

Course Information

Select each item to learn more

**Course Goals
& Objectives**

**Course
Requirements**

**Course
Structure**



Course Information

Select each item to learn more

**Course Goals
& Objectives**

**Course
Requirements**

**Course
Structure**

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

- Describe the position of the Facility Security Officer (FSO) and their roles and responsibilities in DOE Security.
- Identify security requirements needed by FSOs.
- Identify security-related concepts for FSOs.



Course Information

Select each item to learn more

 **Course Goals
& Objectives**

**Course
Requirements**

**Course
Structure**

These are the required steps for completing this course and receiving credit for it on your transcript in the Learning Nucleus (LN) Learning Management System:

- View all pages.
- Pass all tests with a score of 80% or higher.
- Complete the NTC Student Feedback Form.



Course Information

Select each item to learn more

 Course Goals
& Objectives

 Course
Requirements

Course
Structure

This course consists of three lessons, each followed by a lesson test. Each lesson should take approximately 15-20 minutes to complete.

- Lesson 1: Introduction and FSO Roles
- Lesson 2: FSO Oversight Responsibilities
- Lesson 3: Other Related Concepts for FSOs



PMC-110DE

Facility Security Officer Overview

Begin Course

A man with a shaved head, wearing a blue polo shirt, stands in front of a screen. The screen displays three lesson options: Lesson 1, Lesson 2, and Lesson 3. Lesson 1 is highlighted with a white border, while Lesson 2 and Lesson 3 have a grey background and a small 'x' icon to their left. The background behind the man includes a green plant and a window with glass blocks.

Lesson 1

⊗ Lesson 2

⊗ Lesson 3

Select Lesson 1 to begin

Lesson Objectives

When you finish this lesson, you will be familiar with the position of Facility Security Officer (FSO) and the role it plays in DOE security.

The lesson objectives are as follows:

1. Identify the responsibilities of an FSO
2. Identify the role of an FSO
3. Identify Key Officials in DOE Security
4. Identify reference material that is helpful to an FSO



Responsibilities of an FSO

Every organization performing Safeguards and Security (S&S) tasks and services for the U.S. Department of Energy (DOE) is required to appoint its own Facility Security Officer (FSO).

Examples of organizations that require an FSO are DOE offices, prime contractors to DOE, or subcontractors to a prime contractor. DOE, the prime contractor, and the subcontractors each appoint their own FSOs to serve as security points of contact (POCs).

More important than being a POC is the FSOs responsibility for administering the requirements of the S&S Program within their facility and ensuring proper levels of protection are provided to prevent unacceptable, adverse impacts on national security or on the health and safety of DOE and contractor employees, the public, or the environment.

In addition to complying with DOE requirements, companies operating under the auspices of the National Industrial Security Program (NISP) may have additional training requirements. These requirements are based on the company's or facility's involvement with classified information.

Requirements may include an FSO orientation course and for FSOs at facilities with safeguarding capability, an FSO Program Management course.



FSOs must complete training appropriate to their position and the security operations conducted at their assigned facilities.

This training should be completed within 6 months of appointment to the position of FSO. This applies to all DOE facilities and newly appointed FSOs. This online NTC course fulfills this initial requirement.



Roles of an FSO

The importance of the FSO's role within the organization cannot be overstated. In serving as the company's POC for any security-related matter, the FSO directs the implementation of security measures and is responsible for coordinating implementation of a security program with the prime contractor and DOE.

FSOs are instrumental in making sure that personnel are aware of good security procedures and practice them, whether personnel have access to classified information or other DOE security interests or not.

FSOs ensure that the organization's employees know their responsibilities regarding security procedures.

The duties assigned to FSOs can vary widely depending on the structure of their organizations. For example, whether or not the FSO's office location is physically separated from the location where employees work can have an impact on the FSO's role. Another factor is whether the company is a possessing facility.

FSOs are the primary POC for processing the contractor personnel security clearance (PCL) with DOE. This would be for all employees and company key management personnel (KMP).

It is also their duty to verify the termination of all S&S activity and personnel clearances once the contract is no longer active and terminated. FSOs must provide security closeout documentation, for both possessing and non-possessing contractors facilities.



