

HQ-110DE_Initial_Security_Briefing

1. Course Information and Main Menu

1.1 Screen Reader Instructions

HQ-110DE, INITIAL SECURITY BRIEFING

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 Screen Reader Navigation Instructions to fully understand how the course functions with the screen reader.

Screen Reader Navigation Instructions are available on the Navigation Instructions screen, as well as by **selecting the following link:**

[Screen Reader Navigation Instructions](#)



Select the start button to begin the course.

Notes:

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 Screen Reader Navigation Instructions to fully understand how the course functions with the screen reader. Screen Reader Navigation Instructions are available on the Navigation Instructions screen, as well as by selecting the following link: [Screen Reader Navigation Instructions](#).
Select here to start the course.

1.2 Splash screen with music



Notes:

[Music]

1.3 Navigation Instructions

NAVIGATION INSTRUCTIONS

Navigation

To navigate through the course, use the navigation buttons at the upper right or follow the directions on the screen.

Audio and Video

This course contains audio and video. Please prepare your speakers or headphones and follow the instructions below.

- To pause or restart video play, use the player control bar at the bottom of the screen or select any area on the video.
- The Closed Caption button appears at the lower right, only on screens with video.
- To view the narration transcript, select the Transcript button at the upper right.
- For Screen Reader Navigation Instructions, select the following link:
[Screen Reader Navigation Instructions](#)

Back
Main Menu
Resources
Forward

Notes:

Navigation

To navigate through the course, use the navigation buttons at the upper right or follow the directions on the screen.

Audio and Video

This course contains audio and video. Please prepare your speakers or headphones and follow the instructions below.

- To pause or restart video play, use the player control bar at the

bottom of the screen or select any area on the video.

- The closed caption button appears at the lower left, only on narrated screens.
- To view narration transcripts, click the Transcripts button at the upper right.

For Screen Reader Navigation Instructions, select [here](#).

1.4 Course Information

COURSE INFORMATION

 Length	 Credit	 Completion
This course takes about 60 minutes to complete. If you need to stop before finishing, close the browser window and the Learning Management System (LMS) will do the following: • Report the course "In Progress" and bookmark your place. • The system will save your last completed page so that when you return, you may select the "Resume" option.	You must meet the following requirements to receive credit: • View all pages and complete all activities. • Complete the NTC Student Feedback Form.	When you have satisfied the requirements of this course, the LMS will automatically log your completion and add the completed course to your transcript. You can access your certificate from the LMS Transcript tab and print it or email it to your training point-of-contact or supervisor.

Notes:

Length

This course takes about 60 minutes to complete. If you need to stop before finishing, close the browser window and the Learning Management System (LMS) will do the following:

- Report the course "In Progress" and bookmark your place.
- When you return, select "Resume" and the course will open at your last completed page.

Credit

You must meet the following requirements to receive credit:

- View all pages and complete all activities.
- Complete the NTC Student Feedback Form.

Completion

When you have satisfied the requirements of this course, the NTC LMS

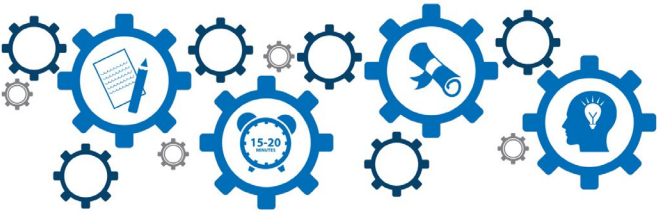
will automatically log your completion and add the completed course to your transcript. You can access your certificate from the LMS Transcript tab and print it or email it to your training point-of-contact or supervisor.

1.5 Additional Information

ADDITIONAL INFORMATION

For optimal learning, follow the recommendations below:

- Complete only one or two topics at a time and write down key points as you go along.
- Take a break every 15-20 minutes to reflect on what you have learned. When taking a break, close your browser window to save your progress.



Notes:

For optimal learning, follow the below recommendations:

- Complete only one or two topics at a time and write down key points as you go along.
- Take a break every 15-20 minutes to reflect on what you have learned. When taking a break, close your browser window to save your progress.

1.6 Goal and Objectives

GOAL AND OBJECTIVES

Upon completion of this course, students will be able to do the following:

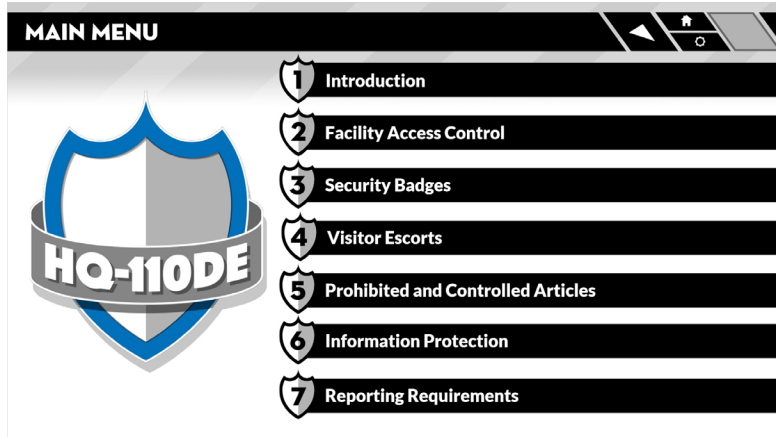
- Understand the importance of employee involvement in security at DOE Headquarters (HQ) facilities.
- Identify the requirements for facility access at DOE HQ.
- Identify the requirements for when and where to wear badges, how to respond to a lost or stolen badge, and returning badges upon termination of employment.
- Identify when visitors must be escorted and the duties of an escort in a Limited Area (LA) or Vault-Type Room (VTR) with an uncleared visitor.
- Identify prohibited and controlled articles and the conditions where they may be permitted.
- Identify unclassified, controlled unclassified, and classified information, and the handling and storage requirements for each.
- Identify examples of suspicious behavior and security infractions and when they must be reported.

Notes:

Upon completion of this course, students will be able to:

- Understand the importance of employee involvement in security at DOE Headquarters (HQ) facilities.
- Identify the requirements for facility access at DOE HQ.
- Identify the requirements for when and where to wear badges, how to respond to a lost or stolen badge, and returning badges upon termination of employment.
- Identify when visitors must be escorted and the duties of an escort in a Limited Area (LA) or Vault-Type Room (VTR) with an uncleared visitor.
- Identify prohibited and controlled articles and the conditions where they may be permitted.
- Identify unclassified, controlled unclassified, and classified information, and the handling and storage requirements for each.
- Identify examples of suspicious behavior and security infractions and when they must be reported.

1.7 Main Menu



Notes:

Main Menu

1. Introduction
2. Facility Access Control
3. Security Badges
4. Visitor Escorts
5. Prohibited and Controlled Articles
6. Information Protection
7. Reporting Requirements

2. Part 1 - Introduction

2.1 Introduction



Notes:

Your Security Involvement

To start the introduction video, **select the image below.**

2.2 Video Intro



Notes:

Welcome to the Department of Energy.
Our philosophy at DOE HQ is that “**security cannot succeed without your involvement.**” Although this statement may seem basic, we cannot stress enough its importance.

You are critical to ensuring a safe, secure workplace - just by making security a routine part of your job responsibilities.

Why Is Security So Important?

To begin, there is the current world situation. With the threat of terrorism a very real possibility, effective security has probably never been so important for all government entities.

In addition, DOE ensures the future of the nation by advancing the national, economic, and energy security of the United States. The search for reliable, clean, and affordable energy promotes America's energy security. Our scientific and technological innovations maintain our economic competitiveness while improving our quality of life.

What is Your Security Role and Your Responsibilities?

Given the many reasons to make security a priority at DOE, it is vital that you know and follow your responsibilities in these efforts.

This briefing will cover the following areas:

- Facility access control at DOE facilities
- Badge requirements
- Escort requirements in Property Protection and Security Areas
- Prohibited and controlled articles
- Information protection, and
- Reporting requirements

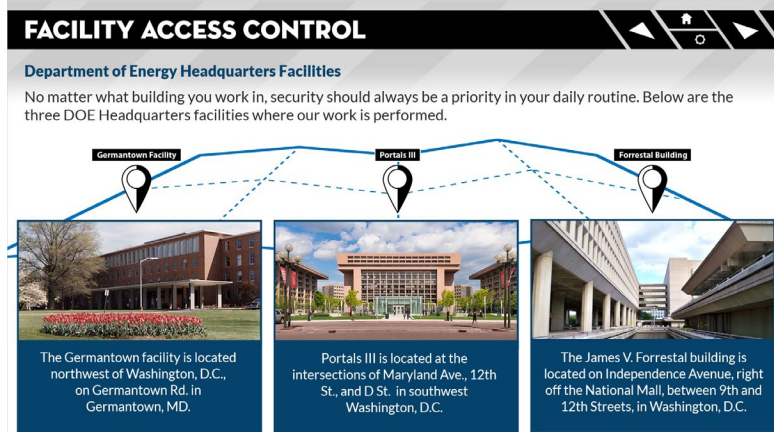
The security responsibilities for most employees will center on:

- The proper use of their DOE security badge, and
- The proper handling of government information

Let's get started.

3. Part 2 - Facility Access Control

3.1 DOE HQ Facilities



Notes:

DOE HQ Facilities

No matter what building you work in, security should always be a priority in your daily routine. **Select each marker to learn more about DOE HQ facilities where our work is performed.**

Forrestal Building

The James V. Forrestal building is located on Independence Avenue, right off the National Mall, between 9th and 12th Streets, in Washington, D.C.

Portals III (Washington, D.C.)

Portals III is located in Washington, D.C.

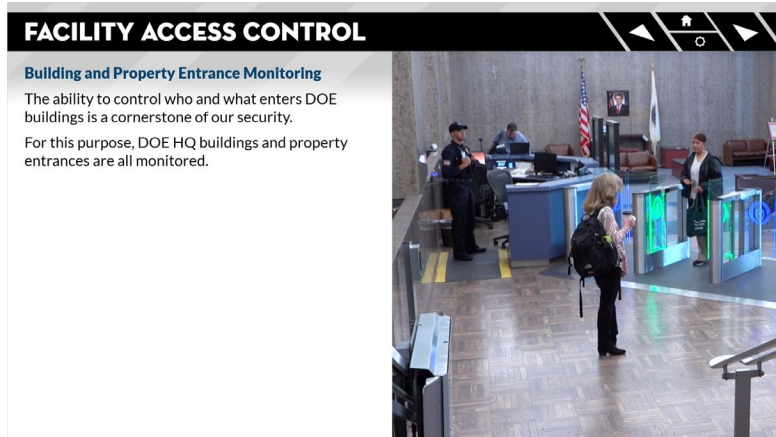
Germantown Facility (Germantown, MD)

The Germantown facility is made up of several buildings located northwest of Washington, D.C., in Germantown, Maryland.

Corporate 270 (Germantown, MD)

Corporate 270 is located in Germantown, not far from DOE HQ.

3.2 Building and Property Entrance Monitoring

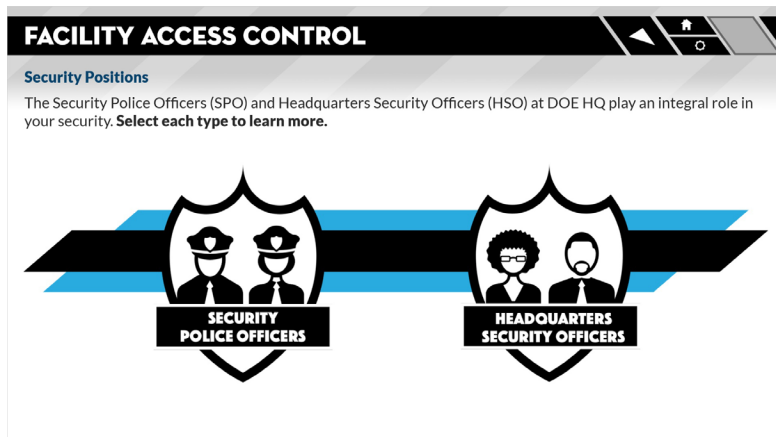


Notes:

Building and Property Entrance Monitoring

The ability to control who and what enters DOE buildings is a cornerstone of our security. For this purpose, DOE HQ buildings and property entrances are all monitored.

