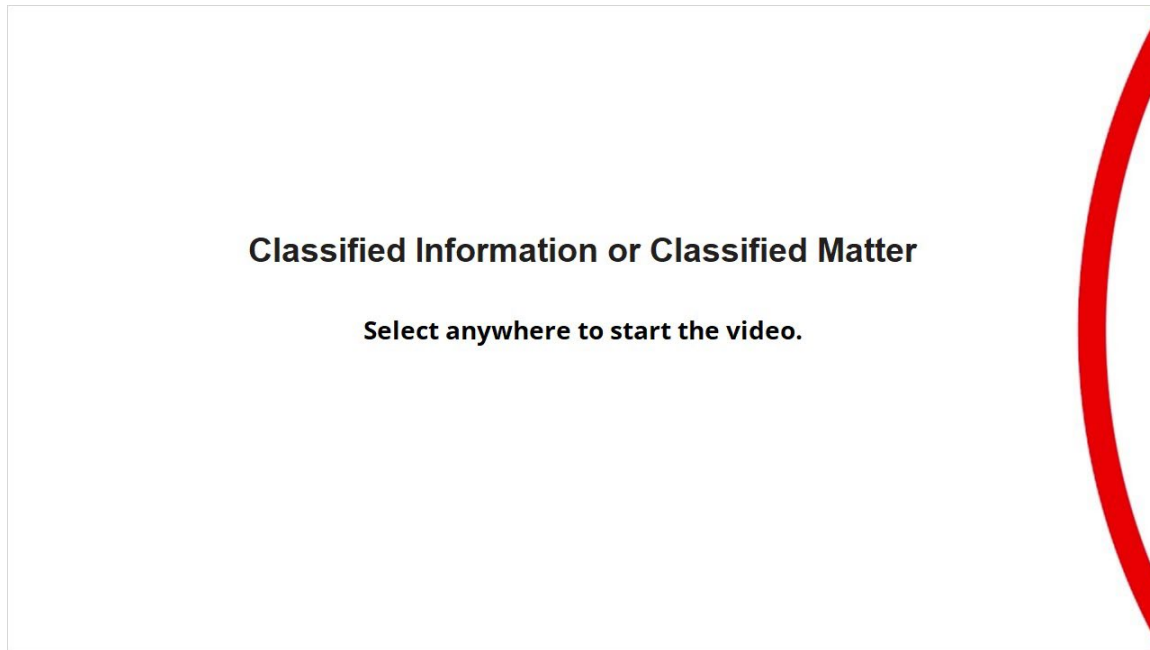
Previous



Continue

Notes:

## 2.13 Classified Information or Classified Matter



### Notes:

#### **CLASSIFIED INFORMATION OR CLASSIFIED MATTER**

Classified information is information that has been determined by the government to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. This information requires protection against unauthorized disclosure, dissemination, and is marked to indicate its classified status. Classified Matter is any combination of documents and material containing classified information.

#### **CLASSIFICATION LEVELS**

All classified information falls within one of three classification levels, Top Secret, Secret, and Confidential. The significance of these levels, reflects their varying degrees of sensitivity.

##### **Top Secret (TS)**

Top Secret is the classification level assigned to information of utmost importance to the national defense and security. Unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security.

##### **Secret (S)**

Secret is the classification level applied to information for which the unauthorized disclosure could reasonably be expected to cause serious damage to national security.

##### **Confidential (C)**

Confidential is the classification level applied to information for which the unauthorized disclosure could reasonably be expected to cause damage to national security.

#### **CLASSIFICATION CATEGORIES**

All classified information falls within one of four classification categories:

##### **Restricted Data (RD)**

RD is all data concerning the design, manufacture, or use of nuclear weapons; productions of special nuclear material; or use of special nuclear material in the production of energy except for data declassified or that has become Formerly Restricted Data or Transclassified Foreign Nuclear Information.

##### **Formerly Restricted Data (FRD)**

FRD is classified information that DOE or its predecessor agencies and the Department of Defense (DoD) have jointly determined (1) to be related primarily to the military use of atomic weapons and (2) can be adequately safeguarded in a manner similar to National Security Information. It is also subject to the restrictions on transmission to other countries and



regional defense organizations that apply to RD.

#### **Transclassified Foreign Nuclear Information (TFNI)**

TFNI is classified information that was RD, related to foreign nuclear programs. DOE or its predecessor agencies and the Intelligence Community determined this classified information could be adequately protected in a manner similar to National Security Information and moved this information into the TFNI category.

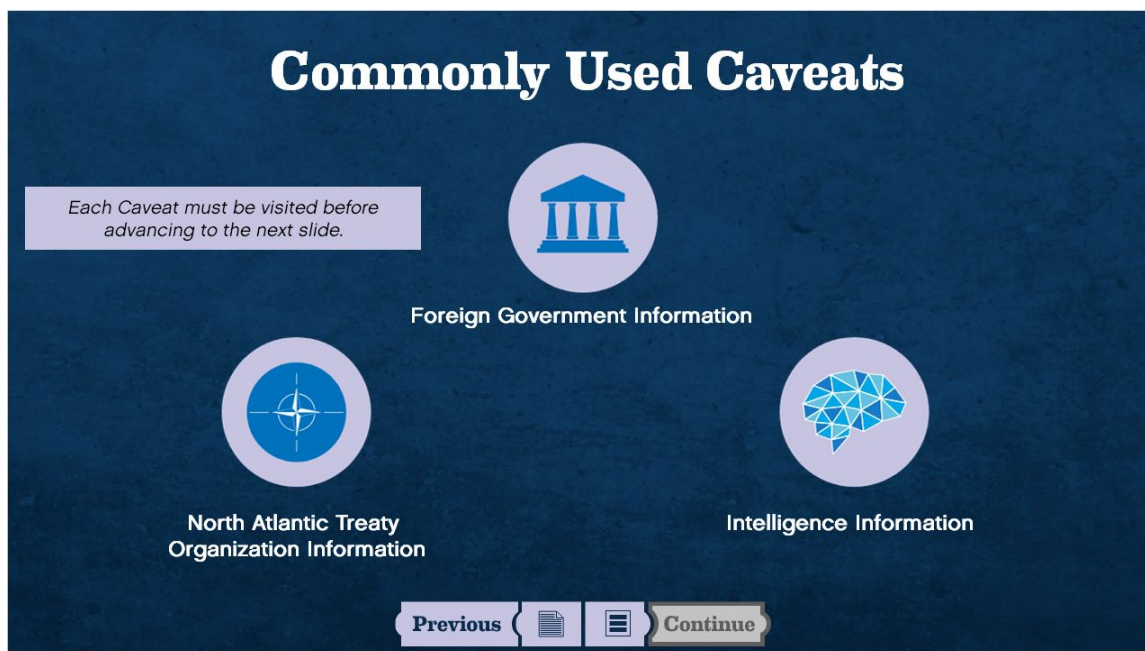
#### **National Security Information (NSI)**

NSI is information that has been determined by Executive Order to require protection against unauthorized disclosure.

#### **SPECIAL MARKINGS AND HANDLING CAVEATS**

In addition to classification level and category markings, special markings and caveat markings are placed on documents either to describe special handling or dissemination requirements or to identify the type of information and the originator. Take some time to review some of the most commonly used caveats.

### **2.14 Commonly used Caveats**



**Notes:**

## FGI (Slide Layer)

[Select here to close](#)

### Foreign Government Information (FGI)

Information that is provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

Information that is produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence; or

Information received and treated as "Foreign Government Information" under the terms of Executive Order 13526 or a predecessor order.

The front page of a document that contains FGI must include the marking "This document contains (indicate country of origin) information." If the identity of the specific government must be concealed, the document must be marked, "This document contains foreign government information."

## NATO (Slide Layer)

[Select here to close](#)

### North Atlantic Treaty Organization (NATO) Information

The following markings used for classified NATO material include:

|                                                                                                                                                                                                                          |                                                                                                                     |                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>The markings used for NATO material include:</p> <ul style="list-style-type: none"><li>o COSMIC TOP SECRET (CTS)</li><li>o NATO SECRET (NS)</li><li>o NATO CONFIDENTIAL (NC)</li><li>o NATO RESTRICTED (NR)</li></ul> | <p>COSMIC is a NATO marking applied to all copies of Top Secret documents prepared for circulation within NATO.</p> | <p>ATOMAL is a North Atlantic Treaty Organization marking applied to:</p> <p>(1) Restricted Data or Formerly Restricted Data provided by the United States to the North Atlantic Treaty Organization or (2) "U.K. Atomic Information" provided by the United Kingdom.</p> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

For more information on special markings, foreign government information, and handling instructions refer to Chapter 5, HQFMSP or see the DOE CMPC Marking Resource.

## Intelligence (Slide Layer)

**Intelligence Information**

The following are markings authorized for Intelligence Information:

**No Foreign Dissemination (NOFORN)**

This marking indicates that the information contained in the document must not be released to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens without originator approval.

**Originator Controlled (ORCON)**

This marking indicates that the originator controls the document. Reproduction, extraction of information, or redistribution of such documents requires the permission of the originator.

**Proprietary Information (PROPIN)**

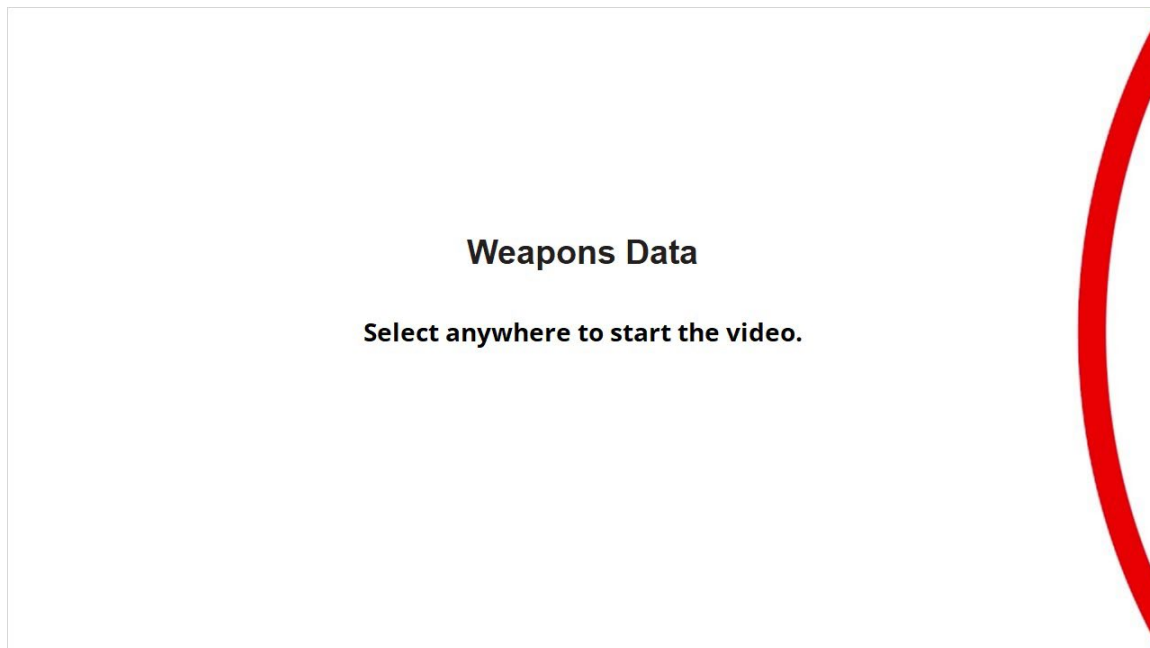
This marking indicates that the information contained in the document must not be released outside the government in any form to an individual, organization, or foreign government without the permission of the originator of the intelligence and provider of this information.

**Authorized for Release to Country (REL)**

This marking applies to classified intelligence information that an originator has predetermined to be releasable or has released through established foreign disclosure procedures and channels to a specified foreign country or countries, and international organization(s). This marking is never used alone. It is generally used with NOFORN (for example, NOFORN REL UK).