Resources

The imp
cannot
for any
implem
for coo
the prin
FSOs a
aware o
whethe
or other
FSOs e
respons

[10 CFR Part 860.4, Unauthorized Introduction of Weapons or Dangerous Materials](#)

[32 CFR Part 117, National Industrial Security Program Operating Manual](#)

[32 CFR Part 2004, National Industrial Security Program](#)

[41 CFR Part 101-20.3, Conduct on Federal Property](#)

[DOE O 470.4B Chg 3, Safeguards and Security Program](#)

[DOE O 474.2 Chg 4, Nuclear Material Control and Accountability](#)

[DOE O 473.1A, Physical Protection Program](#)

[DOE O 471.6 Chg 3, Information Security](#)

[National Training Center \(NTC\) Home Page](#)

[DOE Policy Information Resource \(PIR\) Glossary](#)

on the
not the
tion
role.
cility.

be for
(KMP).
vity and
e and
ntation,
ties.



FSO Requirements

As cited in the DOE Policy Information Resource (PIR) Glossary, an FSO must be a U.S. citizen with an access authorization equivalent to the facility clearance assigned the responsibility of administering the requirements of the S&S Program within the facility.

In order to meet the requirements of 32 CFR Part 117, NISPOM the FSO must ensure adherence to all applicable S&S DOE Orders.

Contractor FSOs and key management personnel must possess access authorizations equivalent to the level of the facility clearance.



Key Security Officials

- Secretary of Energy
- Deputy Secretary
- Under Secretary
- Head of Field Elements
- Director
- Chief Security Officers
- Deputy Under Secretary

Select each official on the left to learn more

For a full description of each key official, select DOE O 470.4B, Chg 3 in the Resources.

i Select the info button to learn more



Key Security Officials

- Secretary of Energy
- Deputy Secretary
- Under Secretary
- Head of Field Elements
- Director
- Chief Security Officers
- Deputy Under Secretary

Select each official on the left to learn more

Secretary of Energy

Ensures that an effective S&S Program is established and executed within DOE under the authorities granted by relevant Executive Orders; the U.S. Department of Energy Organization Act, as amended (42 U.S.C. Sections 7101 to 7352); and the Atomic Energy Act, as amended (42 U.S.C. Sections 2011 to 2286); and in accordance with Protection Level 106-65, the National Nuclear Security Administration Act.

i Select the info button to learn more



Key Security Officials

- ✓ Secretary of Energy
- ✓ Deputy Secretary
- Under Secretary
- Head of Field Elements
- Director
- Chief Security Officers
- Deputy Under Secretary

Select each official on the left to learn more

Deputy Secretary

Exercises responsibility, as Chief Operating Officer of the Department, for S&S policy development and operations.

i Select the info button to learn more

Key Security Officials

- ✓ Secretary of Energy
- ✓ Deputy Secretary
- Under Secretary
- Head of Field Elements
- Director
- Chief Security Officers
- Deputy Under Secretary

Select each official on the left to learn more

Under Secretary for Nuclear Security

Responsible for the management and implementation of S&S programs administered by National Nuclear Security Administration (NNSA) and its subordinate offices, including provision of the appropriate level of authorities and resources to the NNSA Chief Security Officer to effectively manage and execute S&S responsibilities.

Part 1 Part 2 Part 3 ▶

i Select the info button to learn more



Key Security Officials

- ✓ Secretary of Energy
- ✓ Deputy Secretary
- Under Secretary
- Head of Field Elements
- Director
- Chief Security Officers
- Deputy Under Secretary

Select each official on the left to learn more

Under Secretary for Science & Innovation

Responsible for management and implementation of S&S programs administered by the DOE Office of the Under Secretary for Science and Energy and its subordinate offices, including provision of the appropriate level of authorities and resources to the Under Secretary for Science and Energy Chief Security Officer to effectively manage and execute S&S responsibilities.

◀ Part 1 Part 2 Part 3 ▶

i Select the info button to learn more

Key Security Officials


- ✓ Secretary of Energy
- ✓ Deputy Secretary
- ✓ Under Secretary
- Head of Field Elements
- Director
- Chief Security Officers
- Deputy Under Secretary

Select each official on the left to learn more

Under Secretary for Infrastructure

Responsible for management and implementation of S&S programs administered by the Office of the Under Secretary for Management and Performance and its subordinate offices, including provision of the appropriate level of authorities and resources to the Management and Performance Chief Security Officer to manage and execute S&S responsibilities.

◀ Part 1 Part 2 Part 3

 Select the info button to learn more

Key Security Officials


- ✓ Secretary of Energy
- ✓ Deputy Secretary
- ✓ Under Secretary
- ✓ Head of Field Elements
- Director
- Chief Security Officers
- Deputy Under Secretary

Select each official on the left to learn more

Head of Field Elements and Headquarters Departmental Elements

Oversees the development of S&S plans that describe S&S policy implementation in accordance with the requirements in DOE O 470.4B, Chg 3 and its appendices and attachments.