3.3 Security Positions



Notes:

Security Positions

The Security Police Officers (SPO) and Headquarters Security Officers (HSO) at DOE HQ play an integral role in your security. **Select each**

type to learn more.

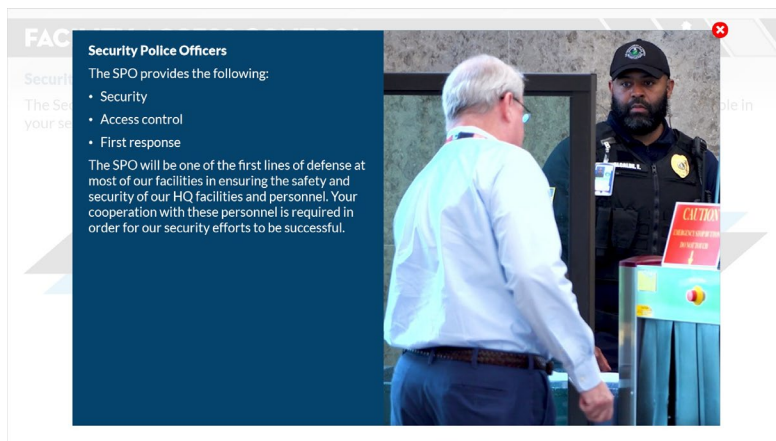
DOE Security Police Officers

The HQ SPO provides security, access control and first response. The SPO will be one of the first lines of defense at most of our facilities in ensuring the safety and security of our HQ facilities and personnel. Your cooperation with these personnel is required in order for our security efforts to be successful.

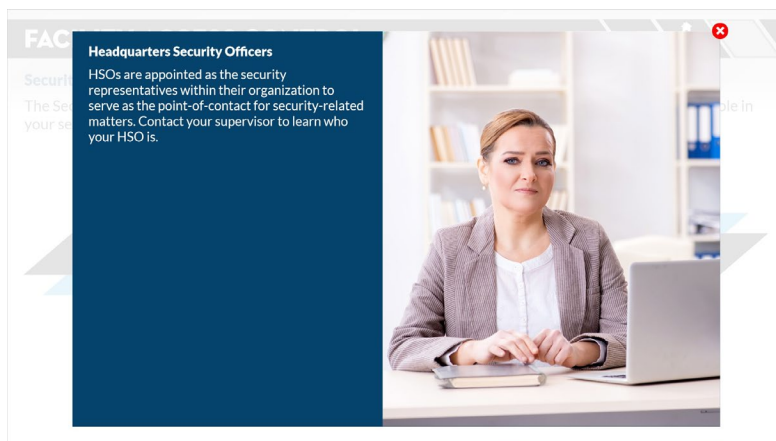
Headquarters Security Officers

HSOs are appointed as the security representatives within their organization to serve as the point-of-contact for security-related matters. Contact your supervisor to learn who your HSO is.

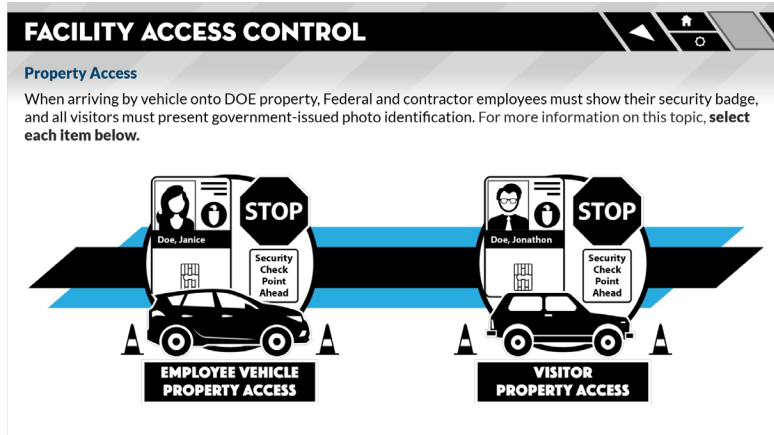
SPO (Slide Layer)



HSO (Slide Layer)



3.4 Property Access



Notes:

Property Access

When arriving by vehicle onto DOE property, Federal and contractor employees must show their security badge, and all visitors must present government-issued photo identification. For more information on this topic, **select each item below.**

Employee Vehicle Property Access

Federal and contractor employees arriving by vehicle must show their security badge to the SPO to gain entry onto the property.

All vehicles driven by badged DOE employees are subject to random vehicle inspection when entering the property.

An unbadged driver is allowed to drop off a badged employee; however, the driver must immediately depart from the property.

Visitor Property Access

All visitors arriving by vehicle onto DOE property must present government-issued photo identification (i.e., a driver's license) for inspection by the SPO.

The SPO will inspect all visitor vehicles prior to granting entry onto DOE property.

Employees hosting visitors should advise their visitors in advance that:

- They are required to have identification documents
- Their vehicle will be inspected, and
- They should plan for the additional time it will take them to be processed onto the property

Employee Vehicle Property Access (Slide Layer)

Employee Vehicle Property Access

Federal and contractor employees arriving by vehicle must show their security badge to the SPO to gain entry onto the property.

All vehicles driven by badged DOE employees are subject to random vehicle inspection when entering the property.

An unbadged driver is allowed to drop off a badged employee; however, the driver must immediately depart from the property.



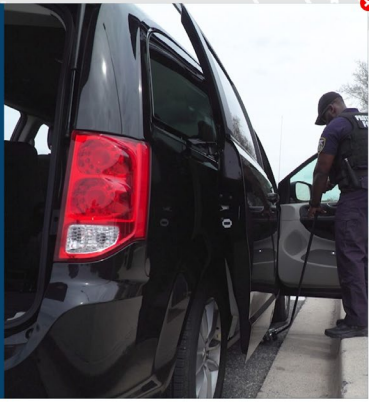
Visitor Property Access (Slide Layer)

Visitor Property Access

All visitors arriving by vehicle onto DOE property must present government-issued photo identification (for example, a driver's license) for inspection by the SPO.

The SPO will inspect all visitor vehicles prior to granting entry onto DOE property. Employees hosting visitors should advise their visitors in advance of the following:

- They are required to have identification documents
- Their vehicle will be inspected
- They should plan for the additional time it will take them to be processed onto the property



3.5 Safe Driving

FACILITY ACCESS CONTROL

Safe Driving
All drivers MUST be extremely attentive when entering or driving on DOE property. Speed limits are strictly enforced by the Federal Protective Service (FPS), which exercises jurisdiction for law enforcement activities at DOE facilities.



Notes:

Safe Driving

All drivers MUST be extremely attentive when entering or driving on DOE property. Speed limits are strictly enforced by the Federal Protective Service (FPS), which exercises jurisdiction for law enforcement activities at DOE facilities.

3.6 Vehicle Barriers

FACILITY ACCESS CONTROL

Vehicle Barriers
All drivers should be extremely attentive when entering DOE property to ensure that the active vehicle barrier is lowered prior to driving through.



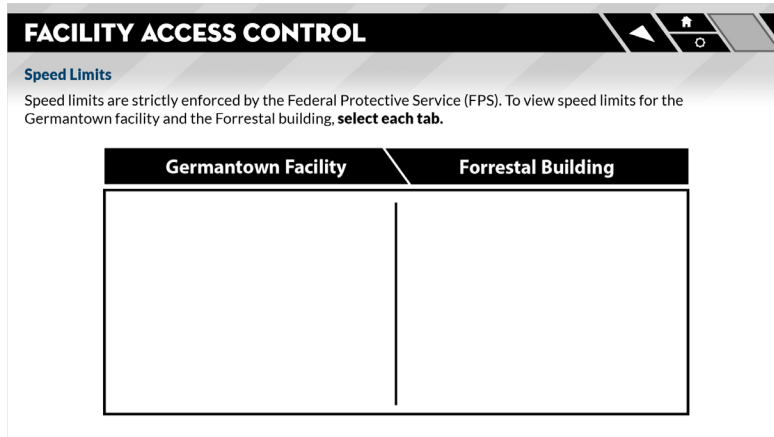
Notes:

Vehicle Barriers

All drivers should be extremely attentive when entering DOE property

to ensure that the active vehicle barrier is lowered prior to driving through.

3.7 Speed Limits



Notes:

Speed Limits

Speed limits are strictly enforced by the FPS. To view speed limits for the Germantown facility and Forrestal building, **select each tab.**

Germantown Facility Speed Limits

The posted speed limits at the Germantown compound are:

- 15 mph on main roads
- 10 mph in parking areas, and
- 5 mph when approaching, entering, and exiting gate areas

Forrestal Building Speed Limits

The posted speed limit in the Forrestal building parking garage is 5 mph.

Germantown (Slide Layer)

FACILITY ACCESS CONTROL

Speed Limits

Speed limits are strictly enforced by the Federal Protective Service (FPS). To view speed limits for the Germantown facility and the Forrestal building, **select each tab**.

Germantown Facility	Forrestal Building
Germantown Facility Speed Limits The posted speed limits at the Germantown compound are the following: • 15 mph on main roads • 10 mph in parking areas • 5 mph when approaching, entering, and exiting gate areas	

Forrestal (Slide Layer)

FACILITY ACCESS CONTROL

Speed Limits

Speed limits are strictly enforced by the Federal Protective Service (FPS). To view speed limits for the Germantown facility and the Forrestal building, **select each tab**.

Germantown Facility	Forrestal Building
	Forrestal Building Speed Limits The posted speed limit in the Forrestal building parking garage is 5 mph.

3.8 Security Inspections

FACILITY ACCESS CONTROL

Security Inspections

HQ maintains two levels of security for entering and exiting facilities. These levels are determined by the time of day and are referred to as "non-security hours" and "security hours." **Review the non-security and security hours below.**

Non-Security Hours (6:00 A.M. - 7:00 P.M.):
All personnel with temporary badges, and randomly selected individuals with a permanent badge, are subject to inspection (including hand-carried items) by the SPO when entering or exiting HQ facilities.

Security Hours
Monday - Friday: 7:00 P.M. - 6:00 A.M.
Weekends: Friday 7:00 P.M. - Monday 6:00 A.M.
Holidays: 7:00 P.M. on the evening preceding a non-Federal work day through 6:00 A.M. on the next Federal work day



Notes:

Security Inspections

HQ maintains two levels of security for entering and exiting facilities. These levels are determined by the time of day and are referred to as “non-security hours” and “security hours.” Review the non-security and security hours below.

Non-Security Hours (6am - 7pm):

All personnel with temporary badges and randomly selected individuals with a permanent badge are subject to inspection (including hand carried items) by the SPO when entering or exiting HQ facilities.

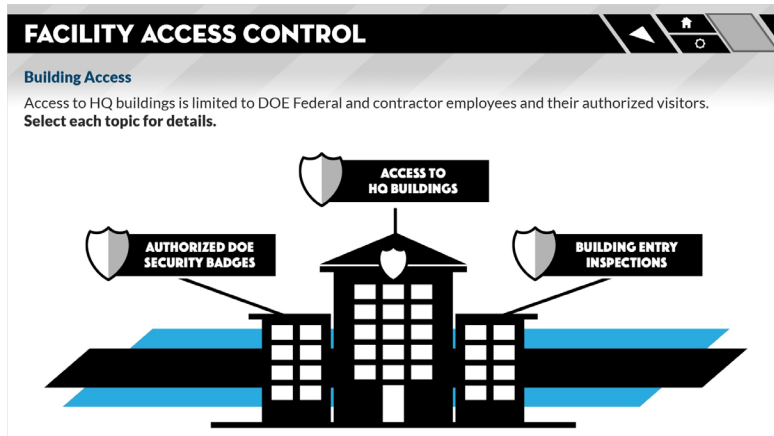
Security Hours:

Monday - Friday: 7:00 P.M. - 6:00 A.M.