Select here to close

## 2.15 Weapons Data



### Notes:

#### WEAPONS DATA

The two markings associated with atomic weapons or nuclear explosive devices are:

#### **Sigma Category**

Sigma categories are subsets of RD and, or, FRD that require additional protection. Sigma categories concern: nuclear

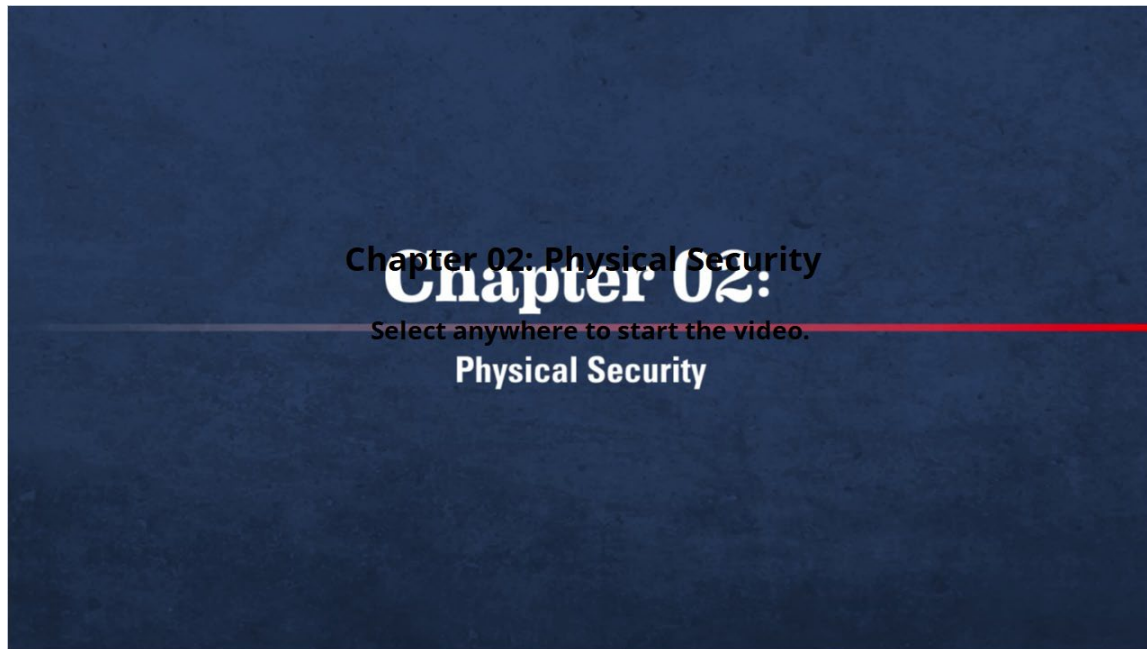
weapons, materials, components or nuclear explosive devices.

**Critical Nuclear Weapons Design Information**

CNWDI is a Department of Defense designation for certain Top Secret, or Secret, RD weapons design information.

## 3. Physical Security

### 3.1 Physical Security



**Notes:**

**Graded Approach to Protection**

When developing and implementing protection programs, the level of effort and magnitude of resources expended for the protection of a particular safeguards and security (S&S) interest must be taken into account. S&S is a general term for any DOE resource or property that requires protection. It includes but is not limited to personnel; classified information; sensitive unclassified information or other Departmental property. At Headquarters, protection of classified matter is given the highest level of protection and is accomplished by layered security, resulting in a graded approach to protection.

**Security Areas**

Security areas are defined areas containing S&S interests that require physical protection measures.

The first layer of security at HQ is the General Access Area. This area is open to the public and is referred to as a GAA. An example is the DOE museum, in the main lobby of the Forrestal facility.

One of the types of security areas at Headquarters is a Property Protection Area. A PPA has defined boundaries and access controls for the protection of Departmental property.

Headquarters also utilizes two types of security areas for the protection of classified information, they are, Limited Areas (LA) and Vault Type Rooms (VTR). These areas also have clearly defined boundaries and access control points. Access to an LA or VTR is limited to appropriately cleared and authorized individuals. All uncleared or unauthorized individuals requiring access to these areas must be escorted by a cleared individual.

Contact your Headquarters Security Officer or HSO if you have questions about the security areas established for your organization. For a more in-depth look at security areas reference Chapters 1 & 5 of the HQMFSP.

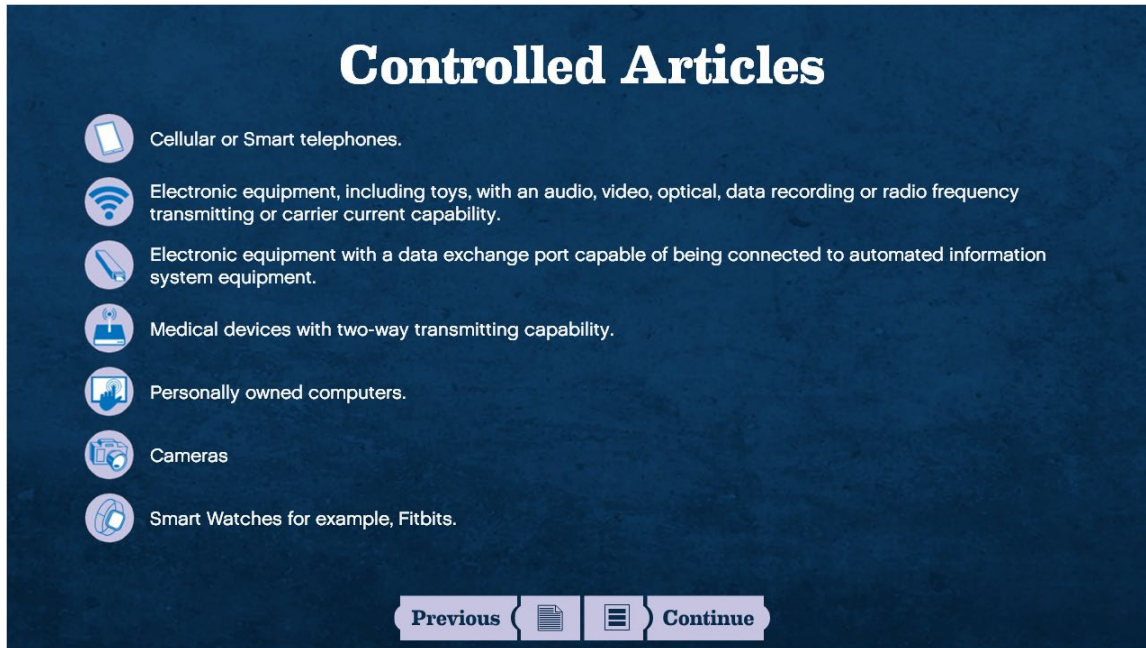
**Controlled Articles**



Because of their potential to be used to record or transmit information without authorization, controlled articles are not permitted in LAs or VTRs. Signs are posted at the entrances listing the articles which are prohibited from being introduced into these areas.

Under certain conditions controlled articles, like cell phones, may be authorized in certain LAs. The decision whether or not to allow electronic devices in an LA rests with the area's senior leadership. Contact your HSO for more information.

### ***3.2 Controlled Articles***

A dark blue rectangular sign with the title "Controlled Articles" in large white serif font at the top. Below the title is a list of seven items, each preceded by a circular icon with a white border. The items are: Cellular or Smart telephones (phone icon), Electronic equipment, including toys, with an audio, video, optical, data recording or radio frequency transmitting or carrier current capability (Wi-Fi icon), Electronic equipment with a data exchange port capable of being connected to automated information system equipment (USB icon), Medical devices with two-way transmitting capability (medical monitor icon), Personally owned computers (laptop icon), Cameras (camera icon), and Smart Watches for example, Fitbits (smartwatch icon). At the bottom of the sign is a navigation bar with three buttons: "Previous" with a left arrow, a central button with a document icon, and "Continue" with a right arrow.

**Controlled Articles**

- Cellular or Smart telephones.
- Electronic equipment, including toys, with an audio, video, optical, data recording or radio frequency transmitting or carrier current capability.
- Electronic equipment with a data exchange port capable of being connected to automated information system equipment.
- Medical devices with two-way transmitting capability.
- Personally owned computers.
- Cameras
- Smart Watches for example, Fitbits.

Previous { } Continue

**Notes:**

### 3.3 Prohibited Articles



#### Notes:

##### **PROHIBITED ARTICLES**

Prohibited articles are not permitted on DOE property. A sign identifying prohibited articles is posted at the entrances to all Headquarters buildings. Weapons, explosives, or other dangerous instruments (to include mock explosive devices) or materials that can injure people or damage property are prohibited. Other prohibited items include alcoholic beverages and controlled substances (for example: illegal drugs or paraphernalia but not prescription medication).

If you have any questions about prohibited articles contact your HSO or refer to Chapter 2 of the HQFMSP for a complete listing of both controlled and prohibited articles.

##### **VISITOR AND ESCORT REQUIREMENTS**

During non-security hours, 6 a.m. to 7 p.m. Monday through Friday, escorts are not required for visitors that are entering Headquarters facilities unless specified by the office or person being visited. However, uncleared visitors must be escorted at all times and on all days in LAs and VTRs.

Foreign national visitors don't need to be escorted, unless requested by the host, while in PPAs during non-security hours. At all other times, to include 24 hours on Federal holidays and weekends, foreign national visitors must be escorted while in DOE Headquarters facilities by the host or their representative. The escort must possess a DOE Headquarters-issued picture badge and must be a U.S. citizen.

The sponsoring office or person being visited is responsible for providing the escort. When escorting visitors, escorts must be with the visitor at all times and must maintain visual contact at all times. If escort responsibilities are delegated to another person, that person must be made aware of their escort responsibilities.

### 3.4 Escorts

## Escorts Must

**Ensure the visitor:**

- Is not afforded unauthorized access to UCNI/CUI, classified data, or LAs and VTRs.
- Wears his/her Headquarters visitor badge above the waist, in a clearly visible manner, at all times.
- Does not introduce any prohibited or controlled articles into the facility, or security areas.
- Does not remove Government property from the facility except in accordance with established property accountability procedures and the host's approval.
- Complies fully with all Headquarters security requirements.

*Note: One escort may not escort more than five (5) visitors in a PPA and three (3) visitors in a VTR at any given time. The escort must stay with his visitor(s) at all times and maintain visual contact and control over their movements and activities. If for any reason the escort is unable to maintain control over his/her visitors the escort must request an appropriately cleared employee assist with escort duties. For more information on escort requirements contact your HSO or reference Chapter 1, HQFMSP.*



[Previous](#)   [Continue](#)

**Notes:**

### 3.5 Inspections

## Security Badges

Select anywhere to start the video.



## Notes:

### SECURITY BADGES

Headquarters issues photo identification security badges to DOE Federal and contractor employees who require long-term routine access to the Headquarters buildings. These badges, also known as an HSPD-12 badge, identify the individual and contain a security clearance indicator (Q, TS, L, S, or C) for those individuals who have been granted a DOE security clearance (additionally, Headquarters also issues temporary badges to visitors and employees who have lost or forgotten their badge). In Headquarters buildings, employees and visitors must wear their badge above the waist, in plain view, with the photo showing. An employee should notify their designated sponsor to obtain a new badge if they officially change their name, or have a significant change in facial appearance.

Immediately notify the badging office if your badge is ever lost or stolen.

Forrestal Badging Office 202-586-5764

Germantown Badging Office 301-903-3330

### INSPECTIONS

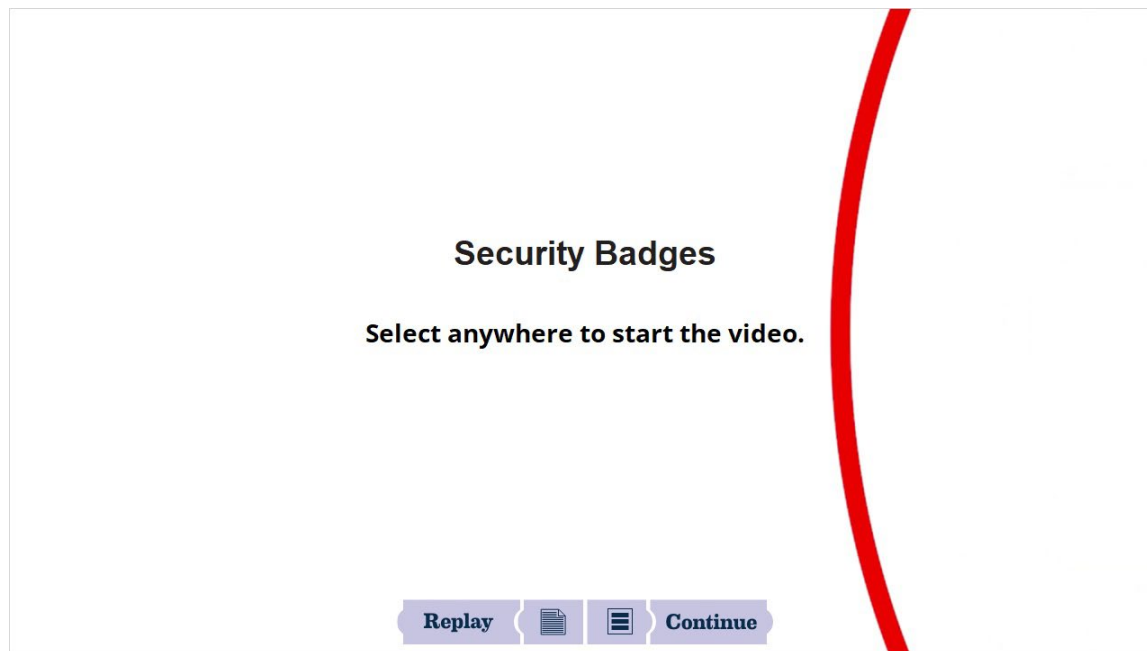
All hand carried articles are subject to inspection by Security Police Officers upon entry, or exit from a Headquarters facility. Directed by Office of Headquarters Security Operations inspections may be conducted with probable cause, of any employee, contractor, or visitor. Headquarters uses a random inspection process and various explosive detection methods to detect and deter vehicle-transported explosive devices. All visitors to Headquarters facilities must undergo an inspection upon entry into the facility.