If you are an FSO at a DOE site or facility, the field office ODFSA is your Federal risk acceptance authority.

 Select the info button to learn more



Key Security Officials

- ✓ Secretary of Energy
- ✓ Deputy Secretary
- ✓ Under Secretary
- ✓ Head of Field Elements
- Director
- ✓ Chief Security Officers
- Deputy Under Secretary

Select each official on the left to learn more

Director, Office of Enterprise Assessments

Responsible for management and implementation of S&S programs administered by the Office of the Under Secretary for Management and Performance and its subordinate offices, including provision of the appropriate level of authorities and resources to the Management and Performance Chief Security Officer to manage and execute S&S responsibilities.

Part 1 Part 2 Part 3 ▶

i Select the info button to learn more

Key Security Officials

- ✓ Secretary of Energy
 - ✓ Deputy Secretary
 - ✓ Under Secretary
 - ✓ Head of Field Elements
 - Director
 - ✓ Chief Security Officers
 - Deputy Under Secretary
- Select each official on the left to learn more

Director, Office of Intelligence & Counterintelligence

Responsible for management and implementation of S&S programs administered by the Office of the Under Secretary for Management and Performance and its subordinate offices, including provision of the appropriate level of authorities and resources to the Management and Performance Chief Security Officer to manage and execute S&S responsibilities.

◀ Part 1 Part 2 Part 3 ▶

i Select the info button to learn more

Key Security Officials

- ✓ Secretary of Energy
 - ✓ Deputy Secretary
 - ✓ Under Secretary
 - ✓ Head of Field Elements
 - ✓ Director
 - ✓ Chief Security Officers
 - Deputy Under Secretary
- Select each official on the left to learn more

Director, Office of Environment, Health, Safety, and Security (EHSS)

Act as the Senior Agency Official, responsible for the direction and administration of the DOE information security program pursuant to section 5.4(d) of E.O. 13526 of December 29, 2009, Classified National Security Information. Responsible for the direction and administration of the DOE implementation of and compliance with the National Industrial Security Program pursuant to section 203(a) of Executive Order 12829 of January 6, 1993, National Industrial Security Program.

◀ Part 1 Part 2 Part 3

i Select the info button to learn more

Key Security Officials

- ✓ Secretary of Energy
- ✓ Deputy Secretary
- ✓ Under Secretary
- ✓ Head of Field Elements
- ✓ Director
- ✓ Chief Security Officers
- Deputy Under Secretary

Select each official on the left to learn more

Chief Security Officers for NNSA, Science and Innovation, and Infrastructure

Responsible and accountable for the development and implementation of the S&S programs for personnel, facilities, and sites within their respective offices.

i Select the info button to learn more



Key Security Officials

- ✓ Secretary of Energy
 - ✓ Deputy Secretary
 - ✓ Under Secretary
 - ✓ Head of Field Elements
 - ✓ Director
 - ✓ Chief Security Officers
 - ✓ Deputy Under Secretary
- Select each official on the left to learn more

Deputy Under Secretary for Counterterrorism and Counterproliferation

Provides recommendations on SECON levels to the Deputy Secretary in coordination with the Under Secretaries, the NNSA Administrator, the Office of Intelligence and Counterintelligence, and the Associate Under Secretary for Environment, Health, Safety and Security.

i Select the info button to learn more



What is the primary role of a Facility Security Officer?

- To serve as the organization's point of contact (POC) for facility related security matters.
- To determine what responsibilities they want to assume and be accountable for.

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Orders and National Drivers

The DOE and national requirement documents shown to the right reference or provide the requirements for an FSO.

A link to each document is provided. The links are also available by selecting the “Resources” icon at the bottom right of the screen.

- [Atomic Energy Act of 1954, as amended](#)
- [DOE O 470.4B, Safeguards and Security Program](#)
- [Executive Order 12829](#)
- [Executive Order 13526](#)
- [Security Executive Agent Directive \(SEAD\) 4 National Security Adjudicative Guidelines](#)
- [32 Code of Federal Regulation \(CFR\) Part 117, National Industrial Security Program Operating Manual \(NISPOM\)](#)



Lesson Summary

You should now be familiar with the following material:

1. The responsibilities of an FSO
2. The role of an FSO
3. Key Officials in DOE Security
4. Reference material that is helpful to an FSO



An exam based on the lesson objectives follows this slide. You may only review course material prior to beginning the exam.

Select NEXT button to begin the test



Test

You have reached the test section of this course. You will be asked 5 questions. Answer 80% of them correctly to complete the test.

Select the Start Test button to begin.

Start Test

Test

Question 1/5

The primary responsibility of an FSO is _____.