Weekends: Friday 7:00 P.M - Monday 6:00 A.M., and

Holidays: 7:00 P.M. on the evening preceding a non-Federal work day through 6:00 A.M. on the next Federal work day

3.9 Building Access



Notes:

Building Access

Access to HQ buildings is limited to DOE Federal and contractor employees and their authorized visitors. **Select each topic for details.**

Authorized DOE Security Badges (Slide Layer)

FAC
Building
Access
Select

Authorized DOE Security Badges

During all hours, employees with authorized DOE security badges are granted facility access without having to sign in at the facility's main entrance.

Employees who arrive to work without their security badge may sign themselves in at the facility main entrance lobby once the SPO or receptionist has verified their identity. These employees will be issued a temporary badge.



Access to HQ Buildings (Slide Layer)

FAC
Building
Access
Select

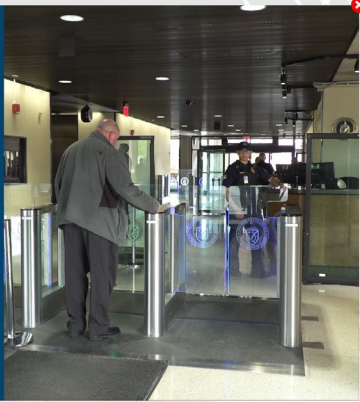
Access To HQ Buildings

Access to HQ buildings is controlled by a combination of the following:

- Automated turnstiles
- Badge readers
- Protective Force personnel

To gain entry, most employees use their permanent DOE security badge by placing it against the badge reader and waiting for the device to activate.

When exiting an HQ building, employees are required to use their security badge in the same fashion as when they enter the facility.



Building Entry Inspections (Slide Layer)

FAC
Building
Access
Select

Building Entry Inspections

Visitors, as well as employees or contractors issued temporary badges, will be inspected, along with their hand-carried items, upon building entry.

They may also be subject to inspection when exiting.

Employees with DOE security badges may be randomly inspected when entering or leaving the facilities.



4. Lightboxes

4.1 Resources

RESOURCES



Acronyms

Reference Documents

Navigation Instructions

Notes:

4.2 Navigation Instructions

NAVIGATION INSTRUCTIONS

Navigation

To navigate through the course, use the navigation buttons at the upper right or follow the directions on the screen.

Audio and Video

This course contains audio and video. Please prepare your speakers or headphones and follow the instructions below.

- To pause or restart video play, use the player control bar at the bottom of the screen or select any area on the video.
- The Closed Caption button appears at the lower left, only on narrated screens.
- To view the narration transcript, select the Transcript button at the upper right.
- For Screen Reader Navigation Instructions, select the following link:

[Screen Reader Navigation Instructions](#)



Back

Main Menu

Resources

Forward

Notes:

4.3 Reference Documents



[Headquarters Facilities Master Security Plan \(HQFMSP\)](#)

[DOE Order 470.4B Chg 3 \(LtdChg\) Safeguards and Security Program](#)

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

[DOE Order 471.7 Controlled Unclassified Information \(CUI\)](#)

[DOE Order 473.1A Physical Protection Program](#)

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

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

[Safeguarding UCNI Quick Reference Guide](#)

[Additional Information: UCNI Markings](#)

Notes:

4.4 Acronyms

ACRONYMS			
CCDF	Centralized Classified Destruction Facility	PII	Personally Identifiable Information
CUI	Controlled Unclassified Information	PPA	Property Protection Area
DOE	Department of Energy	RD	Restricted Data
FPS	Federal Protective Service	RF	Radio Frequency
FRD	Formerly Restricted Data	SAP	Special Access Program
HQ	Headquarters	SCIFs	Sensitive Compartmented Information Facilities
HQFMSP	Headquarters Facilities Master Security Plan	SPO	Security Police Officers
HSO	Headquarters Security Officers	UCNI	Unclassified Controlled Nuclear Information
LA	Limited Area	VTR	Vault-Type Room
LMS	Learning Management System		
LSSO	Local Site Specific Only		
NSI	National Security Information		
NTC	National Training Center		
OGA	Other Government Agency		
OUO	Official Use Only		

Notes:

5. Part 3 - Security Badges

5.1 Security Badge Requirements

SECURITY BADGES

Security Badge Requirements

You literally hold one of the keys to security right in your hand – your security badge. The proper use of this badge goes a long way toward ensuring our security.

Your security badge must follow the protocols below:

- Be worn at all times when you are in a DOE building or on DOE property
- Should not be worn outside of DOE buildings or off DOE property
- Should not be used as means of identification for an unofficial purpose (for example, cashing a check)



To learn the proper way to wear your security badge, select the image.

Notes:

Security Badge Requirements

You literally hold one of the keys to security right in your hand - your security badge. The proper use of this badge goes a long way towards ensuring our security.

Your security badge must:

- Be worn at all times when you are in a DOE building or on DOE property
- Should not be worn outside of DOE buildings or off DOE property, and
- Should not be used as means of identification for an unofficial purpose (i.e., cashing a check)

To learn the proper way to wear your security badge, select the image above.

Wear It Well (Slide Layer)

SECURITY BADGES

Wear It Well
Do you know the proper way to wear your security badge? To ensure you wear your badge correctly, **review the information below in detail.**

- Displayed Prominently**
The badge must be displayed prominently and in plain view.
- Photograph Side Out**
The badge should be worn with the photograph side out.
- Above The Waist And In Front Of Body**
The badge should be positioned above the waist and in front of the body.

5.2 Lost or Missing Badges

SECURITY BADGES

Lost or Missing Badges

If your security badge is lost, misplaced, stolen, or inadvertently destroyed, you must immediately notify the HQ Security Badging Office at either Forrestal or Germantown.

By promptly reporting a missing badge, it can then be deactivated so that an unauthorized person cannot use the badge to gain access to DOE facilities.

In cases of lost or missing badges, a request for a badge replacement must be made, signed by the employee's supervisor, and returned to the Security Badge Office. A new badge will be issued in approximately ten working days.

Take your badge to the Security Badge Office for replacement if one of the following occurs:

- Your badge becomes worn or damaged
- Your physical appearance changes significantly (such as growing a beard or cutting your hair shorter than usual)

Notes:

Lost or Missing Badges

If your security badge is lost, misplaced, stolen, or inadvertently destroyed, you must immediately notify the HQ Security Badging Office at either Forrestal or Germantown.

By promptly reporting a missing badge, it can then be deactivated so that an unauthorized person cannot use the badge to gain access to DOE facilities.

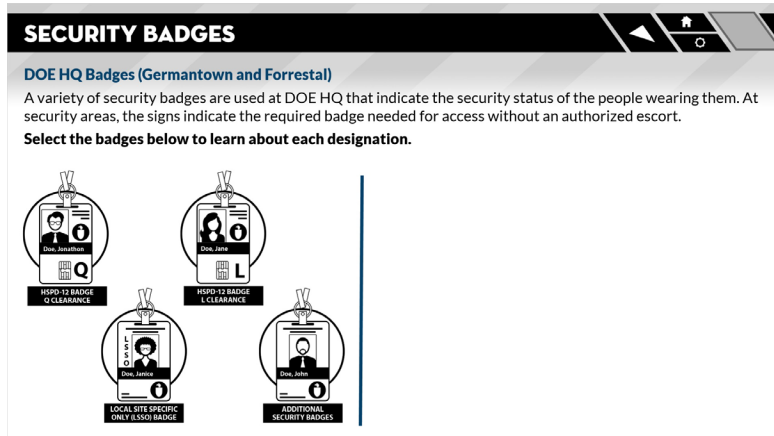
In cases of lost or missing badges, a request for a badge replacement must be made, signed by the employee's supervisor, and returned to the Security Badge Office. A new badge will be issued in approximately

ten working days.

Take your badge to the Security Badge Office for replacement if one of the following occurs:

- Your badge becomes worn or damaged, or
- Your physical appearance changes significantly (such as growing a beard or cutting your hair shorter than usual)

5.3 DOE HQ Badges



Notes:

DOE HQ Badges (Germantown and Forrestal)

A variety of security badges are used at DOE HQ that indicate the security status of the people wearing them. At security areas, the signs indicate the required badge needed for access without an authorized escort. **Select the badges below to learn about each designation.**

HSPD - 12 Badge: Q Clearance

The "Q" letter designation identifies individuals who have been granted an access authorization, also referred to as a security clearance, which permits access to certain levels and categories of classified information. A "Q" access authorization (security clearance) allows the holder to have access to the following levels of classified information: Top Secret, Secret, and Confidential. It also allows access to the following

categories: Restricted Data (RD), Formerly Restricted Data (FRD), and National Security Information (NSI).

HSPD - 12 Badge: L Clearance

The “L” letter designation identifies individuals who have been granted an access authorization, also referred to as a security clearance, which permits access to certain levels and categories of classified information. An “L” access authorization (security clearance) allows the holder to have access to the following levels of classified information: Secret and Confidential. It also allows access to the following categories: FRD and NSI. NOTE: Holders of an “L” access authorization may have access to Confidential/RD but not Top Secret or Secret/RD.

Local Site Specific Only (LSSO) Badge

These badges are issued to DOE employees and contractors who are awaiting their HSPD-12 badge, have lost their HSPD-12 badge, or have failed to meet qualifications for issuance of an HSPD-12 badge (detailed to work at an HQ facility or other specialized need).

Foreign National Badge

Non-PIV Badge

Other Government Agency (OGA) Badge

Child Development Center (CDC) Badge

Q Clearance (Slide Layer)

SECURITY BADGES

DOE HQ Badges (Germantown and Forrestal)

A variety of security badges are used at DOE HQ that indicate the security status of the people wearing them. At security areas, the signs indicate the required badge needed for access without an authorized escort.

Select the badges below to learn about each designation.


HSPD-12 BADGE
Q CLEARANCE


HSPD-12 BADGE
L CLEARANCE


LOCAL SITE SPECIFIC
ONLY (LSSO) BADGE


ADDITIONAL
SECURITY BADGES

HSPD-12 Badge: Q Clearance

The “Q” letter designation identifies individuals who have been granted an access authorization, also referred to as a security clearance, which permits access to certain levels and categories of classified information.

A “Q” access authorization (security clearance) allows the holder to have access to the following levels of classified information: Top Secret, Secret, and Confidential. It also allows access to the following categories: Restricted Data (RD), Formerly Restricted Data (FRD), and National Security Information (NSI).

L Clearance (Slide Layer)

SECURITY BADGES

DOE HQ Badges (Germantown and Forrestal)

A variety of security badges are used at DOE HQ that indicate the security status of the people wearing them. At security areas, the signs indicate the required badge needed for access without an authorized escort.

Select the badges below to learn about each designation.



HSPD-12 Badge: L Clearance

The "L" letter designation identifies individuals who have been granted an access authorization, also referred to as a security clearance, which permits access to certain levels and categories of classified information.

An "L" access authorization (security clearance) allows the holder to have access to the following levels of classified information: Secret and Confidential. It also allows access to the following categories: FRD and NSI.

NOTE: Holders of an "L" access authorization may have access to Confidential/RD but not Top Secret or Secret/RD.

LSSO (Slide Layer)

SECURITY BADGES

DOE HQ Badges (Germantown and Forrestal)

A variety of security badges are used at DOE HQ that indicate the security status of the people wearing them. At security areas, the signs indicate the required badge needed for access without an authorized escort.

Select the badges below to learn about each designation.



Local Site Specific Only (LSSO) Badge

LSSO badges are issued to DOE employees and contractors who are awaiting their HSPD-12 badge, have lost their HSPD-12 badge, or have failed to meet qualifications for issuance of an HSPD-12 badge (detailed to work at an HQ facility or other specialized need).