### CLASSIFIED CONFERENCES AND DISCUSSIONS

As a general rule, classified discussions, conversations, or conferences must be held in a formally established and approved LA or VTR. Hosts of classified conferences or parties to classified discussions must take certain precautions to ensure that classified information is not compromised.

Classified discussions, meetings, or conferences held outside approved security areas require specific case-by-case approvals. Contact your HSO for additional information or reference Chapters 1 & 5 of the Master Plan.

## Replay (Slide Layer)



**Security Badges**

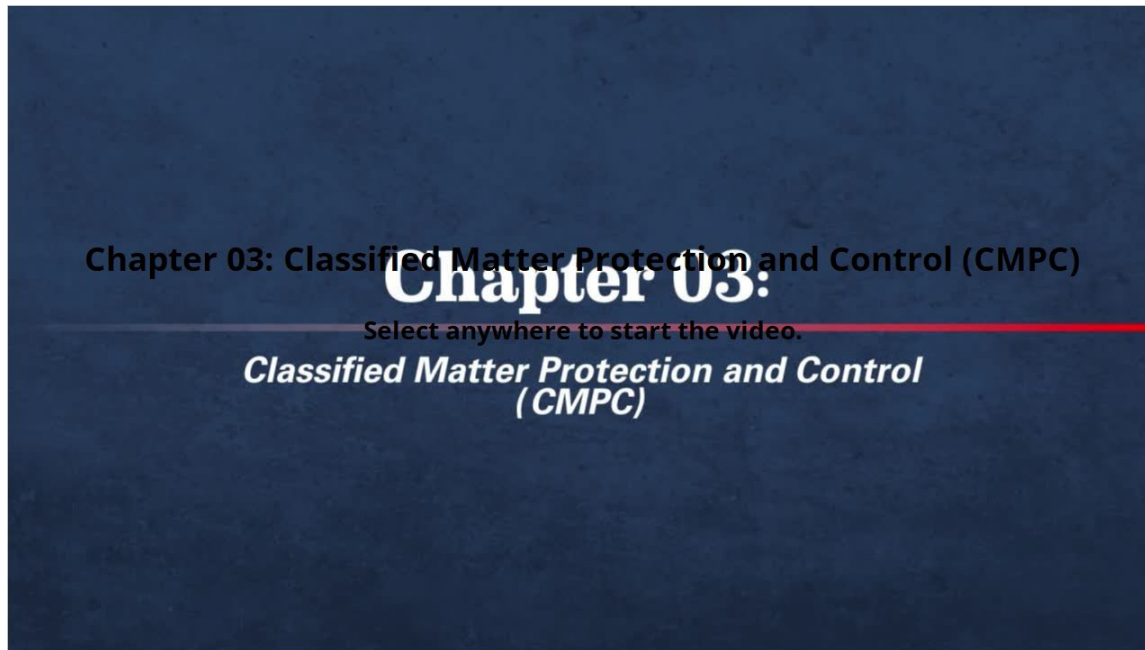
Select anywhere to start the video.

Replay [document icon] [list icon] Continue



## 4. CMPC

### 4.1 CMPC



#### Notes:

##### **CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)**

A strong and cohesive information security program is integral to national security. The U.S. Government requires certain information to be maintained in confidence to protect our citizens, democratic institutions, and activities within the international security community. Marking notifies holders of classified matter about the protection requirements for the information.

It is the responsibility of the person originating the classified document to ensure classified matter is marked in accordance with DOE Directives, includes proper classification markings, and the document is properly classified by a Derivative Classifier. To help you get started, let's go over some of the fundamentals of marking classified documents.

Classified Document Cover Sheets serve as shields to protect Top Secret, Secret, and Confidential documents from inadvertent disclosure. Always place a cover sheet on the face of each classified document when it's in use or removed from a security container. Cover sheets are also required on the back of a classified document if the back page is not marked with the overall highest classification level of the document.

The classifier marking must be placed on the "first page" of the document, whether the cover page, title page, or first page of text and should be placed in the lower left corner. This marking includes the classifier and originator identification, the date of origin, and the declassify date.

The Derivative Declassifier Review Stamp should be close to the Classifier Marking, preferably above it, but as close as possible.

The overall classification level of a document must be marked on the top and bottom of any cover, title, first page of text, and the outside of the back cover or last page of text, this includes all internal pages as well.

If the classified matter has any special markings, caveats, or category like RD, FRD, or TFNI, they must be clearly marked.

## 4.2 Contacts for Classification and UCNi

### Contacts for Classification and UCNi

Staff from these respective offices can assist with classification issues at Headquarters:

**DOE Classification Officer for DOE HQ**  
Director of the HQ Office of Classification (EHSS-60)

**NNSA Program Classification Officer**  
Director of the Classification Division (NA-746)

For classification questions, contact your Classification Representative or one of the following:

**DOE**  
Office of Classification Outreach Program  
Phone: 301-903-7567  
Email: [outreach@hq.doe.gov](mailto:outreach@hq.doe.gov)

**NNSA**  
Shared (low-side) inbox: [classification@nnsa.doe.gov](mailto:classification@nnsa.doe.gov)  
Staff contact via the NNSA Portal

[Previous](#)   [Continue](#)

Notes:

## 4.3 Classification and Upgrading Reviews

### Classification Reviews for Public Release

DOE O 475.2B requires that all matter in a classified subject area receive a review from the Classification Officer (CO) prior to being publicly released. Even if the employee does not believe the matter contains information that is potentially classified, it must still be reviewed by the CO.

At HQ, reviews of this matter are conducted by either EHSS-60 (for DOE personnel) or by NA-476 (for NNSA).

*Public release includes posting to a website, sending in documents to Congress, and giving a DOE briefing to an audience where there could be members of the public or uncleared personnel.*

*Remember: A "classified subject area" is any area for which a classification guide is issued (for example, Safeguards and Security). If you are not certain what falls into these areas, check with your supervisor.*

[Previous](#)   [Continue](#)

Notes:

#### ***4.4 No Comment Policy***

## Gen-16, Rev. 2: No Comment Policy

An authorized person must not comment (verbally or in writing) on the classification status or technical accuracy of any classified information (marked or unmarked) in the open literature. This includes not commenting through social media.

Just because classified information is in the open literature does not mean it is declassified.

If you incorporate open literature information into an unclassified document that is in a classified subject area, you must have the document reviewed in accordance with DOE O 475.2B Identifying Classified Information.

Review full details using either of the following:

[Classification Bulletin GEN-16, Revision 2, "No Comment" Policy on Classification Information](#)

Powerpedia: Search "GEN-16" or "No Comment."

[Previous](#)   [Continue](#)

Notes:



## 4.5 Working Papers

### Working Papers

Prior to obtaining required classification reviews, you must protect information that may be classified at the highest potential classification level and category and in accordance with any associated caveats or special handling instructions.

A classification official must review matter marked as a “working paper” when any of the following is true:

1. The material is retained more than 180 days from the origination date or the date of the last change (if a “living document”).
2. The material is released by the originator outside the originating activity.
3. The material is filed permanently.

The requirements are on pages 4 and 6 of [DOE O 471.6, Information Security](#) and applicable national directives (for example, 10 CFR 1045 for RD/FRD/TFNI).

Previous



Continue

Notes:

## 4.6 Declassification and Downgrading Reviews

### Declassification and Downgrading Reviews

Any time you want to remove, lower, or redact the classification of matter in order to handle it as unclassified, or at a less restrictive classification level or category, you must get a Derivative Declassifier (DD) review.

A DD is trained and authorized to downgrade or declassify documents in their particular classified subject areas and jurisdiction.

This is a separate authority from Derivative Classifier authority.

*You must get a DD review even if matter is marked with a date/event for declassification that already occurred. If you want to extract a section from a document (for example, a chapter) that is marked classified and use it as an unclassified document, DD review is also required. Other required reviews are in DOE O 475.2B, Attachment 4.*

Familiarize yourself with the additional classification review requirements in the course Resources.

Previous



Continue

Notes:

#### ***4.7 Classification and Declassification Challenges***

## **Classification & Declassification Challenges**

Each employee is encouraged and expected to challenge the classification of information or matter believed to be improperly classified or declassified. Under no circumstances is the employee subject to retribution.

If possible, resolve the challenge locally with the DC/DD that made the decision or through the Classification Representative. However, challenges can be submitted in writing directly to the Director, EHSS-60, at any time. Details of the challenge and appeals process are in DOE O 475.2B Attachment 4, paragraph 4.

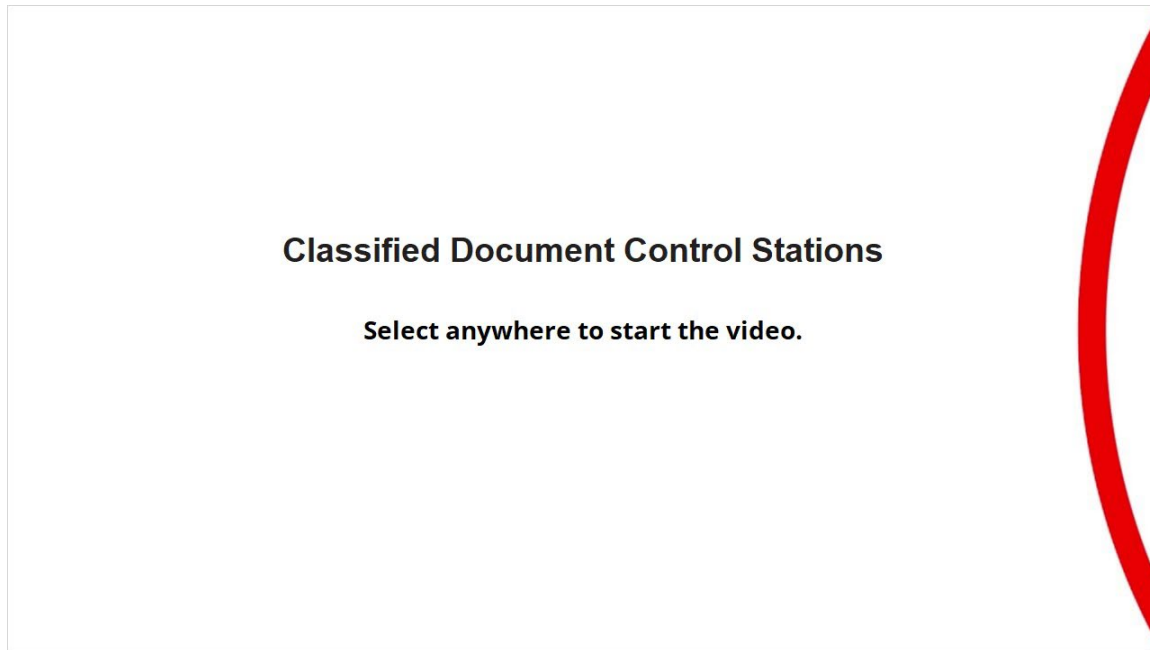
Information/matter being challenged for classification shall remain classified until a final determination is made. If the challenge itself potentially contains classified information, it must be transmitted to a DC for review via secure means.

[Previous](#)   [Continue](#)

Notes:



## 4.8 Classified Document Control Stations



### Notes:

#### **CLASSIFIED DOCUMENT CONTROL STATIONS**

Each Element authorized to store classified matter has established at least one Classified Document Control (CDC) Station for its organization. The purpose of a CDC Station is to maintain records, access lists, and control classified matter received by and or dispatched from Headquarters Elements. CDC Stations are focused on preventing unauthorized access to, or removal of, classified matter. Consult your HSO for additional guidance on CDC Stations for your organization.

#### **ACCOUNTABILITY OF CLASSIFIED MATTER**

Some particularly sensitive classified matter must be placed into an accountability system. The Department has established accountability systems as security mechanisms to control access and ensure that these classified documents can be located at any time. Accountability is a system which provides auditable control measures associated with classified matter through the use of a verifiable inventory and the establishment of a custodial chain.

Accountability records are required when accountable matter is originated, reproduced, transmitted, received, destroyed, or changed in classification.