- Providing guidance to DOE and DOE prime contractor FSOs
- Administering the requirements of DOE S&S Program within their facility
- Determining what responsibilities they want to assume and for which they will be held accountable
- Overridden by the responsibilities of the FSO to their individual companies or organizations

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Test

Question 2/5

Which of the following are true statements about the role of an FSO? Select all that apply.

- An FSO ensures the organization's employees know their responsibilities regarding security procedures.
- The duties assigned to an FSO do not differ from one organization to another.
- An FSO serves as the company's POC for any security-related matter.
- The roles of FSOs within the same organization may differ.

Multiple Response

Choose the correct answer, then select the Submit button.

Submit

Test

Question 3/5

Which key official exercises responsibility, as Chief Operating Officer of the Department, for S&S policy development and operations?

- Under Secretary
- Secretary of Energy
- Deputy Under Secretary
- Deputy Secretary

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Test

Question 4/5

As cited in the DOE Policy Information Resource (PIR) Glossary, an FSO is NOT required to be a U.S. citizen.

- True
- False

True or False

Choose the correct answer, then select the Submit button.

Submit

Test

Question 5/5

To meet the requirements of the 32 CFR Part 117, *National Industrial Security Program Operating Manual (NISPOM)*, the contractor FSO and key management personnel must possess access authorizations equivalent to the level of the facility clearance.

- True
- False

True or False

Choose the correct answer, then select the Submit button.

Submit

A man with a shaved head, wearing a blue long-sleeved polo shirt, stands in a brightly lit hallway. To his left are three black buttons with white text and icons. The top button has a checkmark and says 'Lesson 1'. The middle button says 'Lesson 2'. The bottom button has an 'x' and says 'Lesson 3'. At the bottom of the image is a black banner with white text.

✔ Lesson 1

Lesson 2

✘ Lesson 3

Select Lesson 2 to begin

Lesson Objectives

When you finish this lesson, you will acquire the basic awareness needed by the FSO regarding security requirements.

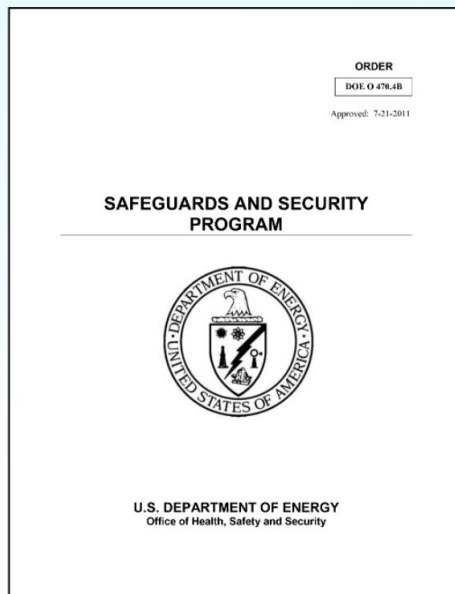
The lesson objectives are as follows:

1. Identify the purpose of the Foreign Ownership, Control, or Influence (FOCI)
2. Categorize facility importance ratings
3. Identify the document and system that formally register a facility within DOE
4. Identify the mandatory S&S awareness briefings
5. Identify incidents of security concern
6. Distinguish between an administrative inquiry and a criminal investigation
7. Identify employee responsibilities during an inquiry
8. Identify the purpose of survey and self assessment
9. Identify FSO responsibilities for Protection Levels 1-8
10. Identify the S&S programs applicable to a facility



Purpose of the FOCI Program

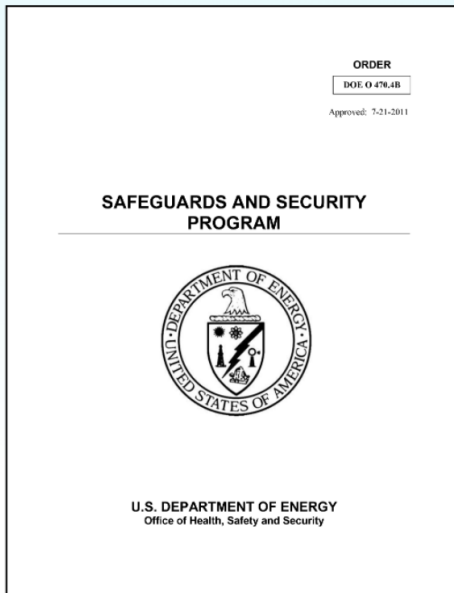
The purpose of the Foreign Ownership, Control, or Influence (FOCI) program is to protect the common defense and security of the facility against any risk because of foreign interests with a U.S. company, if access authorization makes classified information or special nuclear material (SNM) available to contractors or subcontractors whose companies are owned, controlled, or influenced by foreign interests.