Additional Security Badges (Slide Layer)

SECURITY BADGES

DOE HQ Badges (Germantown and Forrestal)

A variety of security badges are used at DOE HQ that indicate the security status of the people wearing them. At security areas, the signs indicate the required badge needed for access without an authorized escort.

Select the badges below to learn about each designation.



Additional Security Badges

Additional security badges are as follows:

- Foreign National Badge
- Non-PIV Badge
- Other Government Agency (OGA) Badge

5.4 Returning Badges

SECURITY BADGES

Returning Badges

All badges are the property of DOE.

When an employee terminates their employment, they must turn in their DOE badge to the Badge Office. If the Badge Office is closed, the employee must turn in their badge to their HSO or supervisor prior to departing DOE.

Remote workers must mail their badge to the address listed on the back of the badge.



Note: All government property in an employee's possession must be turned in to the appropriate official in the organization from which the employee is terminating employment.

Notes:

Returning Badges

All badges are the property of DOE.

When an employee terminates their employment, they must turn in their DOE badge to the Badge Office. If the Badge Office is closed, the employee must turn in their badge to their HSO or supervisor prior to departing DOE.

Note: All government property in an employee's possession must be turned in to the appropriate official in the organization from which the employee is terminating employment.

6. Part 4 - Visitor Escorts

6.1 Escort Requirements

VISITOR ESCORTS

Escort Requirements

Making sure that visitors are properly escorted while in DOE facilities is another important part of our security efforts. Escorting requirements are affected by the time of day.

Review the escort requirements below for non-security and security hours.

**Non-Security Hours**

During non-security hours, escorts generally are not required for visitors entering HQ facilities unless specified by the office or person being visited.

**Security Hours**

Visitors must be escorted at all times during security hours.

Notes:

Escort Requirements

Making sure that visitors are properly escorted while in DOE facilities is another important part of our security efforts. Escorting requirements are affected by the time of day. Review the escort requirements below for non-security and security hours.

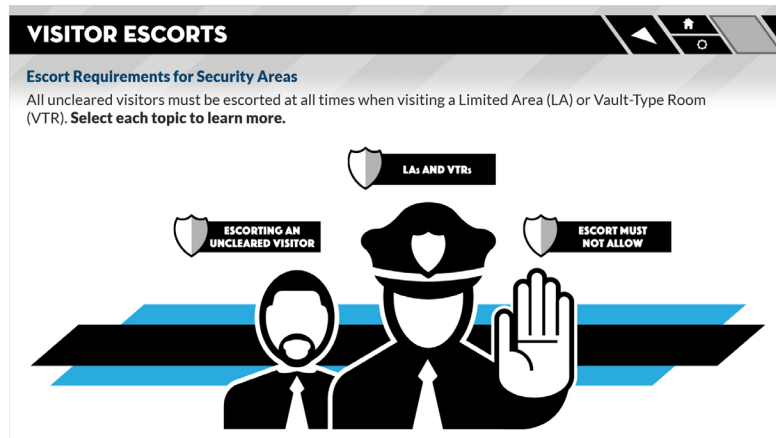
Non-Security Hours

During non-security hours, escorts generally are not required for visitors entering HQ facilities unless specified by the office or person being visited.

Security Hours

Visitors must be escorted at all times during security hours.

6.2 Security Areas



Notes:

Escort Requirements for Security Areas

All uncleared visitors must be escorted at all times when visiting a Limited Area (LA) or Vault-Type Room (VTR). **Select each topic to learn more.**

LAs & VTRs are:

- Security areas established for the protection of classified matter, and
- Distinguished by physical barriers and access controls

Only employees or contractors with "Q" or "L" clearances may escort authorized visitors or persons without a security clearance into an LA or VTR.

VTRs are considered to be locations where your mere presence in the area would normally result in access to classified information.

Escorts are required to be with their visitors at all times when in LAs or VTRs.

When escorting an uncleared visitor in an LA or VTR, the escort must:

- Prevent unauthorized access to classified and/or sensitive data, i.e. PII and OOU

- Ensure the visitor properly wears his/her badge
- Make sure he/she complies fully with DOE security requirements
- Make sure those working in the area are aware of the presence of an uncleared person and they do not discuss sensitive/classified information or allow the visitor to have access to such data, and
- Be especially alert to ensure the visitor does not bring in wireless devices, cell phones, cameras, IT equipment, etc.

The escort must NOT allow the visitor to:

- Bring controlled or prohibited items into the area (this includes the entire facility), or
- Remove government property from the premises without permission

LAs and VTRs (Slide Layer)

VISITORS

Escort
All unclassified (VTR).

LAs & VTRs are as follows:

- Security areas established for the protection of classified matter
- Distinguished by physical barriers and access controls

Only employees or contractors with "Q" or "L" clearances may escort authorized visitors or persons without a security clearance into an LA or VTR.

VTRs are considered to be locations where your mere presence in the area would normally result in access to classified information. Additional protective measures may be required for uncleared visitor access to the VTR. Check with your HSO for more information.

Escorts are required to be with their visitors at all times when in LAs or VTRs.

Escorting an Uncleared Visitor (Slide Layer)

When escorting an uncleared visitor in an LA or VTR, the escort must do the following:

- Prevent unauthorized access to classified and/or sensitive data, for example, Personally Identifiable Information (PII) and Controlled Unclassified Information (CUI)
- Ensure the visitor properly wears his/her badge
- Make sure he/she complies fully with DOE security requirements
- Make sure those working in the area are aware of the presence of an uncleared person and they do not discuss sensitive/classified information or allow the visitor to have access to such data
- Be especially alert to ensure the visitor does not bring in wireless devices, cell phones, cameras, IT equipment, etc.



Not Allowed (Slide Layer)

The escort must NOT allow the visitor to do the following:

- Bring controlled or prohibited items into the area (this includes the entire facility)
- Remove government property from the premises without permission



6.3 Certain Areas

VISITOR ESCORTS

Certain Areas of Germantown, Forrestal, and the Portals Facility are Security Areas

Access to designated security areas, such as LAs and VTRs, is restricted to only those individuals with the proper access authorizations (appropriate security clearance).

Note: LAs and VTRs are identified by signs and additional access control systems.



If entering an LA without authorization and the audio alarm sounds **YOU MUST NOT** enter the area. You must stay where you are until the SPO arrives and evaluates the situation. Failure to stay in place or entering the area after the alarm sounds constitutes a security incident.

Notes:

Certain Areas of Germantown, Forrestal, and the Portals Facility are Security Areas

Access to designated security areas, such as LAs and VTRs, is restricted to only those individuals with the proper access authorizations (appropriate security clearance).

Note: LAs and VTRs are identified by signs and additional access control systems.

If entering an LA without authorization and the audio alarm sounds YOU MUST not enter the area. You must stay where you are until the SPO arrives and evaluates the situation. Failure to stay in place or entering the area after the alarm sounds constitutes a security incident.

6.4 PPAs

VISITOR ESCORTS

Escort Requirements for Property Protection Areas

In addition to LAs and VTRs, DOE HQ has a third type of security area known as a Property Protection Area (PPA).

The PPA:

- Has defined boundaries and access controls for the protection of Department property
- Does not require individuals to possess a security clearance to access it



Notes:

Escort Requirements for Property Protection Areas

In addition to LAs and VTRs, DOE HQ has a third type of security area known as a Property Protection Area (PPA).

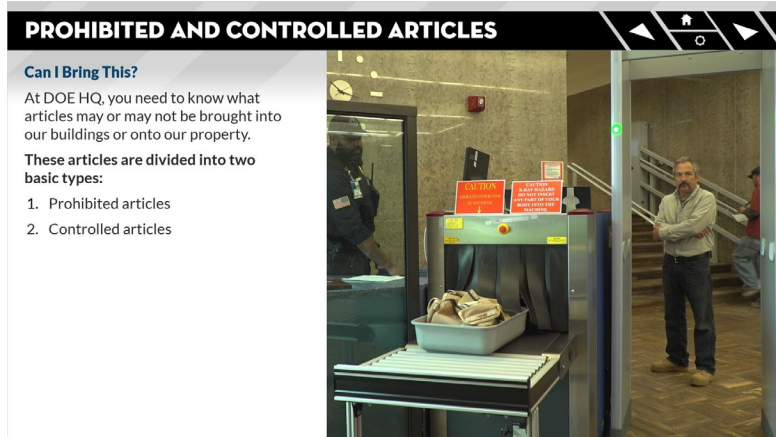
The PPA:

- Has defined boundaries and access controls for the protection of Department property, and
- Does not require individuals to possess a security clearance to

access it.

7. Part 5 - Prohibited and Controlled Articles

7.1 Can I Bring This?



Notes:

Can I Bring This?

At DOE HQ, you need to know what articles may or may not be brought into our buildings or onto our property.

These articles are divided into two basic types:

1. Prohibited articles, and
2. Controlled articles

7.2 Prohibited Articles



Notes:

Prohibited Articles

Do you know what articles are prohibited within HQ facilities? **Select each category to learn more.**

Dangerous weapons and explosives

Dangerous weapons and explosives (including firearms and ammunition) are prohibited without prior approval or an exception being granted by the Office of HQ Security Operations. Only lawfully armed DOE, civilian, or military police, or investigative officers may remain armed in our facilities if on official business.

Realistic replicas of explosives and firearms

Realistic replicas of explosives and/or firearms are not permitted into DOE HQ facilities without the written permission of the Director, Office of Physical Protection. For more information call 202-586-7887.

Instruments likely to injure or damage

Instruments or material likely to produce substantial injury or damage to persons or property (such as knives with a blade of 2.5 inches or longer) are prohibited.

Alcoholic beverages

Alcoholic beverages, including "near" and "nonalcoholic" beer and wine, are prohibited. However, under certain conditions exceptions are

made. Contact your HSO for more information on this subject.

Controlled substances

Controlled substances (e.g., illegal drugs or paraphernalia, but not prescription medication) are prohibited.

Dogs and other animals

Dogs and other service animals (identified in Title 41, CFR Part 101-20.311), except seeing-eye dogs, other guide dogs, and animals used to assist handicapped persons, are prohibited.

Other items prohibited by law

All other items prohibited by law are not allowed into DOE facilities.

Dangerous Weapons and Explosives (Slide Layer)



Realistic Replicas of Explosives and Firearms (Slide Layer)



Dangerous Instruments (Slide Layer)

PROHIBITED AND CONTROLLED ARTICLES

Prohibited
Do you know?

Instruments Likely To Injure Or Damage

Instruments or material likely to produce substantial injury or damage to persons or property (such as knives with a blade of 2.5 inches or longer) are prohibited.



Alcoholic Beverages (Slide Layer)

PROHIBITED AND CONTROLLED ARTICLES

Prohibited
Do you know?

Alcoholic Beverages

Alcoholic beverages, including "near" and "nonalcoholic" beer and wine, are prohibited. However, under certain conditions, exceptions are made. Contact your HSO for more information on this subject.



Controlled Substances (Slide Layer)

PROHIBITED AND CONTROLLED ARTICLES

Prohibited
Do you know?

Controlled Substances

Controlled substances (for example, illegal drugs or paraphernalia, but not prescription medication) are prohibited. This is a Federal facility, substances which may be legal in the state may be prohibited on the premises.



Dogs and Other Animals (Slide Layer)

PROHIBITED AND CONTROLLED ARTICLES

Prohibited
Do you know?

Dogs And Other Animals
Dogs and other service animals (identified in Title 41, CFR Part 101-20.311), except seeing-eye dogs, other guide dogs, and animals used to assist handicapped persons, are prohibited.



Other Items Prohibited by Law (Slide Layer)

PROHIBITED AND CONTROLLED ARTICLES

Prohibited
Do you know?

Other Items Prohibited By Law
All other items prohibited by law are not allowed into DOE facilities.