## 4.9 Accountable Matter

### Accountable Matter

All accountable matter (listed below) must be entered into an accountability system that indicates the following information: **Select each box of accountable matter to reveal more information.**

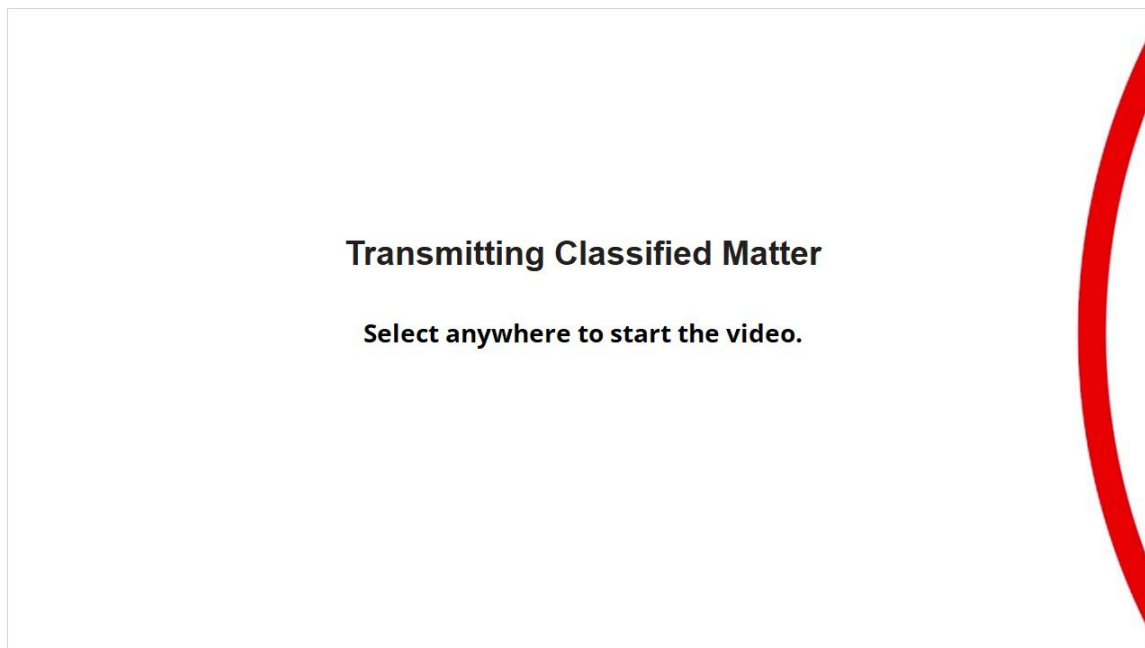
|                                    |                                                                |                                                                         |                                                                                                                       |                                                                                  |
|------------------------------------|----------------------------------------------------------------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| <b>1</b><br>Date of the matter     | <b>2</b><br>Brief description of the matter                    | <b>3</b><br>Unique identification number                                | <b>4</b><br>Numbers and copies and disposition                                                                        | <b>5</b><br>Date received                                                        |
| <b>6</b><br>Originator information | <b>7</b><br>Authority for contractor retention (if applicable) | <b>8</b><br>Activity from which the matter was received (if applicable) | <b>9</b><br>Responsible individual (the individual who checked in and/or out, who has personal responsibility for it) | <b>10</b><br>Classification level and category (if RD, FRD, or TFNI) and caveats |

Contact your HSO or consult the HQFMSP for additional information on CMPC requirements.

Previous   Continue

Notes:

## 4.10 Transmitting Classified Matter



## Notes:

### TRANSMITTING CLASSIFIED MATTER

Before transmitting a classified document, the sender must ensure the recipient has the proper "Need-to-Know" for the information in the performance of their official duties, possesses the appropriate security clearance and is authorized to receive the information, has an approved Classified Mailing Address (CMA), and has approved storage facilities for protecting the information.

CDC Station personnel must prepare the material for transmission. The CMA must be verified in the Safeguards and Security Information Management System (SSIMS) before transmitting the classified matter. All facilities authorized for the receipt of classified matter from Headquarters must be recorded in SSIMS.

### Hand Carrying Classified Matter

Classified matter transmitted outside Headquarters facilities, for example between the Forrestal and Germantown buildings, including hand carried matter, must be double wrapped. CDC Station personnel must prepare the material for transportation.

A Federal or contractor employee must be specifically authorized by their organization to hand carry classified matter and authorization may be granted only if the individual has received a specific "Hand Carry Security Briefing." Hand carrying classified matter aboard a commercial aircraft requires case-by-case approval by your organization and an additional special security briefing.

Contact your HSO for additional information and, if necessary, to receive the proper security briefing.

## 4.11 Hand Carrying Classified Matter

# Hand Carrying Classified Matter

The inner envelope must be properly prepared as discussed before and the outer envelope may be an appropriately addressed and sealed envelope, or a locked briefcase tagged with the CMA. If hand-carrying outside the D.C. Metropolitan Area, a locked briefcase may NOT substitute for the outer wrapping. A manifest listing all hand carried material must be left with your organization's assigned CDC Station personnel each time you hand carry classified material outside a Headquarters building. You must also carry a copy of the manifest with you while hand carrying.

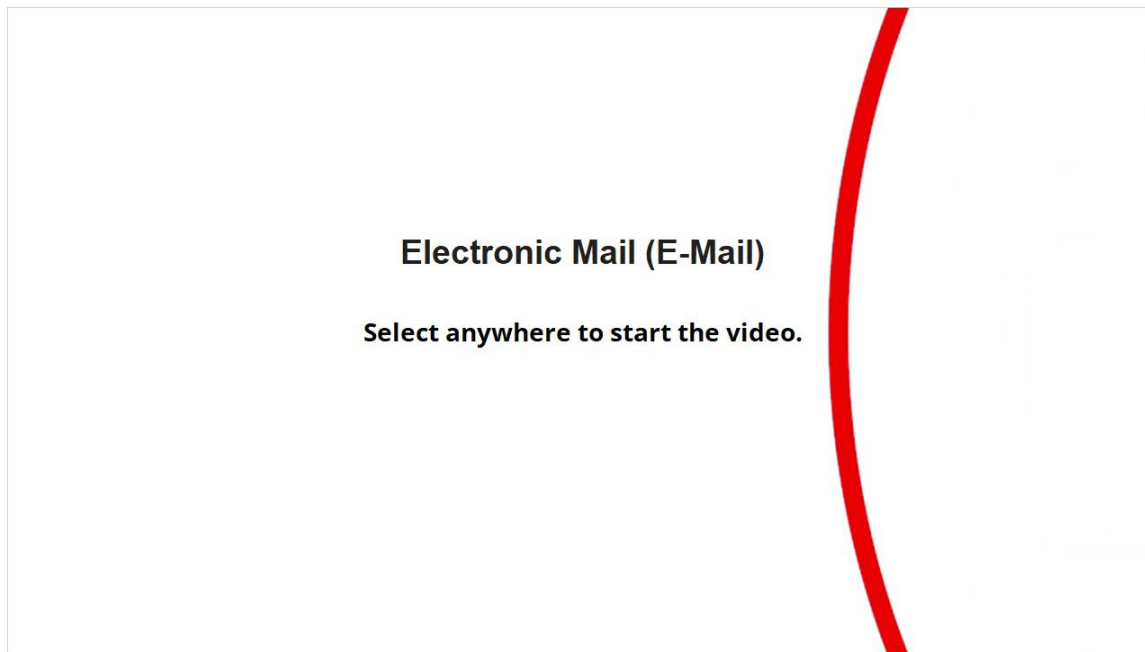
Classified documents carried between security areas in the same Headquarters building may be transported in a HQ F 14105, "Candy-Stripe," envelope. The Candy-Stripe envelope serves as the outer wrapper. No inner wrapper is required, but the document must have the appropriate cover sheet attached. Contact your HSO for guidance if a Candy-Stripe envelope is not available.

The Department discourages hand carrying classified documents. Transmitting classified matter through other approved channels (e.g., secure facsimile or secure IT system) is more efficient. If you do hand carry classified matter, keep the matter continuously in your possession until stored in an approved storage repository. *Additionally, classified matter **may not be removed and taken to private residences or other unapproved places such as restaurants or hotel rooms.***

[Previous](#)   [Continue](#)

## Notes:

## 4.12 Electronic Mail



### Notes:

#### **ELECTRONIC MAIL (E-MAIL)**

Classified e-mail messages may be transmitted only on accredited computers approved for classified transmissions and in accordance with an approved security plan. Consult your HSO or your Element's Information Systems Security Officer for additional information.

#### **REPRODUCING CLASSIFIED DOCUMENTS**

Reproduction of classified documents must be limited to the minimum number of copies consistent with operational requirements and further reproduction limitations indicated on the document.

Reproduction of classified documents must be performed on machines located only within LAs or VTRs and that are specifically approved for classified reproduction. Contact your HSO for additional information.

#### **DESTROYING CLASSIFIED MATTER**

Multiple copies, obsolete documents, and classified waste must be destroyed when no longer required. When the decision is made to destroy classified matter, the actual destruction requires additional considerations.

The Centralized Classified Destruction Facility, is located at the Germantown facility for the bulk destruction of classified matter generated by Headquarters organizations. Offices wishing to maintain and use their own individual HSO-approved shredders must ensure that those shredders conform to the standards established by DOE Directives. Contact your HSO for further details about those organizational shredders approved for classified destruction.

Shredders approved by HSOs for classified destruction must be located in LAs or VTRs and must be designated by conspicuously posted signs.

All shredders located in an LA or VTR that are not approved for destruction of classified matter must have a Not Authorized for Classified Destruction sign posted on the shredder.

Paper, plastics, and metal are to be sorted into separate, properly annotated burn bags. Be sure to remove paper clips, and metal or plastic fasteners from all documents. The name, routing symbol, telephone number, and room number of the person responsible for the bag must be clearly marked on the side of each bag for identification. Red-stripe burn bags for classified waste and plain brown burn bags for UCNI or CUI waste are available in the self-service supply rooms.

Classified waste must be placed in red-striped burn bags and UCNI or CUI must be placed in plain brown burn bags prior to transport to the Germantown CCDF.

Both (candy striped or plain) bags must be annotated with the user's name and office location information and may not



exceed 15 pounds in weight at the Germantown facility and 10 pounds at the Forrestal facility collection areas. Always store classified waste in GSA-approved security containers or in vaults or vault-type rooms approved for classified open storage. If you make changes to your LA or VTR, to include moving your classified container, be sure to notify your HSO. Contact your HSO or consult Chapter 5 of the Master Plan for additional information regarding collection locations, destruction witnessing requirements, records of destruction, etc.

#### **CLASSIFIED REPOSITORIES AND STORAGE**

Unless a Security Area is approved for open storage, classified matter **MUST** be stored in GSA-approved security containers. Never store funds, firearms, medical items, or high theft items in containers that are used to store classified matter.

Always protect combinations to classified repositories, like a GSA-approved safe, security container or VTR, at the classification level and category of the information contained in the repository.

It's very important to understand that the combination itself must be protected as classified and stored in another classified storage repository at the equivalent or higher classification level.

Generally, combinations must be changed whenever personnel knowing the combination transfer, terminate employment, their security clearance is downgraded to a level lower than the matter stored in the repository, terminated, or when the combination is known or suspected to have been compromised.

Only an appropriately cleared and authorized individual may change classified repository combinations.

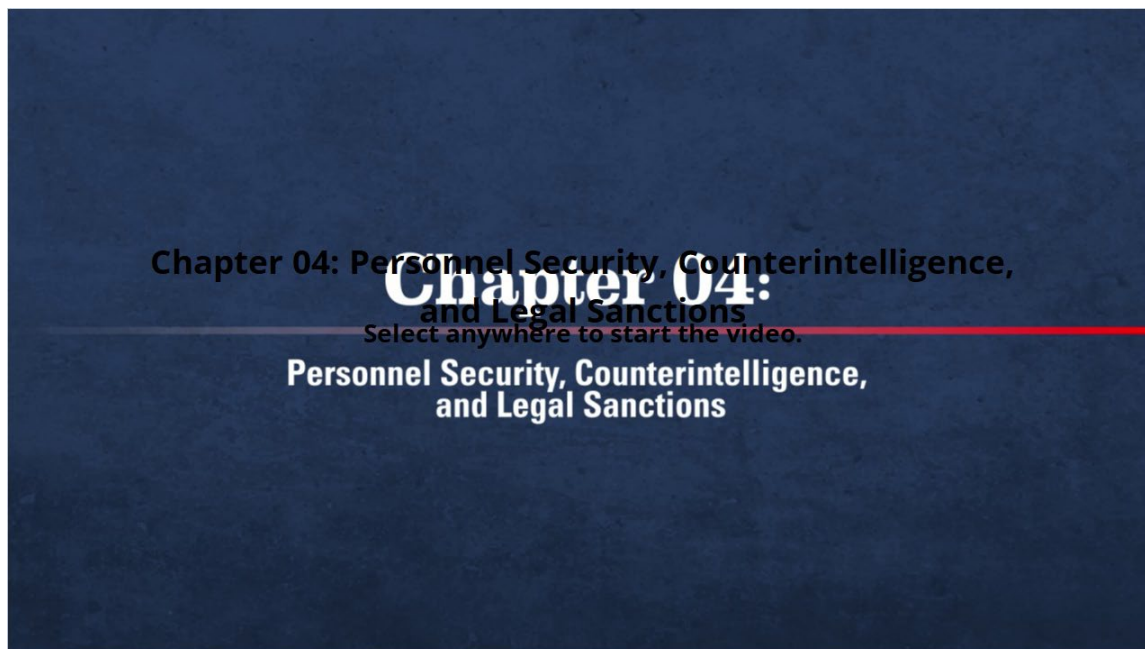
The SF 700, "Security Container Information," must be used to record security container combinations and the SF 700 must be protected as classified matter. Consult the Master Plan for additional information on the proper use and handling of the SF 700 and protecting and storing combinations to classified repositories.