Select the image for more information on
**DOE O 470.4B, Appendix B, Section 2,
*Foreign Ownership, Control, or
Influence Program***



General FOCI Program Information



A facility clearance (FCL) will not be granted until all relevant aspects of FOCI have been resolved and, if necessary, favorably adjudicated.

A FOCI determination is required for contractors who will have employees and key management personnel with access authorizations.

If there is a change in a company with an existing FCL that impacts a favorable FOCI determination, the FCL will be suspended or terminated unless security measures are taken to remove the possibility of unauthorized access or adverse impacts to contract performance.

Select the image for more information on DOE O 470.4B, Appendix B, *Section 2, Foreign Ownership, Control, or Influence Program*

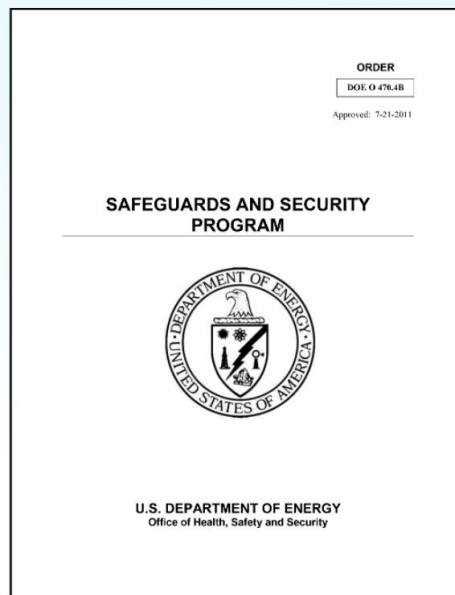


eFOCI Submission Site

The DOE has an electronic system for the submission of FOCI information.

FSOs should be aware of the electronic submission system, eFOCI which may be accessed at <https://foci.anl.gov>.

Applicants must use this system for the submission of FOCI packages, including changes to update their FOCI information.



Select the image for more information on
**DOE O 470.4B, Appendix B, Section 2,
*Foreign Ownership, Control, or
Influence Program***



Facility Importance Ratings



Facility importance ratings (FIR) are used to establish a risk-based system for identifying the level of protection applicable to security assets and activities of facilities.

FIRs are also used to provide a means of identifying the type of S&S facility and/or the type of S&S activities offered by a company seeking to do business with the Department.



Facility Importance Ratings



Each facility granted a facility clearance must be assigned an importance rating, which must be recorded on DOE Form 470.2, Facility Data and Approval Record (FDAR).

The FDAR and the initial facility survey are used as the basis for assigning an importance rating to the facility.



Select the info button to learn more



Facility Importance Ratings



Each facility granted a facility clearance must be assigned an importance rating which must be recorded on DOE Form 470.2, Facility Data and Approval Record (FDAR).

The FDAR and the initial facility survey are used as the basis for assigning an importance rating to the facility.

i

For facilities that do not have classified interests or SNM, the frequency of the periodic survey as required in DOE O 470.4B Chg 3, may be established consistent with risk management principles and documented in the applicable security plan with a description of the reasons for the schedule (e.g., good performance on past surveys and self-assessments, regular satisfactory performance testing, non-possessing facilities, etc.).



Facility Importance Ratings

- A
- B
- C
- D
- E
- PP
- NP

Select each facility importance rating on the left to learn more

For a full description of the seven FIRs, select DOE O 470.4B Chg 3, Appendix B, Section I, Chapter II in the Resources.



Facility Importance Ratings

- A
- B
- C
- D
- E
- PP
- NP

Select each facility importance rating on the left to learn more

FIR A

Assigned to activities and facilities that meet any of the following criteria:

- Engaged in administrative activities essential to the direction and continuity of the overall DOE nuclear weapons program, according to determination by heads of Headquarters elements or field officer
- Authorized to possess Top Secret matter
- Authorized to possess Category I quantities of SNM



Facility Importance Ratings

- A
- B
- C
- D
- E
- PP
- NP

Select each facility importance rating on the left to learn more

FIR B

Assigned to activities and facilities that meet any of the following criteria:

- Engaged in activities other than those categorized as "A" and authorized to possess Secret Restricted Data and/or weapons data
- Designated as a Field Intelligence Element (FIE)
- Authorized to possess Category II quantities of SNM



Facility Importance Ratings

- A
- B
- C
- D
- E
- PP
- NP

Select each facility importance rating on the left to learn more

FIR C

Assigned to activities and facilities that meet any of the following criteria:

- Authorized to possess Categories III and IV quantities of SNM or other nuclear materials requiring safeguard controls or special accounting practices
- Authorized to possess classified matter other than the type categorized for "A" and "B" facilities



Facility Importance Ratings

- A
- B
- C
- D
- E
- PP
- NP

Select each facility importance rating on the left to learn more

FIR D

Assigned to activities and facilities that provide common carrier, commercial carrier, or mail service. These facilities are not authorized to store classified matter or nuclear material. Carriers who do must be assigned an "A," "B," or "C" importance rating.