7.3 Prohibited Articles Signs

PROHIBITED AND CONTROLLED ARTICLES

Prohibited Articles Signs
Signs identifying prohibited articles are posted at DOE facility entrances.
The signs include a notice of the following:

- The area is monitored by surveillance equipment
- Packages, vehicles, and hand-carried items may be inspected

In general, prohibited articles are not allowed within PPAs, including all LAs and VTRs, without prior authorization from the Office of Headquarters Security Operations.

PROHIBITED ARTICLES

PRIOR AUTHORIZATION IS NEEDED FOR ADMITTING:

- FIREARMS, WEAPONS, EXPLOSIVES, AND INCENDIARY DEVICES
- CONTROLLED SUBSTANCES AND ILLEGAL DRUGS

UPON ENTERING OR LEAVING THIS SITE, YOU ARE SUBJECT TO SEARCH. ALL PERSONS SHALL, UPON REQUEST, SUBMIT TO A SEARCH OF THEIR PERSON, HAND CARRIED ITEMS, AND/OR VEHICLES.

By Order of the
United States
Department of Energy



Notes:

Prohibited Articles Signs

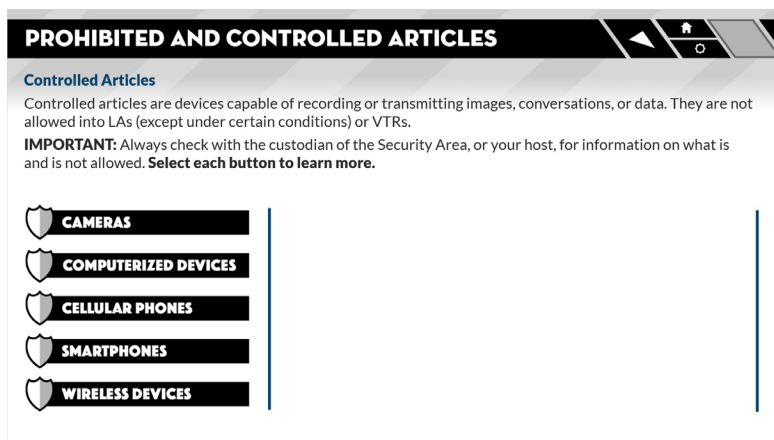
Signs identifying prohibited articles are posted at DOE facility entrances.

The signs include a notice that:

- The area is monitored by surveillance equipment, and
- Packages, vehicles, and hand-carried items may be inspected

In general, prohibited articles are not allowed within PPAs, including all LA and VTRs, without prior authorization from the Office of Headquarters Security Operations.

7.4 Controlled Articles



Notes:

Controlled Articles

Controlled articles are devices capable of recording or transmitting images, conversations or data. They are not allowed into LAs (except under certain conditions) or VTRs.

IMPORTANT: Always check with the custodian of the Security Area or your host for information on what is and is not allowed.

Select each button to learn more.

Cameras

Photography is severely restricted and all photographic equipment, including cell phone cameras, is strictly controlled within LAs and VTRs.

Computerized devices

Laptop computers, notebooks (i.e. iPads/iPods), and similar computerized devices are considered controlled articles.

Cellular phones

Smartphones

All smartphones, iPads, tablets, cameras, etc. are considered controlled articles.

Wireless devices

Wireless devices with the ability to store data via fixed or removable media and have a two-way transmitting capability such as some electronic picture frames, wireless headphones/earbuds, and certain medical devices are considered controlled articles. Contact your HSO for more information on what can and cannot be used in an LA.

Cameras (Slide Layer)

PROHIBITED AND CONTROLLED ARTICLES

Controlled Articles

Controlled articles are devices capable of recording or transmitting images, conversations, or data. They are not allowed into LAs (except under certain conditions) or VTRs.

IMPORTANT: Always check with the custodian of the Security Area, or your host, for information on what is and is not allowed. **Select each button to learn more.**

- CAMERAS**
- COMPUTERIZED DEVICES**
- CELLULAR PHONES**
- SMARTPHONES**
- WIRELESS DEVICES**

Cameras

Photography is severely restricted and all photographic equipment, including cell phone cameras, is strictly controlled within LAs and VTRs.

Computerized Devices (Slide Layer)

PROHIBITED AND CONTROLLED ARTICLES

Controlled Articles

Controlled articles are devices capable of recording or transmitting images, conversations, or data. They are not allowed into LAs (except under certain conditions) or VTRs.

IMPORTANT: Always check with the custodian of the Security Area, or your host, for information on what is and is not allowed. **Select each button to learn more.**

**CAMERAS**

**COMPUTERIZED DEVICES**

**CELLULAR PHONES**

**SMARTPHONES**

**WIRELESS DEVICES**

Computerized Devices

Laptop computers, notebooks (for example, iPads/iPods), and similar computerized devices are considered controlled articles.

Cellular Phones (Slide Layer)

PROHIBITED AND CONTROLLED ARTICLES

Controlled Articles

Controlled articles are devices capable of recording or transmitting images, conversations, or data. They are not allowed into LAs (except under certain conditions) or VTRs.

IMPORTANT: Always check with the custodian of the Security Area, or your host, for information on what is and is not allowed. **Select each button to learn more.**

**CAMERAS**

**COMPUTERIZED DEVICES**

**CELLULAR PHONES**

**SMARTPHONES**

**WIRELESS DEVICES**

Cellular Phones

Cell phones are considered controlled articles.

Smartphones (Slide Layer)

PROHIBITED AND CONTROLLED ARTICLES

Controlled Articles

Controlled articles are devices capable of recording or transmitting images, conversations, or data. They are not allowed into LAs (except under certain conditions) or VTRs.

IMPORTANT: Always check with the custodian of the Security Area, or your host, for information on what is and is not allowed. **Select each button to learn more.**

**CAMERAS**

**COMPUTERIZED DEVICES**

**CELLULAR PHONES**

**SMARTPHONES**

**WIRELESS DEVICES**

Smartphones

All smartphones, iPads, tablets, cameras, etc. are considered controlled articles.

Wireless Devices (Slide Layer)

PROHIBITED AND CONTROLLED ARTICLES

Controlled Articles
Controlled articles are devices capable of recording or transmitting images, conversations, or data. They are not allowed into LAs (except under certain conditions) or VTRs.
IMPORTANT: Always check with the custodian of the Security Area, or your host, for information on what is and is not allowed. **Select each button to learn more.**

**CAMERAS**

**COMPUTERIZED DEVICES**

**CELLULAR PHONES**

**SMARTPHONES**

**WIRELESS DEVICES**

Wireless Devices
Wireless devices with the ability to store data via fixed or removable media that have a two-way transmitting capability, such as some electronic picture frames, wireless headphones/earbuds, smartwatches, mobile hotspots, and certain medical devices are considered controlled articles. Contact your HSO for more information on what can and cannot be used in an LA.

7.5 Prohibited and Controlled Articles and LAs/VTRs

PROHIBITED AND CONTROLLED ARTICLES

Prohibited and Controlled Articles and LAs/VTRs
Remember, uncleared persons entering an LA or VTR must be **under escort at all times** while in these areas.
The escort is also responsible for ensuring the uncleared visitor does not bring prohibited or controlled articles into the LA or VTR.



Notes:

Prohibited and Controlled Articles and LAs/VTRs

Remember, uncleared persons entering an LA or VTR must be **under escort at all times** while in these areas.

The escort is also responsible for ensuring the uncleared visitor does not bring prohibited or controlled articles into the LA or VTR.

7.6 Controlled Article Exceptions and Conditions

PROHIBITED AND CONTROLLED ARTICLES

Controlled Article Exceptions and Conditions
Under certain conditions, DOE HQ policy allows certain designated controlled articles into LAs.
The LA must:

- Be authorized for storing, processing, and discussing classified information up to the Secret/Restricted Data (S/RD) level
- NOT be a TEMPEST Protected Area



For a list of authorized controlled articles, select the image above.

Notes:

Controlled Article Exceptions and Conditions

Under certain conditions, DOE HQ policy allows certain designated controlled articles into LAs.

The LA must:

- Be authorized for storing, processing, and discussing classified information up to the Secret/Restricted Data (S/RD) level, and
- NOT be a TEMPEST Protected Area

For a list of authorized controlled articles, **select the image above.**

The list of authorized controlled articles includes:

- Smartphones, PDAs, and BlackBerry-type devices
- eBook Readers without cellular capability, and
- iPod/MP3 type devices

Although these devices may be taken into a Limited Area, they must have their batteries removed if possible, or be turned off and placed in an approved Radio Frequency attenuation container (RF bag or box) whenever classified information is being processed or discussed.

Authorized Controlled Articles (Slide Layer)

PROHIBITED AND CONTROLLED ARTICLES

Authorized Controlled Articles

The list of authorized controlled articles includes the following:

- Smartphones, PDAs, and BlackBerry-type devices
- eBook Readers without cellular capability
- iPod/MP3 type devices

Although these devices may be taken into a Limited Area, they must have their batteries removed if possible, or be turned off and placed in an approved Radio Frequency attenuation container (RF bag or box) whenever classified information is being processed or discussed.

As a rule, controlled articles, to include mobile devices, are not allowed in LAs. For this reason, it is important to coordinate with your HSO prior to bringing any electronic device into an LA.



7.7 Electronic Devices

PROHIBITED AND CONTROLLED ARTICLES

Electronic Devices

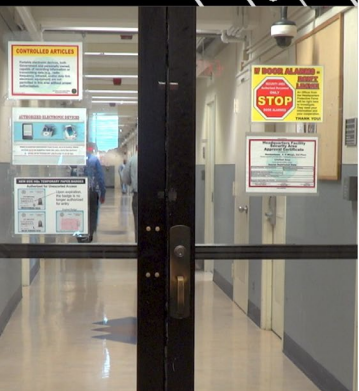
Electronic devices are prohibited in the following locations:

- VTRs
- Top Secret LAs
- Sensitive Compartmented Information Facilities (SCIFs)
- TEMPEST Protected Areas
- Areas where Special Access Program (SAP) information is stored, processed, or discussed

Your HSO can give you additional information on the use of cell phones and other electronic devices.

For more information on specific devices, contact your HSO or refer to the Chapter 2 – HQ Facility Master Security Plan (HQFMSP).

Remember, unless specifically permitted, electronic devices are not allowed into LAs and VTRs.



Notes:

Electronic Devices

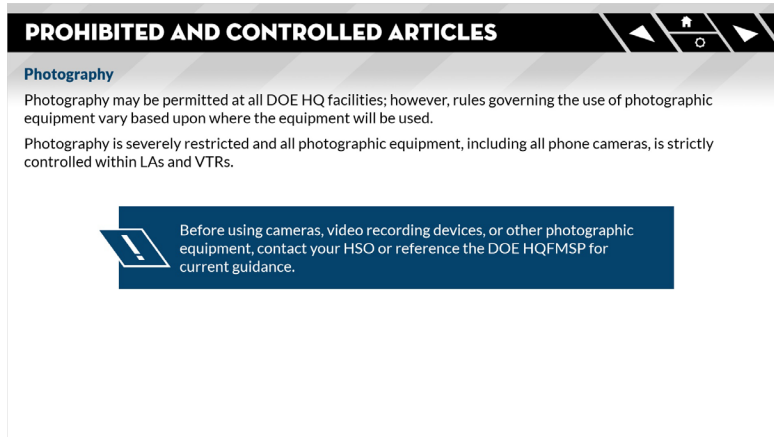
Electronic devices are prohibited in:

- VTRs
- Top Secret LAs
- Sensitive Compartmented Information Facilities (SCIFs)
- TEMPEST Protected Areas, and
- Areas where Special Access Program (SAP) information is stored, processed, or discussed

Your HSO can give you additional information on the use of cell phones and other electronic devices.

For more information on specific devices, contact your HSO or refer to Chapter 2 of the HQ Facilities Master Security Plan (HQFMSP). Remember, unless specifically permitted, electronic devices are not allowed into LAs and VTRs.