The SF 702, "Security Container Check Sheet" must be used to record the times, dates, and the initials of individuals who have opened, closed, or checked a particular container, vault, or VTR.

The SF 701, "Activity Security Checklist," provides a systematic means of recording the checking of end-of-day activities for a particular work area approved for classified operations like LAs or VTRs. Contact your HSO for additional information about the use of security checklists in your area.

## **5. Personnel Security Counterintelligence and Legal Sanctions**

### **5.1 Personnel Security Program**



## Notes:

### PERSONNEL VETTING PROGRAM

The DOE Personnel Vetting Program is designed to ensure that individuals authorized to access classified information do not pose a threat to national security interests. This assurance is provided by the process for issuing initial and continuing security clearances, which is intended to ensure that only personnel who meet defined Federal standards for honesty, reliability, and trustworthiness are allowed such access.

## 5.2 Sources of Legal Authority & Guidance

# Authority and Guidance Documents

Sources of Legal Authority and Guidance

Within DOE HQ, the following directives have been adopted to implement the HQ Personnel Security Program: *To review, select the associated link.*

[Privacy Act of 1974](#)

[Title 10, Code of Federal Regulations, Part 707](#)

[Title 10, Code of Federal Regulations, Part 710](#)

[DOE Order 470.4B, Safeguards and Security Program](#)

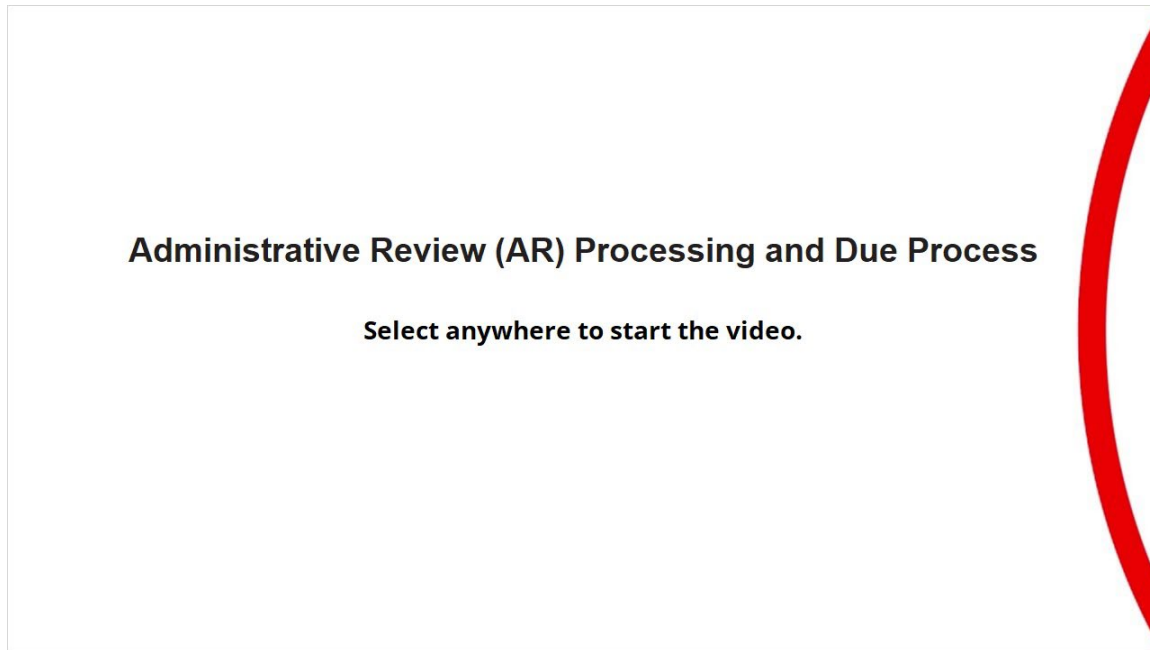
[DOE Order 472.2A, Personnel Security](#)

[DOE Order 475.1, Counterintelligence Program](#)

[Previous](#)   [Continue](#)

## Notes:

## 5.3 Adjudication Guidelines



### Notes:

#### **ADMINISTRATIVE REVIEW (AR) PROCESSING AND DUE PROCESS**

The Office of Headquarters Personnel Security Operations initiates an Administrative review (AR), outlined in 10 CFR 710, when an individual's eligibility for a security clearance has been suspended or cannot be granted because of unresolved security concerns.

#### **Request for Reconsideration**

The request for reconsideration must be submitted in writing to the Director, Office of Departmental Personnel Security, and accompanied by an affidavit detailing the new evidence or evidence of rehabilitation or reformation. The Office of Departmental Personnel Security notifies the individual if their security clearance eligibility will be reconsidered, and what actions will need to be taken before the decision regarding eligibility for a security clearance can be made.

For more information on security clearance action see Chapter 3, HQFMSP.

#### **Adjudication Factors and Guidelines**

DOE uses the National Security Adjudicative Guidelines to determine eligibility to be granted and to maintain access to classified information. In other words, security clearance adjudicative guidelines are used to determine eligibility for a security clearance. The government uses 13 adjudicative criteria, referred to as guidelines, for determining whether or not an individual should obtain access to classified information. Decisions are based on national security and a 'common sense' judgment of the person's overall trustworthiness. The 13 adjudicative criteria are:

## 5.4 Adjudication Criteria

### Adjudicative Criteria

|                          |             |
|--------------------------|-------------|
| <input type="checkbox"/> | Guideline A |
| <input type="checkbox"/> | Guideline B |
| <input type="checkbox"/> | Guideline C |
| <input type="checkbox"/> | Guideline D |
| <input type="checkbox"/> | Guideline E |
| <input type="checkbox"/> | Guideline F |
| <input type="checkbox"/> | Guideline G |
| <input type="checkbox"/> | Guideline H |
| <input type="checkbox"/> | Guideline I |
| <input type="checkbox"/> | Guideline J |
| <input type="checkbox"/> | Guideline K |
| <input type="checkbox"/> | Guideline L |
| <input type="checkbox"/> | Guideline M |

Select each Guideline for examples

Previous   Continue

Notes:

### Allegiance (Slide Layer)

### Adjudicative Criteria

|                          |             |
|--------------------------|-------------|
| <input type="checkbox"/> | Guideline A |
| <input type="checkbox"/> | Guideline B |
| <input type="checkbox"/> | Guideline C |
| <input type="checkbox"/> | Guideline D |
| <input type="checkbox"/> | Guideline E |
| <input type="checkbox"/> | Guideline F |
| <input type="checkbox"/> | Guideline G |
| <input type="checkbox"/> | Guideline H |
| <input type="checkbox"/> | Guideline I |
| <input type="checkbox"/> | Guideline J |
| <input type="checkbox"/> | Guideline K |
| <input type="checkbox"/> | Guideline L |
| <input type="checkbox"/> | Guideline M |

**Guideline A: Allegiance to the United States**



Previous   Continue



## Foreign Influence (Slide Layer)

# Adjudicative Criteria

☐ Guideline A

☐ Guideline B

☐ Guideline C

☐ Guideline D

☐ Guideline E

☐ Guideline F

☐ Guideline G

☐ Guideline H

☐ Guideline I

☐ Guideline J

☐ Guideline K

☐ Guideline L

☐ Guideline M

## Guideline B: Foreign Influence



Previous

Continue

## Foreign Preference (Slide Layer)

# Adjudicative Criteria

☐ Guideline A

☐ Guideline B

☐ Guideline C

☐ Guideline D

☐ Guideline E

☐ Guideline F

☐ Guideline G

☐ Guideline H

☐ Guideline I

☐ Guideline J

☐ Guideline K

☐ Guideline L

☐ Guideline M

## Guideline C: Foreign Preference



Previous

Continue

## Sexual Behavior (Slide Layer)

# Adjudicative Criteria

☐ Guideline A

☐ Guideline B

☐ Guideline C

☐ Guideline D

☐ Guideline E

☐ Guideline F

☐ Guideline G

☐ Guideline H

☐ Guideline I

☐ Guideline J

☐ Guideline K

☐ Guideline L

☐ Guideline M

## Guideline D: Sexual Behavior



Previous

Continue

## Personal Conduct (Slide Layer)

# Adjudicative Criteria

☐ Guideline A

☐ Guideline B

☐ Guideline C

☐ Guideline D

☐ Guideline E

☐ Guideline F

☐ Guideline G

☐ Guideline H

☐ Guideline I

☐ Guideline J

☐ Guideline K

☐ Guideline L

☐ Guideline M

## Guideline E: Personal Conduct



Previous

Continue

## Financial Considerations (Slide Layer)

# Adjudicative Criteria

☐ Guideline A

☐ Guideline B

☐ Guideline C

☐ Guideline D

☐ Guideline E

☐ Guideline F

☐ Guideline G

☐ Guideline H

☐ Guideline I

☐ Guideline J

☐ Guideline K

☐ Guideline L

☐ Guideline M

## Guideline F: Financial Considerations



Previous

Continue

## Alcohol Consumption (Slide Layer)

# Adjudicative Criteria

☐ Guideline A

☐ Guideline B

☐ Guideline C

☐ Guideline D

☐ Guideline E

☐ Guideline F

☐ Guideline G

☐ Guideline H

☐ Guideline I

☐ Guideline J

☐ Guideline K

☐ Guideline L

☐ Guideline M

## Guideline G: Alcohol Consumption



Previous

Continue



## Drug Involvement (Slide Layer)

# Adjudicative Criteria

☐ Guideline A

☐ Guideline B

☐ Guideline C

☐ Guideline D

☐ Guideline E

☐ Guideline F

☐ Guideline G

☐ Guideline H

☐ Guideline I

☐ Guideline J

☐ Guideline K

☐ Guideline L

☐ Guideline M

## Guideline H: Drug Involvement



Previous

Continue

## Psychological Conditions (Slide Layer)

# Adjudicative Criteria

☐ Guideline A

☐ Guideline B

☐ Guideline C

☐ Guideline D

☐ Guideline E

☐ Guideline F

☐ Guideline G

☐ Guideline H

☐ Guideline I

☐ Guideline J

☐ Guideline K

☐ Guideline L

☐ Guideline M

## Guideline I: Psychological Conditions



Previous

Continue



## Criminal Conduct (Slide Layer)

☐ Guideline A

☐ Guideline B

☐ Guideline C

☐ Guideline D

☐ Guideline E

☐ Guideline F

☐ Guideline G

☐ Guideline H

☐ Guideline I

☐ Guideline J

☐ Guideline K

☐ Guideline L

☐ Guideline M

# Adjudicative Criteria

## Guideline J: Criminal Conduct

A close-up photograph of a person's hands, palms facing each other, wearing metal handcuffs. The person is wearing a dark blue shirt and dark pants. The background is a plain, light-colored wall.

Previous

Continue

## Handling Protected Information (Slide Layer)

☐ Guideline A

☐ Guideline B

☐ Guideline C

☐ Guideline D

☐ Guideline E

☐ Guideline F

☐ Guideline G

☐ Guideline H

☐ Guideline I

☐ Guideline J

☐ Guideline K

☐ Guideline L

☐ Guideline M

# Adjudicative Criteria

## Guideline K: Handling Protected Information

A photograph of a person's hands writing on a document. The person is wearing a dark blue shirt. The document is on a clipboard, which is resting on a cardboard box. The background is a plain, light-colored wall.