Facility Importance Ratings

- ✓ A
- ✓ B
- ✓ C
- ✓ D
- ✓ E
- PP
- NP

Select each facility importance rating on the left to learn more

FIR E

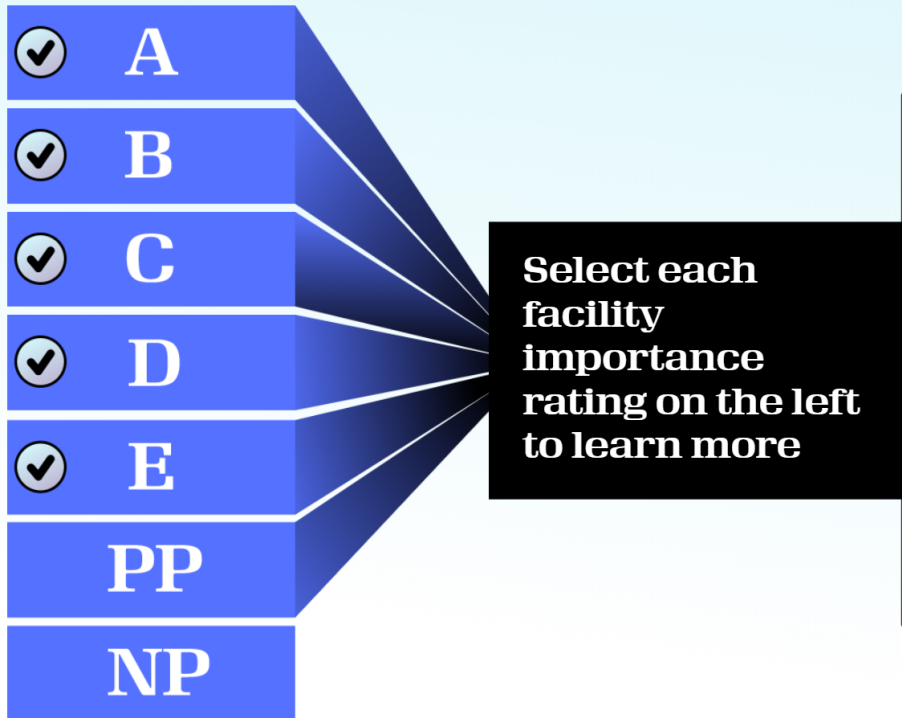
Excluded Parent – assigned to a corporate tier “parent” of a contractor organization that has been barred from participation in the activities related to a contract with DOE.



Back



Facility Importance Ratings



A vertical stack of seven blue buttons with white text. The top five buttons (A, B, C, D, E) each have a white checkmark in a circle on the left. The bottom two buttons (PP, NP) do not. A black callout box with white text is positioned to the right of the top five buttons, pointing towards them.

A

B

C

D

E

PP

NP

Select each facility importance rating on the left to learn more

Property Protection

Assigned to facilities to which a special standard of protection must be applied when a facility has any of the following:

- Government property of a significant monetary value (\$5 million or more)
- Nuclear materials other than those categorized as types "A," "B," or "C" that require safeguard controls or special accounting procedures



Back



Facility Importance Ratings

- ✓ A
- ✓ B
- ✓ C
- ✓ D
- ✓ E
- ✓ PP
- NP

Select each facility importance rating on the left to learn more

Property Protection

- DOE program continuity
- National security considerations
- Responsibilities for protection of public health and safety
- Basic considerations that include physical protection to prevent or deter acts of arson, civil disorder, riots, sabotage, terrorism, vandalism, and theft or destruction of DOE property and facilities



Back



Facility Importance Ratings

✓ A
✓ B
✓ C
✓ D
✓ E
✓ PP
✓ NP

Select each facility importance rating on the left to learn more

Non-Possessing

Assigned to facilities that have authorized access to classified information or SNM at other approved locations.

Non-possessing facilities do not, themselves, possess any classified matter or nuclear material.