7.8 Photography



PROHIBITED AND CONTROLLED ARTICLES

Photography

Photography may be permitted at all DOE HQ facilities; however, rules governing the use of photographic equipment vary based upon where the equipment will be used.

Photography is severely restricted and all photographic equipment, including all phone cameras, is strictly controlled within LAs and VTRs.

Before using cameras, video recording devices, or other photographic equipment, contact your HSO or reference the DOE HQFMSP for current guidance.

Notes:

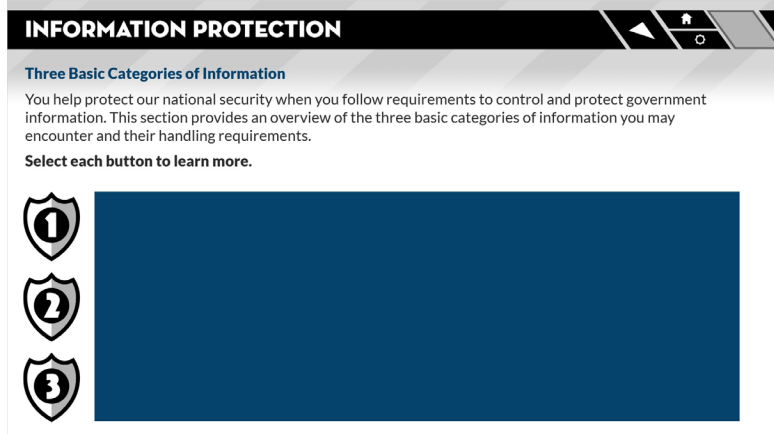
Photography

Photography may be permitted at all DOE HQ facilities; however, rules governing the use of photographic equipment vary based upon where the equipment will be used and the location it will be used.

Photography is **severely restricted** and all photographic equipment, including all phone cameras, is strictly controlled within LAs & VTRs. Before using cameras, video recording devices, or other photographic equipment, contact your HSO or reference the DOE HQFMSP for current guidance.

8. Part 6 - Information Protection

8.1 Three Basic Categories of Information



Notes:

Three Basic Categories of Information

You help protect our national security when you follow requirements to control and protect government information. This section provides an overview of the three basic categories of information you may encounter and their handling requirements.

Select each button to learn more.

Unclassified information

Unclassified information may or may not be marked as such. In either case, unclassified information does not require any special handling or controls.

Controlled Unclassified Information (CUI)

Within DOE, Controlled Unclassified Information (CUI) is a term used for **unclassified** information that is controlled because of its sensitivity. There are two primary types of CUI - Official Use Only (OUO) and Unclassified Controlled Nuclear Information (UCNI). You will learn more about OUO and UCNI later in this section.

Classified matter

Classified matter is any combination of documents and material containing classified information. Access is restricted to persons with

an access authorization (security clearance) and a “need-to-know.” No one is entitled to access classified information based on rank, office, position, or security clearance. You will learn more about classified matter later in this section.

category1-Unclassified (Slide Layer)

INFORMATION PROTECTION

Three Basic Categories of Information
You help protect our national security when you follow requirements to control and protect government information. This section provides an overview of the three basic categories of information you may encounter and their handling requirements.
Select each button to learn more.

**Unclassified Information**
Unclassified information may or may not be marked as such. In either case, unclassified information does not require any special handling or controls.





category2-Controlled (Slide Layer)

INFORMATION PROTECTION

Three Basic Categories of Information
You help protect our national security when you follow requirements to control and protect government information. This section provides an overview of the three basic categories of information you may encounter and their handling requirements.
Select each button to learn more.

**Controlled Information**
Within DOE, there are categories of unclassified information that are controlled because of their sensitivity. These include the following:



1. **Controlled Unclassified Information (CUI)** – certain unclassified information that is identified as requiring safeguarding and dissemination controls.



2. **Unclassified Controlled Nuclear Information (UCNI)** – unclassified information about nuclear facilities and weapons that must be controlled because its unauthorized release could have a significant adverse effect on the national security or public health and safety.

You will learn more about CUI and UCNI in this section.

category3-Classified (Slide Layer)

INFORMATION PROTECTION

Three Basic Categories of Information

You help protect our national security when you follow requirements to control and protect government information. This section provides an overview of the three basic categories of information you may encounter and their handling requirements.

Select each button to learn more.

1 Classified Matter

Classified matter is any combination of documents and materials containing classified information. Access is restricted to persons with an access authorization (security clearance) and a "need-to-know." No one is entitled to access classified information based on rank, office, position, or security clearance. You will learn more about classified matter later in this section.

2

3

8.2 CUI & UCNi

INFORMATION PROTECTION

Controlled Unclassified Information (CUI) & Unclassified Controlled Nuclear Information (UCNI)

CUI and UCNi are the main types of sensitive information you could encounter. Select each type to learn more.

Controlled Unclassified Information (CUI) **Unclassified Controlled Nuclear Information (UCNI)**

Notes:

Controlled Unclassified Information (CUI)

OUO and UCNi are the two primary types of CUI you could encounter.

Select each type to learn more.

Official Use Only Information

What is OUO?

OUO information is unclassified information that has the potential to damage governmental, commercial, or private interests if released to DOE employees or any other persons who do not have a "need to know" the information to perform their jobs or other DOE-authorized activities and may be exempt from public release under the Freedom of

Information Act.

Security Clearance Needed?

A security clearance is not required for OOU access. In general, OOU information may be given to a person who needs it to perform their duties. However, some OOU (e.g., Export Controlled Information) has additional access restrictions.

Unclassified Controlled Nuclear Information (UCNI)

What is UCNI?

UCNI is certain unclassified information about nuclear facilities and nuclear weapons. This information must be controlled because its unauthorized release could have a significant adverse effect on the national security or public health and safety.

Security Clearance Needed?

A security clearance is not required for access to UCNI. Any Federal or contractor employee with a need to know may have access to UCNI.

CUI (Slide Layer)

INFORMATION PROTECTION

Controlled Unclassified Information (CUI) & Unclassified Controlled Nuclear Information (UCNI)

CUI and UCNI are the main types of sensitive information you could encounter. **Select each type to learn more.**

Controlled Unclassified Information (CUI)	Unclassified Controlled Nuclear Information (UCNI)
Controlled Unclassified Information (CUI) What is CUI? CUI is information the government creates or possess, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy (LRGWP) requires or permits an agency to handle, using safeguarding or dissemination controls. Prior to the implementation of CUI, DOE controlled unclassified information was identified as Official Use Only (OUO). "Legacy OUO" is still found throughout the DOE. Contact your HSO for information on handling Legacy OUO. Security Clearance Needed? CUI can be accessed for a Lawful Government Purpose, which is any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement).	

UCNI (Slide Layer)

INFORMATION PROTECTION

Controlled Unclassified Information (CUI) & Unclassified Controlled Nuclear Information (UCNI)

CUI and UCNI are the main types of sensitive information you could encounter. **Select each type to learn more.**

Controlled Unclassified Information (CUI)**Unclassified Controlled Nuclear Information (UCNI)**

Unclassified Controlled Nuclear Information

What is UCNI?

UCNI is certain unclassified government information under section 148 of the Atomic Energy Act whose release would significantly increase the likelihood of illegal production of a nuclear weapon or the theft, diversion, or sabotage of nuclear material, equipment, or facilities (as identified by guide topic).

Requirements for UCNI can be found in 10 Code of Federal Regulations (CFR) Part 1017 and DOE Order 471.1B. See the Resources page to access these documents.

Security Clearance Needed?

A security clearance is not required for access to UCNI. Any DOE Federal or contractor employee with a "need to know" may have access to UCNI in order to perform official duties. For others, consult 10 CFR 1017, Subpart D.

8.3 Having Potential UCNI Reviewed

INFORMATION PROTECTION

Unclassified Controlled Nuclear Information (UCNI)

Matter that potentially contains UCNI must be reviewed by the appropriate personnel.

Having Matter That Potentially Contains UCNI Reviewed

You must refer matter that may contain UCNI to an UCNI Reviewing Official (RO) for review. For information on how to mark and protect the matter pending a review, see the Resources page.

Examples of UCNI Subject Areas include the design of facilities that produce or use uranium, plutonium, or other special nuclear material; security for those facilities or nuclear material contained in them or in transit; Radiological Emergency Response; Nonproliferation; the Transportation Safeguards System, etc.

If you have questions, talk to your supervisor/HQ Classification Representative, or contact the HQ Office of Classification. An UCNI awareness briefing can be provided.

Notes:

Controlled Unclassified Information (CUI)

OUO and UCNI are the two primary types of CUI you could encounter.

Select each type to learn more.

Official Use Only Information

What is OUO?

OUO information is unclassified information that has the potential to damage governmental, commercial, or private interests if released to DOE employees or any other persons who do not have a "need to know" the information to perform their jobs or other DOE-authorized activities and may be exempt from public release under the Freedom of

Information Act.

Security Clearance Needed?

A security clearance is not required for OUI access. In general, OUI information may be given to a person who needs it to perform their duties. However, some OUI (e.g., Export Controlled Information) has additional access restrictions.

Unclassified Controlled Nuclear Information (UCNI)

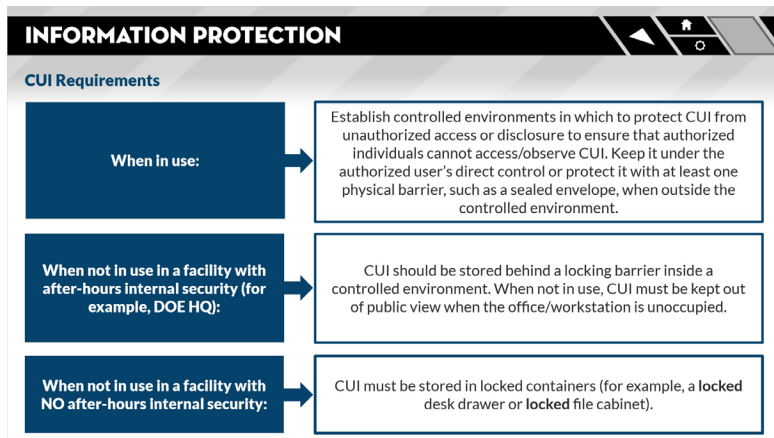
What is UCNI?

UCNI is certain unclassified information about nuclear facilities and nuclear weapons. This information must be controlled because its unauthorized release could have a significant adverse effect on the national security or public health and safety.

Security Clearance Needed?

A security clearance is not required for access to UCNI. Any Federal or contractor employee with a need to know may have access to UCNI.

8.4 CUI Requirements



Notes:

CUI Storage Requirements

When not in use in a facility with after-hours internal security (for example, DOE HQ):

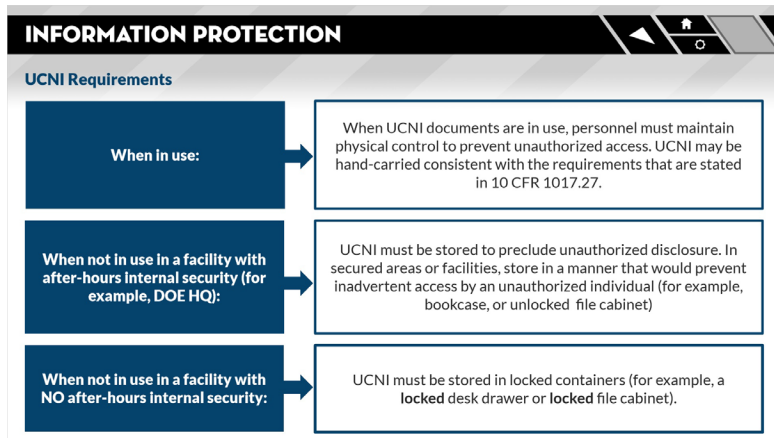
- OUI and UCNI may be stored in unlocked containers (for example, a

desk drawer or a file cabinet). OUO and UCNI must be kept out of public view when the office/workstation is unoccupied. It is stored in such a manner as to prevent easy access to those without a need-to-know.