Previous

Continue

---

Published by Articulate® Storyline [www.articulate.com](http://www.articulate.com)

## Outside Activities (Slide Layer)

# Adjudicative Criteria

☐ Guideline A

☐ Guideline B

☐ Guideline C

☐ Guideline D

☐ Guideline E

☐ Guideline F

☐ Guideline G

☐ Guideline H

☐ Guideline I

☐ Guideline J

☐ Guideline K

☐ Guideline L

☐ Guideline M

### Guideline L: Outside Activities



Previous

Continue

## Use of Information Technology Systems (Slide Layer)

# Adjudicative Criteria

☐ Guideline A

☐ Guideline B

☐ Guideline C

☐ Guideline D

☐ Guideline E

☐ Guideline F

☐ Guideline G

☐ Guideline H

☐ Guideline I

☐ Guideline J

☐ Guideline K

☐ Guideline L

☐ Guideline M

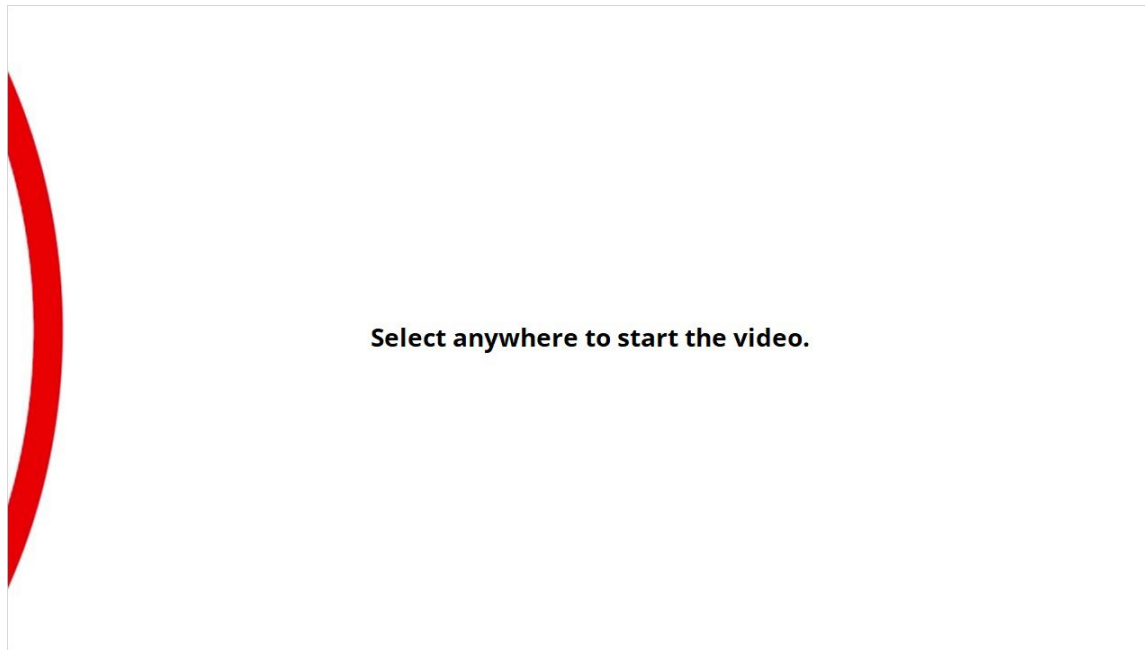
### Guideline M: Use of Information Technology Systems



Previous

Continue

## 5.5 FIS Threat



### Notes:

Each of these criteria are considered in light of the “whole-person” concept. The ‘whole-person’ concept refers to how a combination of variables are weighed some of these include the seriousness of conduct, frequency, motivation, and likeliness of recurrence. Access decisions also take into account a person's reliability, trustworthiness and ability to protect classified information. When a person's life history shows evidence of unreliability or untrustworthiness, questions arise whether the person can be relied on and trusted to exercise the responsibility necessary for working in a secure environment where protecting classified information is paramount. The bottom line, your ability to be granted and to maintain a security clearance is based on your trustworthiness, reliability, and loyalty to the U.S. government.

### THE FOREIGN INTELLIGENCE SERVICES THREAT

DOE research and development activity remains a high priority for foreign intelligence services. FIS agents often begin their targeting and recruitment of DOE Federal and contractor employees by identifying who has access to the information they need. FIS will conduct Internet or directory searches, review journals or other publications, and gather any available information useful when approaching and developing you as a source of information.

Through elicitation or surveillance methods, FIS agents are able to collect a wide variety of information about you such as biographical, professional, technical, and behavioral information. Additionally, if you conduct foreign travel, have foreign interactions, or attend conferences and symposiums, the chance of such collection activity is increased. Elicitation is the process of simply getting you to provide information, usually within a seemingly ordinary conversation, without being obvious to you that you're being asked a set list of questions. Taken together, elicitation responses may reveal your vulnerabilities.

## 5.6 Methods of Elicitation

# FIS Elicitation Methods

Some methods of elicitation include:

- Dropping a deliberate error into conversation that requires correcting.
- Expressing sympathy that a current project has been canceled.
- Outright flattery.
- Sharing mutual interests.
- Request for an individual to make a special presentation.

Be aware of the possibility of elicitation and employ these defensive measures:

- Avoid being steered into sensitive topics.
- Plead ignorance or being out of the loop if you find yourself in a sensitive area.
- Change the topic.
- Turn the conversation around by asking, "Why do you ask?"
- Include a co-worker in the conversation or just to observe.

Previous   Continue

Notes:

## 5.7 Risk Mitigation



Select anywhere to start the video.



## Notes:

Interactions with foreign nationals involving travel or hosting visits have resulted in reports indicating that FIS activity is targeting U. S. citizens. Your own awareness and vigilance about the potential threat from hostile intelligence targeting is critical.

Be aware of countries that may appear on the sensitive country list for reasons of national security, nuclear nonproliferation, regional instability, threat to national economic security, or terrorism support. The Forrestal Field Office maintains a list of sensitive countries.

### Risk Mitigation

Although the threat is real, your risk can be mitigated by following this simple advice:

Report personal and professional contacts with sensitive country foreign nationals.

Report official and unofficial travel to sensitive countries

Report any inappropriate requests for classified information, CUI, or UCNI

Notify the Forrestal Field Office, Office of Intelligence and Counterintelligence, and any anomalies or other indications that you or someone else may be the target of a foreign country's intelligence collection efforts.

For more information on the FIS threat and what to do about it contact your HSO or contact the Forrestal Field Office.

## UNAUTHORIZED DISCLOSURE

An unauthorized disclosure is a communication or physical transfer of sensitive information to an unauthorized recipient. Unauthorized disclosure may result in either a security infraction or a security violation.

### Security Infractions

A security infraction is any knowing, willful, or negligent action contrary to the requirements of the Atomic Energy Act of 1954 and/or Executive Order, that don't constitute a "violation." 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. Committing a security infraction can result in administrative discipline including loss of security clearance. The following incidents may be considered security infractions.

## 5.8 Security Infractions

# Security Infractions

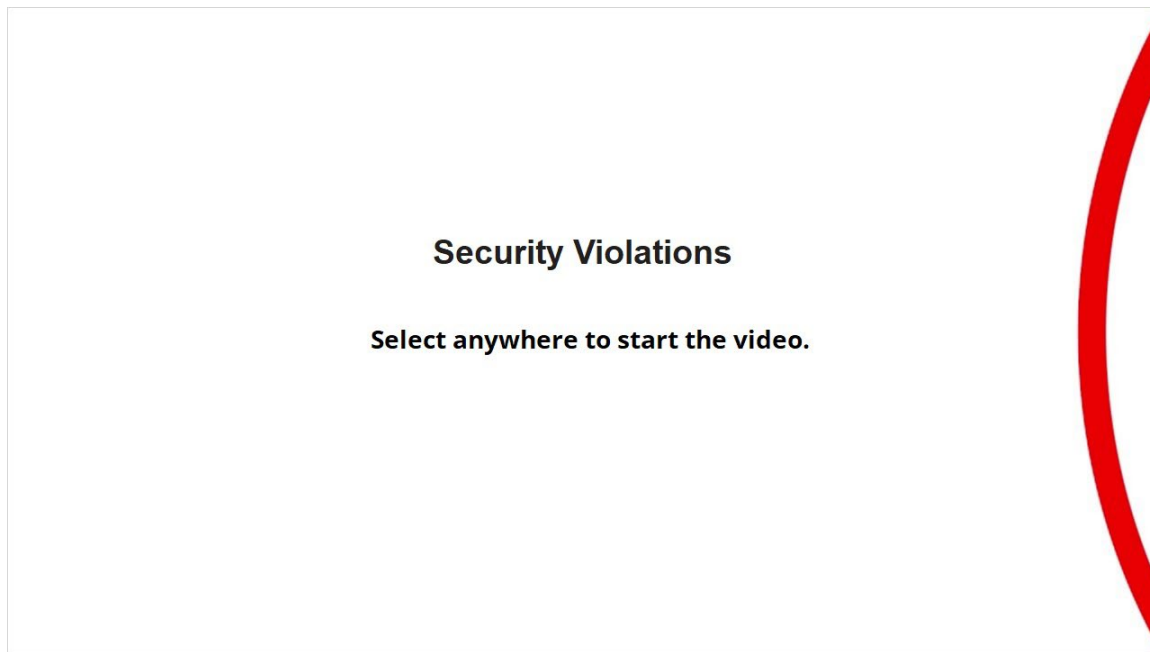
- Leaving classified documents or material exposed and unattended or unsecured, to include leaving a classified repository open and unattended.
- Failure to properly safeguard classified documents or combinations to repositories.
- Changing a document's classification marking without proper authority.
- Failure to have a document reviewed for classification, as required.
- Destruction of classified documents in other than the prescribed manner.
- Improper transmission of classified documents or material.
- Failure to escort uncleared persons within security areas.
- Failure to comply with Cyber Security Policy, i.e. sending classified information over an improper computer system.
- Unauthorized possession of prohibited articles in Headquarters facilities.

*Note: This list is not all-inclusive.*

[Previous](#)   [Continue](#)

## Notes:

## 5.9 Security Violations



### Notes:

#### **SECURITY VIOLATIONS**

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 known violations 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.

Punishment for a security violation may be severe.

Contact your HSO or consult the HQFMSP for additional information on these subjects.

#### **REPORTING RESPONSIBILITIES**

Incidents of Security Concern are events which are of concern to the DOE S&S Program that warrant preliminary inquiry and subsequent reporting. Knowing or willful involvement in an incident of security concern may have an impact on the individual's access and security clearance eligibility.

## 5.10 Incidents of Security Concern

# Reporting Responsibilities

Some information must be reported immediately and other reports may be delayed a day or two. The following is a sample list of reportable items that must be reported immediately.

- Incidents of safeguards and security concern including those involving classified information/matter or Special Nuclear Material.
- Criminal violations relating to DOE programs like fraud.
- Deliberate compromise or foreign involvement in suspected compromise of classified information.
- Violations of security regulations.



Select here for more information on reporting requirements.

[Previous](#)   [Continue](#)

Notes:

### RR1 (Slide Layer)

## Reporting Requirements

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 or holding a DOE security clearance. Such matters, listed below, must be reported verbally and directly to the Office of Departmental Personnel Security Operations immediately upon the individual becoming aware of the situation or incident, and in no later than two (2) working days after the event.

*NOTE: Federal management officials must report any conditions which could affect the status of an employee's or applicant's security clearance, including death, employment termination, or a change in circumstance such that the individual no longer requires access to classified information.*

*Contractors must report any potential employee who declines an offer of employment, fails to report to duty, is terminated, dies, or whose circumstances have changed such that the individual no longer requires access to classified information.*



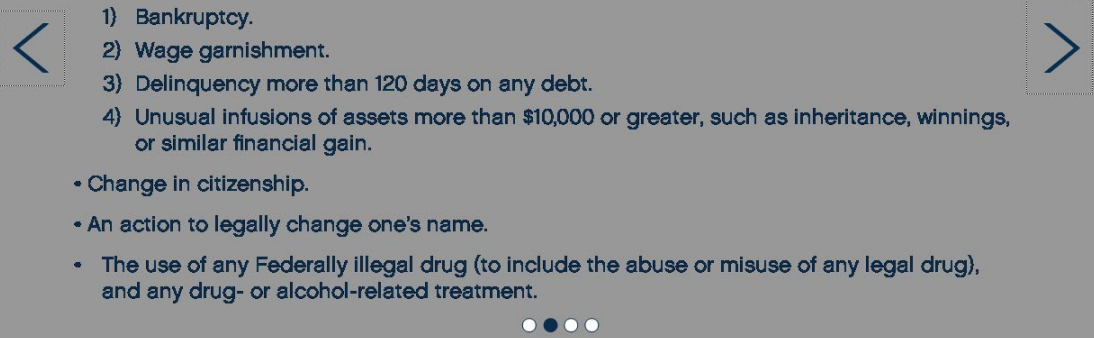
● ○ ○ ○ ○

## RR2 (Slide Layer)

### Reporting Requirements

Other reportable information includes, but is not limited to:

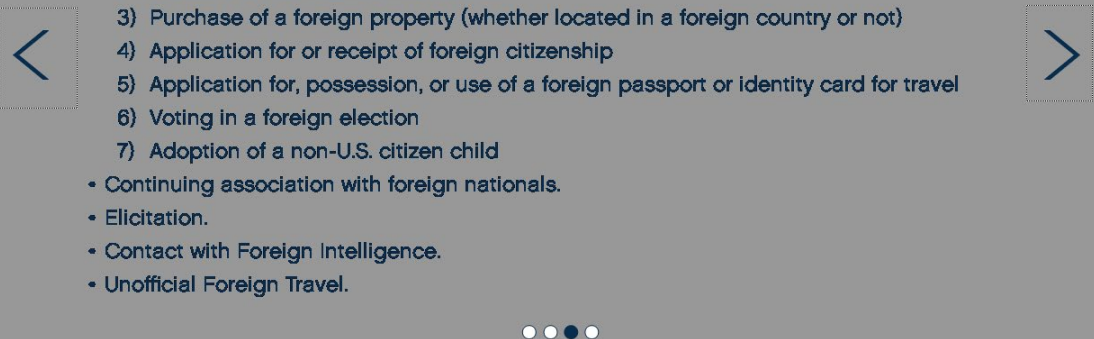
- Arrests, criminal charges (including charges that are dismissed), citations, tickets, summons, or detentions by Federal, state, or other law enforcement authorities for violations of law within or outside the U.S. Traffic violations for which a fine of less than \$300 was imposed need not be reported, unless the violation was alcohol- or drug-related.
- Financial anomalies including, but not limited to:
  - 1) Bankruptcy.
  - 2) Wage garnishment.
  - 3) Delinquency more than 120 days on any debt.
  - 4) Unusual infusions of assets more than \$10,000 or greater, such as inheritance, winnings, or similar financial gain.
- Change in citizenship.
- An action to legally change one's name.
- The use of any Federally illegal drug (to include the abuse or misuse of any legal drug), and any drug- or alcohol-related treatment.