Back



Facility Clearance Program



The facility clearance program regulates Departmental approval of a facility's eligibility to access, receive, generate, reproduce, store, transmit, or destroy classified matter, SNM, other hazardous material presenting a potential radiological or toxicological sabotage threat, and/or over \$5 million of DOE property exclusive of facilities and land value (collectively, S&S activities). DOE requires that a facility clearance (FCL) be granted to a facility before any performance of S&S activities is permitted.

It is important to note that the term *facility clearance*, as used in this lesson, applies to both the contractor clearance (for non-possessing facilities) and the contractor facility clearance (for possessing facilities).

The terms *facility*, *facility clearance*, and *S&S activity* have DOE-specific meanings exclusive to a DOE environment.

Select the forward arrow to learn more



Facility Clearance Program



Facility

An educational institution, manufacturing plant, laboratory, office building, or complex of buildings located on the same site that is operated and protected by the Department of the U.S. Nuclear Regulatory Commission, or their contractors.

◀ 1 2 3 ▶

Facility Clearance Program



Facility Clearance (FCL)

An administrative determination that a facility is eligible to access, receive, produce, use, and/or store classified matter, nuclear materials, or Departmental property of significant monetary value.

DOE Form 470.2, Facility Data Approval Record (FDAR), basically acts as the facility's "birth certificate". The FDAR serves to formally register a facility with DOE. The facility cannot perform any work for DOE until the FDAR is in place.

FSOs have a responsibility to report any changes within the company, whether or not there are FOCl concerns.

A company's FDAR information must be accurate and current. Changes must be reported to the responsible DOE office and in the eFOCl submission site for companies with DOE FOCl determinations.



Facility Clearance Program



S&S Activity

Any work performed under contract, subcontract, or other agreement that involves access to classified information, nuclear material, or Departmental property of significant monetary value by the Department, a Departmental contractor, or any other activity under the Department's jurisdiction.

Also included is the verification of the capabilities of approved Federal locations.



What type of facility would a Facility Importance Rating A be assigned to?

- A facility that is not authorized to possess Top Secret matter
- A facility that is authorized to possess Top Secret matter

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

S&S Awareness Briefings

An FSO is responsible for providing mandatory security briefings; the extent to which the FSO is responsible for providing these briefings differs from organization to organization. It is influenced by the organization's Site Security Plan (SSP) agreement with the lead responsible office or the prime contractor's FSO.

Required briefing subjects are described in DOE O 470.4B Chg 3, Safeguards and Security Program. Subjects include facility overview, classification and access authorization procedures, protection of unclassified controlled information, badging and access control procedures, prohibited articles, property protection procedures, reporting responsibilities, and substance abuse policies.

Briefings are at the heart of any security awareness program. Each program must include the development and presentation of at least four types of briefings: initial, comprehensive, refresher, and termination.



i For more detailed information on FSO responsibilities for S&S briefings, see DOE O 470.4B, *Safeguards and Security Program* (search Appendix A, Section 1, Chapter 1, Security Plans) in the resources.



Types of Briefings

Initial
Briefing

Comprehensive
Briefing

Refresher
Briefing

Termination
Briefing

Select each type of briefing to learn more



Types of Briefings

**Initial
Briefing**

**Comprehensive
Briefing**

**Refresher
Briefing**

**Termination
Briefing**

DOE Federal and contractor employees who receive a DOE security badge must receive an initial briefing before they are given unescorted access to other-than-public areas of the facility/site.

The initial briefing must be completed before personnel assume their duties. A transferred individual must complete a site-specific initial briefing before assuming duties at the new site.

Initial briefing records must be maintained. Records may be maintained in conjunction with badging records or other records pertaining to access control.

Part 1

Part 2



Types of Briefings



**Initial
Briefing**

**Comprehensive
Briefing**

**Refresher
Briefing**

**Termination
Briefing**

Content of the briefing includes

- overview of DOE facility/organization's mission
- overview of facility/organization's major S&S program responsibilities
- access control
- escort procedures
- protection of Government property and badge procedures
- identification of controlled and prohibited articles
- protection of controlled unclassified information (CUI), including Official Use Only information
- procedures for reporting incidents of security concern (e.g., attempts to gain unauthorized access to the facility or to classified information or matter)
- identification of classification markings



Part 1

Part 2



Types of Briefings



Initial
Briefing

Comprehensive
Briefing

Refresher
Briefing

Termination
Briefing

An individual must receive a comprehensive briefing upon receipt of a security clearance and before receiving initial access to classified information or matter, or SNM.