When not in use in a facility with NO after-hours internal security:

- OUO and UCNI must be stored in locked containers (for example, a locked desk drawer or locked file cabinet)

8.5 UCNI Requirements



Notes:

CUI Storage Requirements

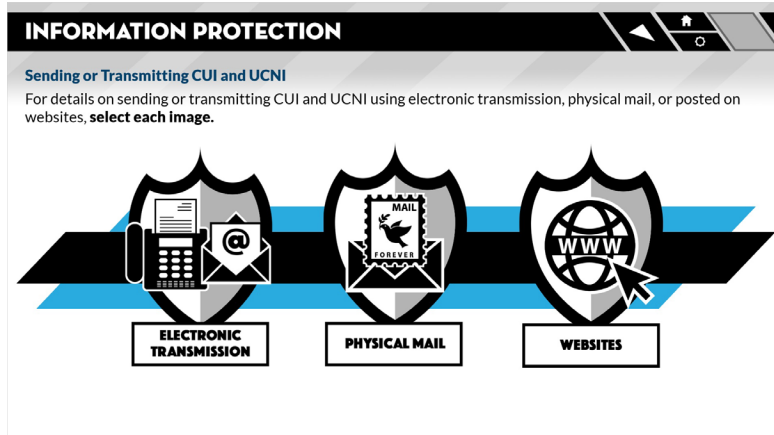
When not in use in a facility with after-hours internal security (for example, DOE HQ):

- OUO and UCNI may be stored in unlocked containers (for example, a desk drawer or a file cabinet). OUO and UCNI must be kept out of public view when the office/workstation is unoccupied. It is stored in such a manner as to prevent easy access to those without a need-to-know.

When not in use in a facility with NO after-hours internal security:

- OUO and UCNI must be stored in locked containers (for example, a locked desk drawer or locked file cabinet)

8.6 Sending or Transmitting CUI and UCNi



Notes:

Sending or Transmitting OUO and UCNi

For details on sending or transmitting OUO and UCNi using electronic transmission, physical mail or posted on websites, **select each image.**

Physical Mail

When sending by internal or outside mail, OUO and UCNi must be packaged in a single, opaque envelope or wrapping to conceal the presence of the material.

The address of the recipient and the sender must be indicated on the outside of the envelope or wrapping, along with the words "TO BE OPENED BY ADDRESSEE ONLY."

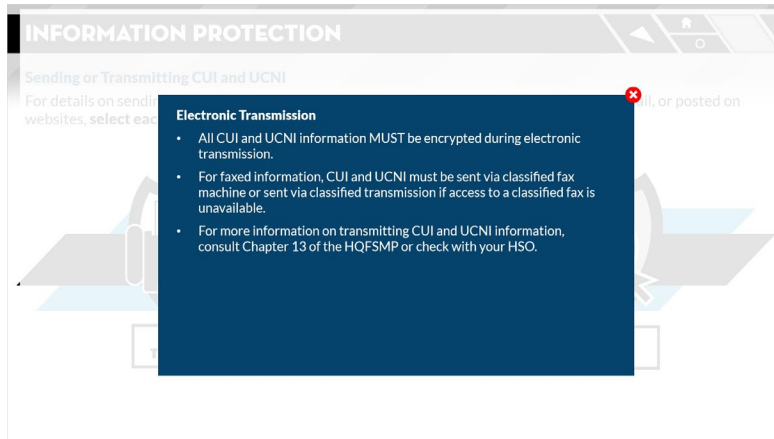
Electronic Transmission

- UCNi and PII must be encrypted during electronic transmission (fax or email)
- OUO information should be encrypted during electronic transmission
- If not possible, password-protect email messages and transmit the password in a separate email
- For faxed information, contact the recipient before transmission to ensure they are standing by the fax machine waiting for the

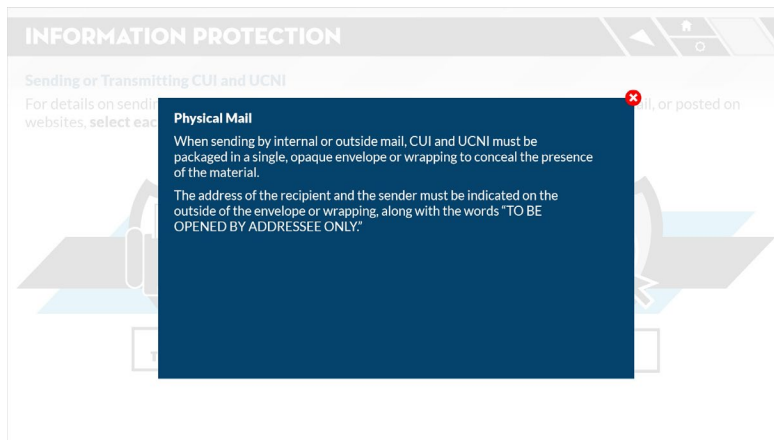
unencrypted file

In addition, OOU (including PII) and UCNI must **not be posted on websites** available to the public.

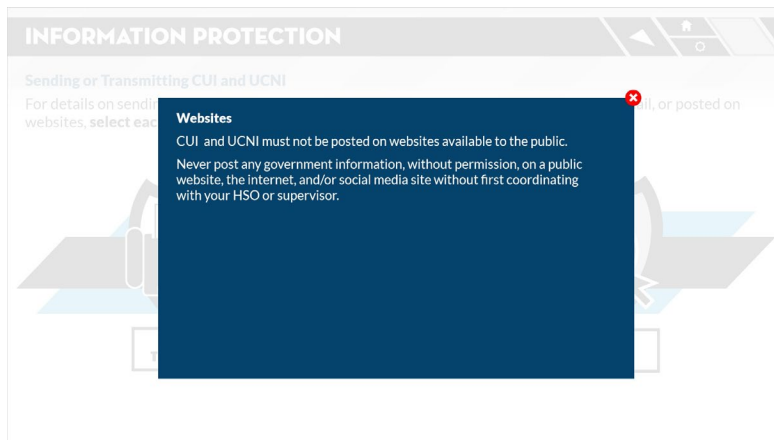
Electronic Transmission (Slide Layer)



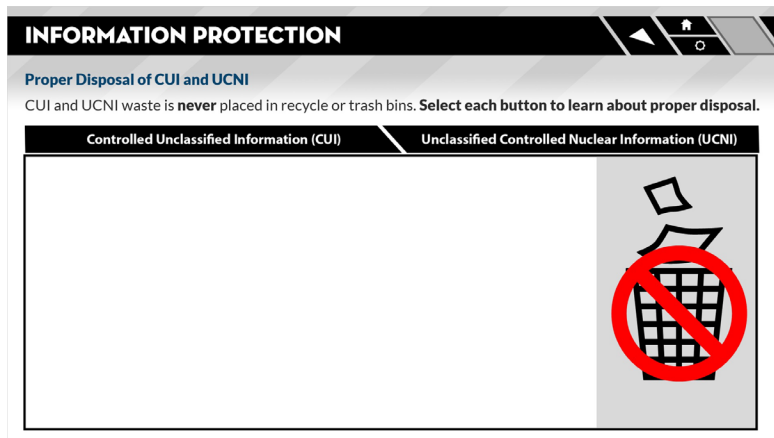
Physical Mail (Slide Layer)



Websites (Slide Layer)



8.7 Proper Disposal of CUI & UCNI



Notes:

Controlled Unclassified Information (CUI)

OUO and UCNI are the two primary types of CUI you could encounter.

Select each type to learn more.

Official Use Only Information

What is OUO?

OUO information is unclassified information that has the potential to damage governmental, commercial, or private interests if released to DOE employees or any other persons who do not have a "need to know" the information to perform their jobs or other DOE-authorized activities and may be exempt from public release under the Freedom of

Information Act.

Security Clearance Needed?

A security clearance is not required for OOU access. In general, OOU information may be given to a person who needs it to perform their duties. However, some OOU (e.g., Export Controlled Information) has additional access restrictions.

Unclassified Controlled Nuclear Information (UCNI)

What is UCNI?

UCNI is certain unclassified information about nuclear facilities and nuclear weapons. This information must be controlled because its unauthorized release could have a significant adverse effect on the national security or public health and safety.

Security Clearance Needed?

A security clearance is not required for access to UCNI. Any Federal or contractor employee with a need to know may have access to UCNI.

CUI (Slide Layer)

INFORMATION PROTECTION

Proper Disposal of CUI and UCNI
CUI and UCNI waste is **never** placed in recycle or trash bins. **Select each button to learn about proper disposal.**

Controlled Unclassified Information (CUI)

Unclassified Controlled Nuclear Information (UCNI)

CUI Disposal Methods

- CUI regulation requires that agencies destroy CUI in a manner that makes it unreadable, indecipherable, and irrecoverable.
- At a minimum, paper CUI must be destroyed using a cross-cut shredder producing waste particles no larger than 1 mm x 5 mm (0.04 in. x 0.2 in.).
- Discard bulk CUI waste in brown burn bags before delivery to the Centralized Classified Destruction Facility (CCDF). CUI must be protected accordingly before it is delivered.
- Consult with DOE's CUI policy regarding the specific instructions to destroy electronic media types, individuals handling CUI should ensure the methods of destruction align with the guidelines in the 32 CFR 2002.14(F), DOE O 471.7, and the NIST SP 800 88 or successor standards.



UCNI (Slide Layer)

INFORMATION PROTECTION

Proper Disposal of CUI and UCNI

CUI and UCNI waste is **never** placed in recycle or trash bins. **Select each button to learn about proper disposal.**

Controlled Unclassified Information (CUI)

Unclassified Controlled Nuclear Information (UCNI)

UCNI Disposal Methods

- At a minimum, paper containing UCNI must be destroyed using a cross-cut shredder producing waste particles no larger than 1/4 in. x 2 in.
- Discard bulk UCNI waste in brown burn bags marked as "UCNI" before delivery to the Centralized Classified Destruction Facility (CCDF). UCNI must be protected accordingly before it is delivered.
- UCNI hard matter, such as videotapes or floppy disks, may also be destroyed at the CCDF. Consult Chapter 13 of the HQFSMP or contact your HSO for more information.



8.8 CUI and UCNI Additional Resources

INFORMATION PROTECTION

CUI and UCNI Additional Resources

For additional information on CUI and UCNI, refer to the following:



Chapter 13, HQFSMP
(See Resources page for
more information)



Contact the Office of
Classification's Outreach
Program at
(301) 903-7567



For UCNI questions, email
outreach@hq.doe.gov
For CUI questions, email
doecui@hq.doe.gov

Notes:

OUO and UCNI Additional Resources

For additional information on OUO and UCNI, refer to the following:

- Chapter 13, HQFSMP or
- Contact the Office of Classification's Outreach program at (301) 371-7567 or
- Send an email to: outreach@hq.doe.gov

8.9 Classified Information Categories

INFORMATION PROTECTION			
Classified Information Categories			
Classified information falls within one of three classification levels and categories shown below. Each level indicates an increased degree of damage that could result from unauthorized disclosure. The access authorization of a person must be equal to, or higher than, the classification level and category of the classified matter.			
	TOP SECRET	SECRET	CONFIDENTIAL
National Security Information (NSI)			
Formerly Restricted Data (FRD)			
Restricted Data (RD)			

Notes:

Classified Information Categories

Classified information falls within one of three classification levels and categories shown below. Each level indicates an increased degree of damage that could result from unauthorized disclosure. The access authorization of a person must be equal to, or higher than, the classification level and category of the classified matter.