## RR3 (Slide Layer)

### Reporting Requirements

- An immediate family member assuming residence in a sensitive country.
- Hospitalization for mental health reasons.
- Foreign activities, such as:
  - 1) Direct involvement in a foreign business
  - 2) Opening of a foreign bank account
  - 3) Purchase of a foreign property (whether located in a foreign country or not)
  - 4) Application for or receipt of foreign citizenship
  - 5) Application for, possession, or use of a foreign passport or identity card for travel
  - 6) Voting in a foreign election
  - 7) Adoption of a non-U.S. citizen child
- Continuing association with foreign nationals.
- Elicitation.
- Contact with Foreign Intelligence.
- Unofficial Foreign Travel.





## RR4 (Slide Layer)

Select here to close

### Reporting Requirements

- All reports of planned unofficial foreign travel must include, at a minimum, the following information as available and applicable:
  - 1) Full itinerary
  - 2) Dates of travel
  - 3) Mode(s) of transport, including identity of carriers
  - 4) Passport number
  - 5) Emergency point of contact
  - 6) Names and association of foreign national traveling companions
  - 7) Planned interactions with foreign governments, companies or citizens during travel and reasons for contact (routine travel/tourism-related contacts excepted)
- When the need for emergency unofficial foreign travel precludes full compliance with the above requirements, the individual must, at a minimum, verbally notify their supervisor/management chain concerning the nature of the emergency. Full reporting must be accomplished within five (5) working days of return.

<

● ● ● ● ●

## 5.11 Legal Administrative Sanctions

### Legal and Administrative Sanctions

Select anywhere to start the video.

### Notes:

#### LEGAL AND ADMINISTRATIVE SANCTIONS

Administrative and legal sanctions may be imposed on individuals who knowingly or willfully disregard security procedures and Federal regulations. Administrative Sanctions may include: reprimand, suspension, reassignment, termination of classification authority, loss or denial of security clearance, termination of employment, or other sanctions in accordance with

applicable laws and agency regulations.

## 5.12 Legal Sanctions

### Legal Sanctions

#### Legal Sanctions:

- Title 18, U.S.C. Section 793. Gathering, transmitting, or losing defense information.
- Title 18, U.S.C. Section 794. Gathering or delivering defense information to aid foreign government.
- Title 18, U.S.C. Section 798. Disclosure of classified information.
- Title 18, U.S.C. Section 1924. Unauthorized removal and retention of classified documents or material.
- An individual who has been found guilty of one or more of these felonies may be sentenced to pay a fine of not more than \$250,000 and may be imprisoned for any term of years or for life, or may be punished by death.
- Atomic Energy Act of 1954, section 224. Unauthorized Communication of Restricted Data shall be punished by imprisonment for life, or by imprisonment for any term of years or a fine of not more than \$100,000 or both.

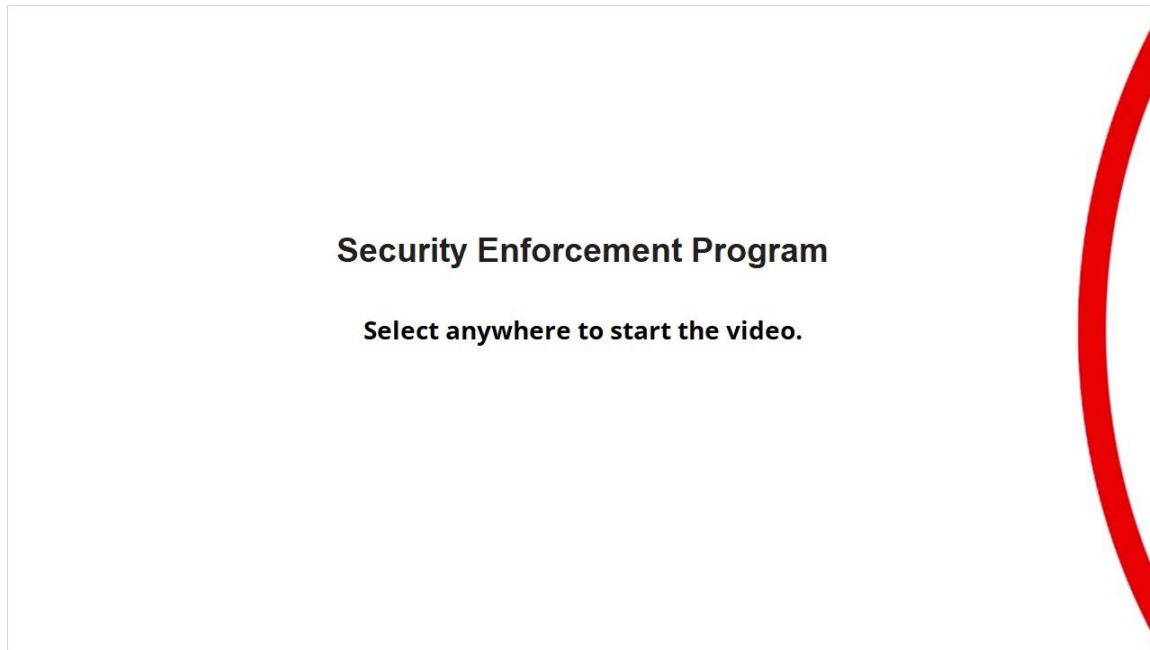
Previous



Continue

Notes:

## 5.13 Security Enforcement Program



### Notes:

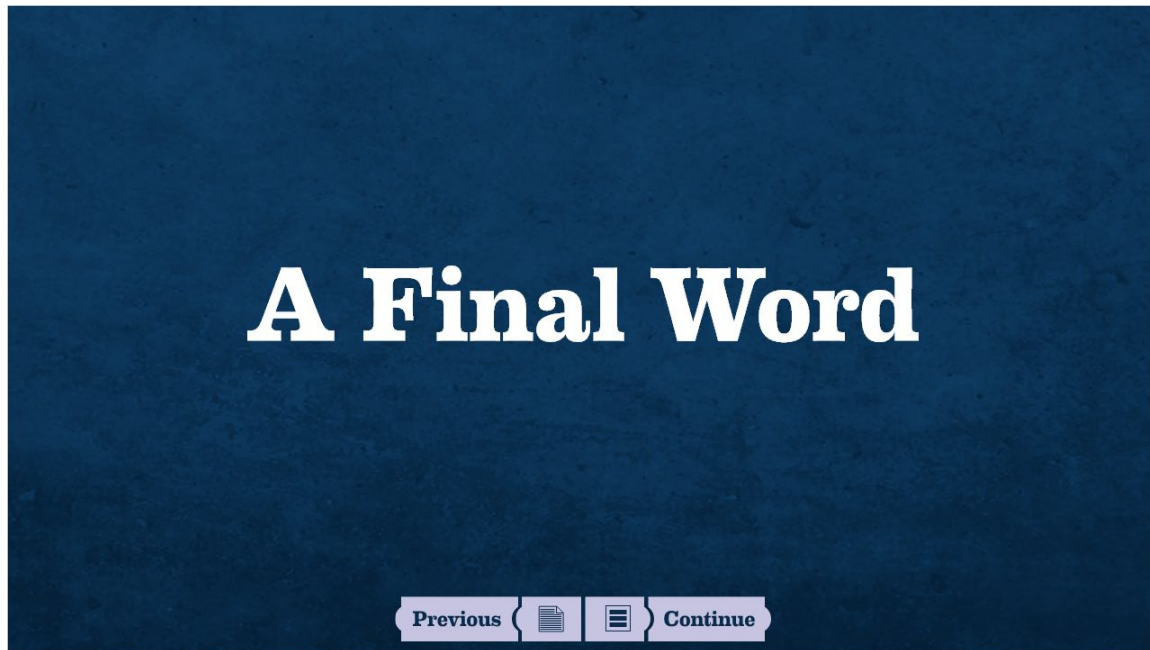
#### **SECURITY ENFORCEMENT PROGRAM**

The Security Enforcement Program is designed to implement the requirements of Title 10, Code of Federal Regulations, Part 824. This rule was published by DOE to implement Section 234B of the Atomic Energy Act of 1954. Section 234B stipulates that a contractor or subcontractor to the DOE who violates any rule, regulation, or order relating to the safeguarding or security of Restricted Data, other classified information, or sensitive information shall be subject to a civil penalty. In publishing 10 CFR Part 824, DOE has determined that civil penalties under Part 824 will only be assessed for violations of requirements for the protection of classified information (RD, FRD, TFNI and NSI).

#### **TERMINATION OF SECURITY CLEARANCE**

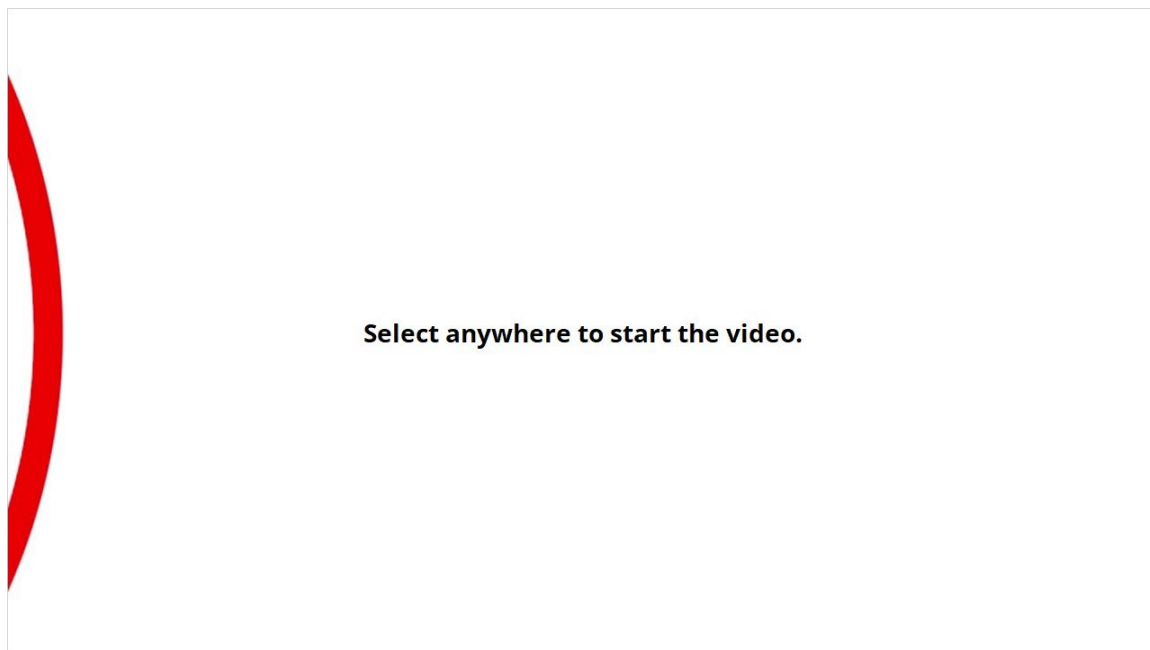
At such time your security clearance is terminated, it is your responsibility to complete a Security Termination Briefing. The Security Termination Briefing will reiterate: your continuing responsibility not to disclose classified information to which you had access, the potential penalties for noncompliance, and your obligation to return to DOE all documents and materials containing sensitive information. At the conclusion of the termination briefing you will be required to sign a Security Termination Briefing Statement and return your DOE security badge. In such cases, your first stop should be your HSO's office.

### ***5.14 Final Word Title***



**Notes:**

### ***5.15 Conclusion***





## Notes:

### A FINAL WORD

The work done by the Department of Energy is essential to the entire Nation. As a select member of the DOE community who has been granted a security clearance, you've been asked to participate in some of the most significant activities of the U.S. Government - the protection of our Nation's secrets. You're personally responsible for protecting sensitive information that is critical to the security of our country. If you have any questions regarding your responsibilities, please contact your HSO or the Office of Headquarters Security Operations at 301-903-9990.

You've completed the Headquarters Comprehensive Security Briefing. Please read and sign the "Classified Information Nondisclosure Agreement," SF 312 that you will be asked to sign when you pick up your DOE security badge at the badge office.

For additional information and more in-depth coverage of the Headquarters security program you're encouraged to review and print a copy of the Comprehensive Security Briefing book. The link is available in the reference section of this briefing. Don't forget to bring a copy of your certificate of completion verifying that you've finished this briefing. The certificate is available immediately following this presentation. Take a screen shot of the certificate and present it to the badge office when picking up your badge. You won't be issued a badge if you don't have proof of completing this briefing.