8.10 Classification and Declassification Reviews

INFORMATION PROTECTION	
Classified Materials Markings and Handling	
Personnel are expected to be familiar with the requirements for classification and declassification of materials.	
Classification and Declassification Reviews Specific details of required reviews for classification and declassification are in Attachment 4 of DOE O 475.2B. Personnel are expected to be familiar with these requirements and to obtain the required reviews. Only a Derivative Classifier (DC) can make the determination that matter is classified. Only a Derivative Declassifier (DD) can remove or lower the classification of matter. Examples of Classified Subject Areas include security information, design and production of nuclear weapons, Radiological Emergency Response, nonproliferation, production or processing of uranium and plutonium, transporting nuclear weapons, etc. If you are uncertain whether matter is classified, protect it at the highest sensitivity of the information believed to be in it until appropriately reviewed. 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 NNSA Shared (low-side) inbox: classification@nnsa.doe.gov	

Notes:

Controlled Unclassified Information (CUI)

OUO and UCNI are the two primary types of CUI you could encounter.

Select each type to learn more.

Official Use Only Information

What is OUO?

OUO information is unclassified information that has the potential to damage governmental, commercial, or private interests if released to DOE employees or any other persons who do not have a “need to know” the information to perform their jobs or other DOE-authorized activities and may be exempt from public release under the Freedom of Information Act.

Security Clearance Needed?

A security clearance is not required for OUO access. In general, OUO information may be given to a person who needs it to perform their duties. However, some OUO (e.g., Export Controlled Information) has additional access restrictions.

Unclassified Controlled Nuclear Information (UCNI)

What is UCNI?

UCNI is certain unclassified information about nuclear facilities and nuclear weapons. This information must be controlled because its unauthorized release could have a significant adverse effect on the national security or public health and safety.

Security Clearance Needed?

A security clearance is not required for access to UCNI. Any Federal or contractor employee with a need to know may have access to UCNI.

8.11 Classified Material Markings and Handling

INFORMATION PROTECTION

Classified Material Markings and Handling

Any document containing classified information must be clearly identified as such on the outside and requires special handling and protection.

The possibility of discovering unattended classified material in a non-secure area is remote. However, you still need to be able to recognize its markings to protect it.

Select the image to review classified material markings and handling to become familiar with them.



Notes:

Classified Material Markings and Handling

Any document containing classified information must be clearly identified as such on the outside and requires special handling and protection.

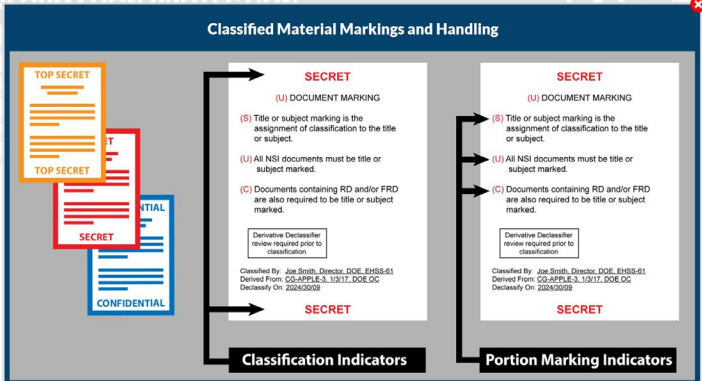
The possibility of discovering unattended classified material in a non-secure area is remote. However, you still need to be able to recognize its markings to protect it.

Select the image to review classified material markings and handling to become familiar with them.

Markings (Slide Layer)

INFORMATION PROTECTION

Classified Material Markings and Handling



Classification Indicators

Portion Marking Indicators

8.12 Classified Material Markings and Handling

INFORMATION PROTECTION

Classified Material Markings and Handling
If you discover material with classified markings in a non-secure area, you are responsible for the following:

- Immediately protecting the material
- Contacting your organizational HSO or an SPO to retrieve it
- NOT destroying or modifying, under any circumstance, the classified matter
- Under no circumstance are you to take classified material to your home or to remove it from the facility without proper authorization



Notes:

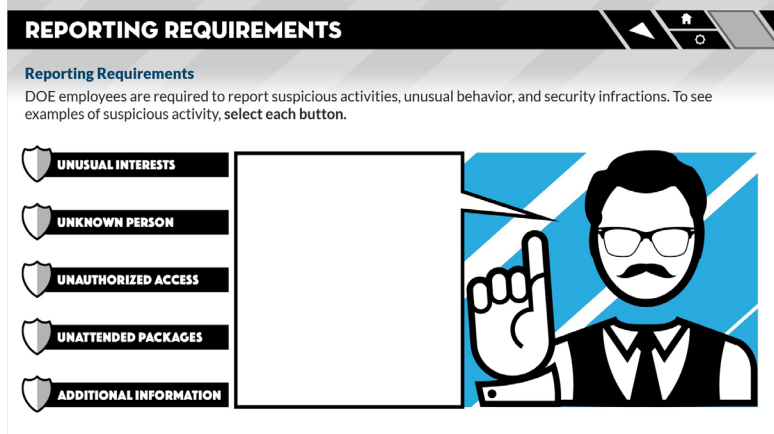
Classified Material Markings and Handling

If you discover material with classified markings in a non-secure area, you are responsible for:

- Immediately protecting the material
- Contacting your organizational HSO or a SPO to retrieve it
- NOT destroying or modifying, under any circumstance, the classified matter, and
- Under no circumstance are you to take classified material to your home or to remove it from the facility without proper authorization

9. Part 7 - Reporting Requirements

9.1 Reporting Requirements



Notes:

Reporting Requirements

DOE employees are required to report suspicious activities, unusual behavior, and security infractions. To see examples of suspicious activity, **select each button.**

Examples of suspicious activity include:

- Someone showing unusual interest in DOE facilities or operations
 - pay particular attention to someone photographing, videotaping, inquiring about security, or making notes about these activities
- Attempts to gain unauthorized access to DOE facilities/areas
- An unidentified or unknown person wandering in an area where they do not belong, or
- Unattended packages, briefcases, or luggage left in or around DOE facilities

Additionally, you should report the discovery of any classified or controlled unclassified information that is unprotected, an unlocked security container, or anything that is a security concern.

Unusual Interest (Slide Layer)

REPORTING REQUIREMENTS

Reporting Requirements
DOE employees are required to report suspicious activities, unusual behavior, and security infractions. To see examples of suspicious activity, **select each button.**

**UNUSUAL INTERESTS**

**UNKNOWN PERSON**

**UNAUTHORIZED ACCESS**

**UNATTENDED PACKAGES**

**ADDITIONAL INFORMATION**

Unusual Interest
Watch out for someone showing unusual interest in DOE facilities or operations.

Pay particular attention to someone photographing, videotaping, inquiring about security, or making notes about these activities.



Additional Information (Slide Layer)

REPORTING REQUIREMENTS

Reporting Requirements
DOE employees are required to report suspicious activities, unusual behavior, and security infractions. To see examples of suspicious activity, **select each button.**

**UNUSUAL INTERESTS**

**UNKNOWN PERSON**

**UNAUTHORIZED ACCESS**

**UNATTENDED PACKAGES**

**ADDITIONAL INFORMATION**

Additional Information
Additionally, you should report the discovery of any classified or controlled unclassified information that is unprotected, an unlocked security container, or anything that is a security concern.

If you see or are aware of any of these suspicious activities, immediately report it to your HSO, supervisor, or an SPO. When in doubt, contact your HSO.



Unknown Person (Slide Layer)

REPORTING REQUIREMENTS

Reporting Requirements
DOE employees are required to report suspicious activities, unusual behavior, and security infractions. To see examples of suspicious activity, **select each button.**

**UNUSUAL INTERESTS**

**UNKNOWN PERSON**

**UNAUTHORIZED ACCESS**

**UNATTENDED PACKAGES**

**ADDITIONAL INFORMATION**

Unknown Person
An unidentified or unknown person wandering in an area where they do not belong.



Unauthorized Access (Slide Layer)

REPORTING REQUIREMENTS

Reporting Requirements
DOE employees are required to report suspicious activities, unusual behavior, and security infractions. To see examples of suspicious activity, select each button.

 **UNUSUAL INTERESTS**

 **UNKNOWN PERSON**

 **UNAUTHORIZED ACCESS**

 **UNATTENDED PACKAGES**

 **ADDITIONAL INFORMATION**

Unauthorized Access
Attempts to gain unauthorized access to DOE facilities/areas.



Unattended Packages (Slide Layer)

REPORTING REQUIREMENTS

Reporting Requirements
DOE employees are required to report suspicious activities, unusual behavior, and security infractions. To see examples of suspicious activity, select each button.

 **UNUSUAL INTERESTS**

 **UNKNOWN PERSON**

 **UNAUTHORIZED ACCESS**

 **UNATTENDED PACKAGES**

 **ADDITIONAL INFORMATION**

Unattended Packages
Unattended packages, briefcases, or luggage left in or around DOE facilities.



9.2 Security Infractions

REPORTING REQUIREMENTS

Security Infractions
A security infraction is any knowing, willful, or negligent action contrary to DOE security orders and directives that does not constitute a "violation," which is more serious than an infraction. Select the image below to see a few common examples of security incidents, which could result in an infraction.



Notes:

Security Infractions

A security infraction is any knowing, willful, or negligent action contrary to DOE security orders and directives that does not constitute a “violation,” which is more serious than an infraction. **Select the image below to see a few common examples of security incidents, which could result in an infraction.**

A few common examples of security incidents, which could result in an infraction, are:

- Improperly storing classified materials (i.e., failing to lock a security container)
 - Failing to display a security badge while in DOE facilities
 - Unauthorized possession of prohibited articles in HQ facilities
 - Attempts to gain unauthorized access to classified information/matter or CUI, or
 - Sending classified information from an unauthorized IT system, i.e. personal computer that is not authorized to process such information
- The commission of a security infraction may result in administrative discipline being taken against an employee.

Security Infractions Examples (Slide Layer)

REPORTING REQUIREMENTS

Security Infractions

A few common examples of security incidents, which could result in an infraction, are below:

- Improperly storing classified materials, for example, failing to lock a security container
- Failing to display a security badge while in DOE facilities
- Unauthorized possession of prohibited articles in HQ facilities
- Attempts to gain unauthorized access to classified information/matter or CUI
- Sending classified information from an unauthorized IT system, for example, a personal computer that is not authorized to process such information

The commission of a security infraction may result in administrative discipline being taken against an employee.

9.3 Witnessing and Reporting

REPORTING REQUIREMENTS

Witnessing and Reporting

If you witness a security incident, immediately report it to one of the following:

- Your organizational HSO
- A SPO
- A representative of the Office of Headquarters Security Operations

 For a complete list of Security Safeguards reporting requirements, contact your HSO or refer to Chapter 11 of the HQFMSP.

Notes:

Witnessing and Reporting

If you witness a security incident, immediately report it to one of the following:

- Your organizational HSO
- An SPO, or
- A representative of the Office of Headquarters Security Operations

For a complete list of Security Safeguards reporting requirements, contact your HSO or refer to Chapter 3 of the HQFMSP.

9.4 Conclusion

CONCLUSION

Security Is Everyone's Responsibility

To start the conclusion video, **select the image below.**



Notes:

Security Is Everyone's Responsibility

To start the conclusion video, **select the image below.**

9.5 Conclusion Video



Notes:

Remember, as you go about your daily duties, please take your security responsibilities seriously. Because security is everyone's responsibility. Don't hesitate...if you see it, report it! You can make a difference!

9.6 For More Information

CONCLUSION

For more information regarding DOE HQ security requirements, policies, and actions, contact your HSO or refer to the HQFMSP by selecting the link below. You can call the Office of Headquarters Security Operations at 301-903-9990 for more information on these and any other security related matters at HQ.

 [Headquarters Facilities Master Security Plan](#)

AND REMEMBER, SECURITY IS EVERYONE'S RESPONSIBILITY!

Notes:

For more information regarding DOE HQ security requirements, policies, and actions, contact your HSO or refer to the HQFMSP by selecting the link below. And remember, security is everyone's responsibility.

9.7 Exit



Notes:

You Have Successfully Completed the Course. Select the Exit Course button below to close the window.