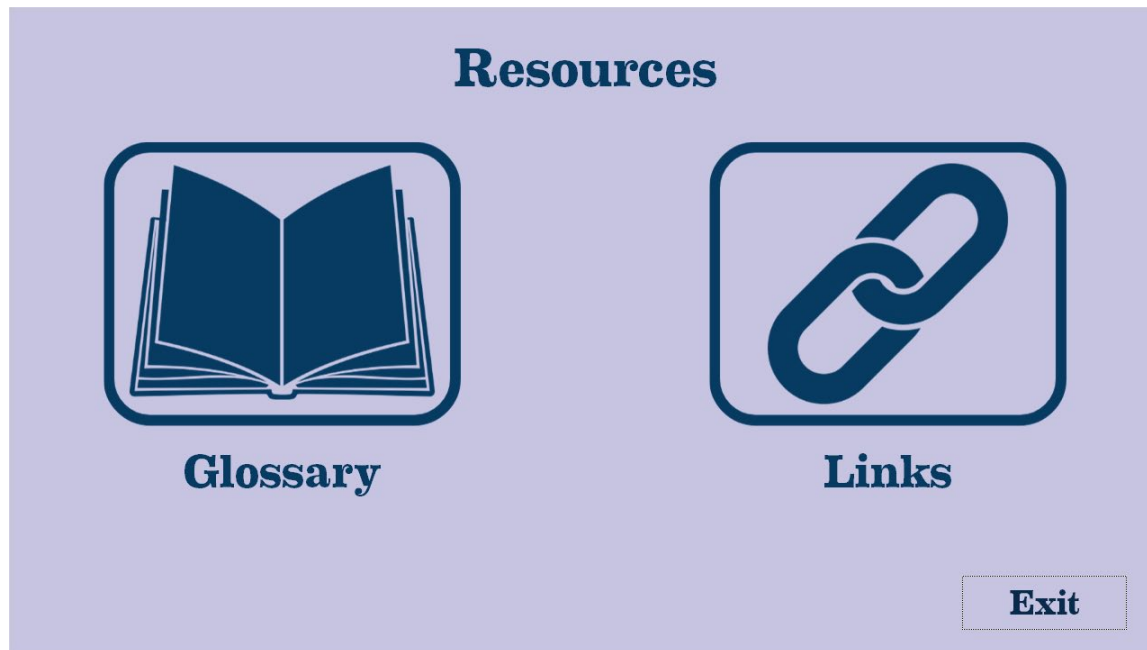
## 5.16 Exit Course



## Notes:

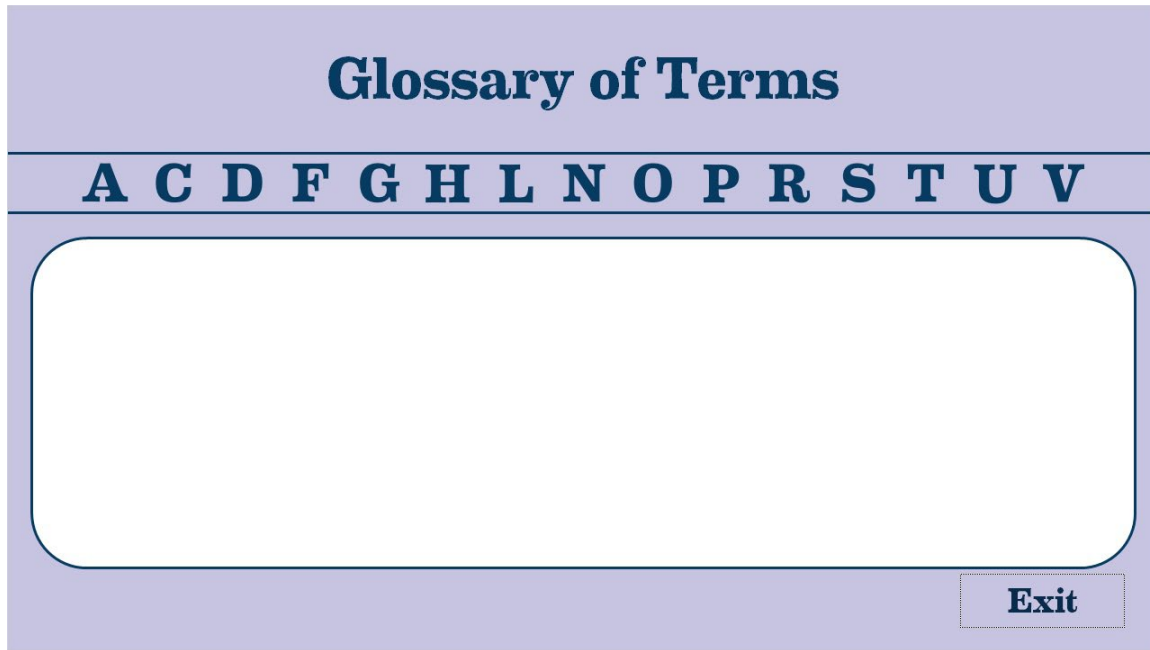
## 6. Resources

### 6.1 Resources



Notes:

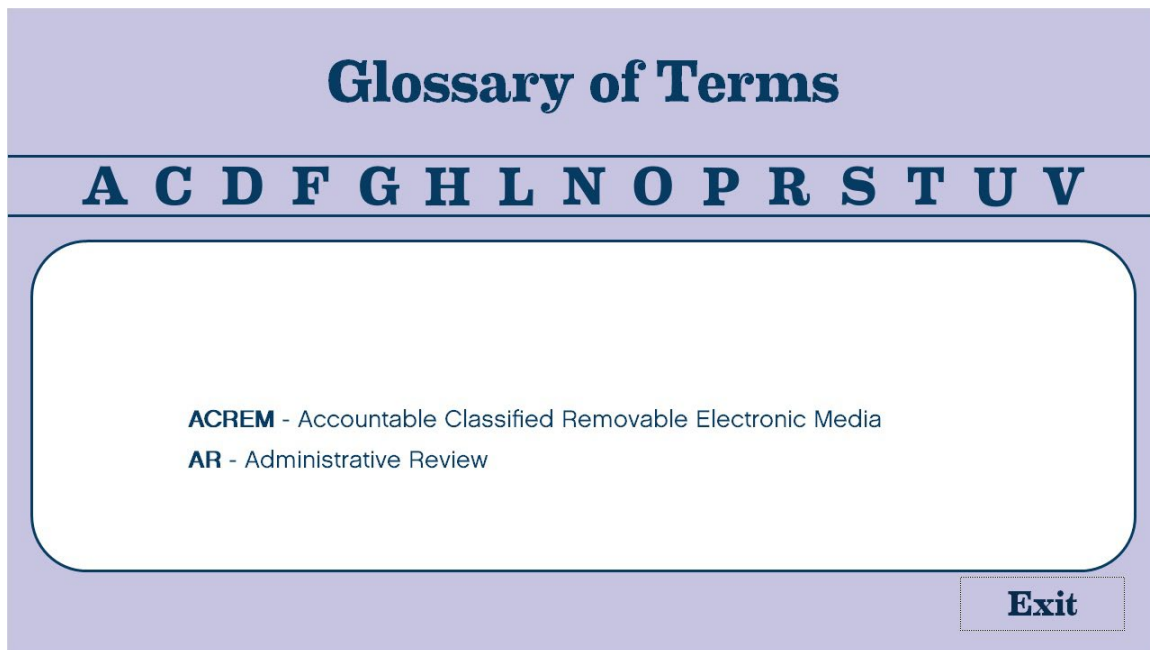
## 6.2 Glossary



A screenshot of a presentation slide titled "Glossary of Terms". The slide has a light purple background. At the top, the title "Glossary of Terms" is centered in a dark blue, serif font. Below the title is a horizontal bar with the letters "A C D F G H L N O P R S T U V" in a dark blue, serif font. Below this bar is a large, empty white rounded rectangle with a dark blue border. In the bottom right corner of the slide, there is a small rectangular button with a dashed border and the word "Exit" in a dark blue, serif font.

Notes:

A (Slide Layer)



A screenshot of a presentation slide titled "Glossary of Terms", similar to the one above but with content. The slide has a light purple background. At the top, the title "Glossary of Terms" is centered in a dark blue, serif font. Below the title is a horizontal bar with the letters "A C D F G H L N O P R S T U V" in a dark blue, serif font. Below this bar is a large white rounded rectangle with a dark blue border. Inside this rectangle, the following text is displayed in a dark blue, serif font:  
**ACREM** - Accountable Classified Removable Electronic Media  
**AR** - Administrative Review  
In the bottom right corner of the slide, there is a small rectangular button with a dashed border and the word "Exit" in a dark blue, serif font.

**C (Slide Layer)**

## Glossary of Terms

**A C D F G H L N O P R S T U V**

**CCDF** – Centralized Classified Destruction Facility

**CDC** - Classified Document Control

**CMA** - Classified Mailing Address

**CMPC** - Classified Matter Protection and Control

**CNWDI** - Critical Nuclear Weapons Design Information

**CREM** - Classified Removable Electronic Media

**CTS** - Cosmic Top Secret

**CUI** – Controlled Unclassified Information

Exit

**D (Slide Layer)**

## Glossary of Terms

**A C D F G H L N O P R S T U V**

**DOE** - Department of Energy

Exit



## F (Slide Layer)

# Glossary of Terms

**A C D F G H L N O P R S T U V**

**FFO** - Forrestral Field Office  
**FGI** - Foreign Government Information  
**FIS** - Foreign Intelligence Services Threat  
**FOIA** - Freedom of Information Act  
**FRD** - Formerly Restricted Data

**Exit**

## G (Slide Layer)

# Glossary of Terms

**A C D F G H L N O P R S T U V**

**GAA** - General Access Area

**Exit**

## H (Slide Layer)

### Glossary of Terms

**A C D F G H L N O P R S T U V**

**HQFMSP** - Headquarters Facility Master Security Plan  
**HSO** - Headquarters Security Officer

Exit

## L (Slide Layer)

### Glossary of Terms

**A C D F G H L N O P R S T U V**

**LA** - Limited Areas

Exit

## N (Slide Layer)

### Glossary of Terms

**A C D F G H L N O P R S T U V**

**NATO** - National Atlantic Treaty Organization

**NC** - NATO Confidential

**NOFORN** - No Foreign Dissemination

**NR** - NATO Restricted

**NS** - NATO Secret

**NSI** - National Security Information

Exit

## O (Slide Layer)

### Glossary of Terms

**A C D F G H L N O P R S T U V**

**ORCON** - Originator Controlled

**OUO** - Official Use Only

Exit

**P (Slide Layer)**

## Glossary of Terms

**A C D F G H L N O P R S T U V**

**PII** - Personally Identifiable Information

**PPA** - Property Protection Area

**PROPIN** - Proprietary Information

Exit

**R (Slide Layer)**

## Glossary of Terms

**A C D F G H L N O P R S T U V**

**RD** - Restricted Data

**REL** - Authorized for Release to Country

**RELINDO** - Releasable by Information Disclosure Official

Exit



**S (Slide Layer)**

## Glossary of Terms

**A C D F G H L N O P R S T U V**

**S/RD** - Secret Restricted Data

Exit

**T (Slide Layer)**

## Glossary of Terms

**A C D F G H L N O P R S T U V**

**TFNI** - Transclassified Foreign Nuclear Information

Exit

## U (Slide Layer)

### Glossary of Terms

**A C D F G H L N O P R S T U V**

**UCNI** - Unclassified Controlled Nuclear Information

**Exit**

## V (Slide Layer)

### Glossary of Terms

**A C D F G H L N O P R S T U V**

**VTR** - Vault Type Rooms

**Exit**

## 6.3 Guiding Documents



# Reference Documents

[10 CFR 1017, Identification and Protection of Unclassified Controlled Nuclear Information](#)

[10 CFR 1045, Nuclear Classification and Declassification](#)

[32 CFR Part 2001, Classified National Security Information](#)

[Classification Review Requirements](#)

[CMPC Marking Resource](#)

[DOE Order 470.4B, Safeguards and Security Program](#)

[DOE O 471.1B, Identification and Protection of Unclassified Controlled Nuclear Information](#)

[DOE Order 472.2A, Personnel Security](#)

[DOE Order 475.1, Counterintelligence Program](#)

[DOE Order 475.2B, Identifying Classified Information](#)

[DOE Order 486.1A, Foreign Government Talent Recruitment Program](#)

[E.O. 13526, Classified National Security Information](#)

[Foreign National Visits & Assignments Questionnaire](#)

[Headquarters Facilities Master Security Plan, "Master Plan"](#)

[Privacy Act of 1974](#)

[Title 10, Code of Federal Regulations, Part 707](#)

[Title 10, Code of Federal Regulations, Part 710](#)

[UCNI Marking: Additional Information](#)

[UCNI Safeguarding Quick Reference Guide](#)

**Exit**

**Notes:**