The content for the comprehensive briefing must include the following items:

- **Basic classification security policies and principles**
 - definition of classified information or matter
 - purpose of DOE classification program
 - levels and categories of classified information or matter
 - damage criteria associated with each classification level
 - classification awareness requirements contained in DOE O 475.2B, Identifying Classified Information.

Part 1

Part 2

Part 3



Types of Briefings



**Initial
Briefing**

**Comprehensive
Briefing**

**Refresher
Briefing**

**Termination
Briefing**

o **Classified information or matter protection elements**

- procedures for protecting classified information and matter
- definition and penalties of unauthorized disclosures
- conditions and restrictions for access to classified information or matter
- individual's S&S reporting requirements
- protection and control of classified information or matter, and controlled unclassified information, including telecommunications and electronic transmissions and Official Use Only information

- information pertaining to security badges, security clearance levels, and access controls
- responsibilities associated with escorting
- targeting and recruitment methods of foreign intelligence services
- general information concerning the protection of SNM, if applicable
- purpose and requirements of and responsibilities for the Standard Form (SF) 312
- legal and administrative sanctions for security infractions and violations of law

Part 1

Part 2

Part 3



Types of Briefings



- **Personnel security elements**
 - purpose of the personnel security program
 - sources of legal authority and guidance
 - the access authorization process
 - key terms associated with adjudications
 - adjudication factors
 - due process
 - individual reporting requirements

Comprehensive briefings must be completed before individuals are granted access to classified information or matter, or SNM. A comprehensive briefing may also be completed when a security clearance is shared or transferred to another DOE facility/organization. Initial and comprehensive briefings may be combined at the discretion of facility/site security management. Under such circumstances, the briefings must include information prescribed for both initial and comprehensive briefings.

Documentation of the comprehensive briefing must be maintained. The Standard Form (SF) 312 must be used to document the first comprehensive briefing after the grant of a security clearance, and may be used to document subsequent comprehensive briefings.

Part 1 Part 2 Part 3

Types of Briefings



**Initial
Briefing**



**Comprehensive
Briefing**

**Refresher
Briefing**

**Termination
Briefing**

Cleared individuals must receive annual refresher briefings. Agreements between DOE elements and/or contractor organizations may be established to ensure that individuals temporarily assigned to other DOE locations receive refresher briefings on schedule.

The refresher briefing offers a critical opportunity to influence and affect a person's understanding and knowledge of security. It is essential that coordinators stay aware of local and national security developments, issues, and concerns. The refresher briefing may be delivered by the various methods including:

- oral presentation
- video
- computer- or web-based presentations

Refresher briefings must selectively reinforce the information provided in the comprehensive briefing based upon current facility/site-specific security issues as well as counterintelligence (CI) awareness, and address the classification refresher requirements contained in DOE O 475.2B.

Part 1

Part 2



Types of Briefings

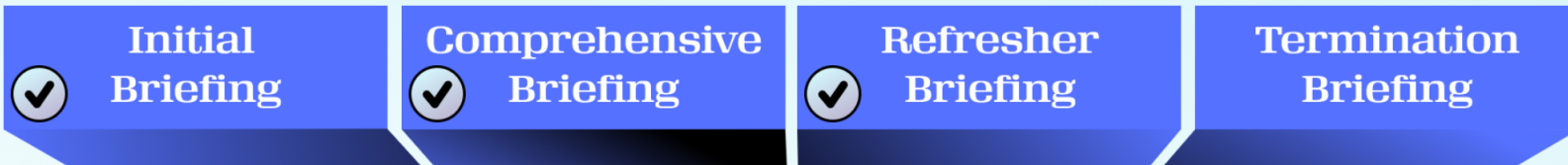


Failure to complete the annual refresher briefing by an individual who holds a security clearance will result in administrative actions determined by the cognizant security office, including possible administrative termination of the security clearance, until such time as the individual has complied with the briefing requirement. The processing personnel security office responsible for the clearance must be notified in accordance with DOE O 470.4B requirements when a clearance is terminated for this reason.

Refresher briefings must be conducted each calendar year at approximately 12-month intervals.

Documentation of refresher briefings must be maintained for individuals until their next briefing. Documentation may be in electronic or hard copy format. Documentation must include the ability to identify individuals who have not met their refresher briefing requirement.

Types of Briefings



A termination briefing is required whenever a security clearance has been or will be terminated. Termination briefings must reiterate to the individual the continuing responsibility not to disclose classified information or matter to which they had access, the potential penalties for noncompliance, and the obligation to return all unclassified controlled and classified documents and materials in the individual's possession to the cognizant security office or to the DOE.

The content for the termination briefing must include:

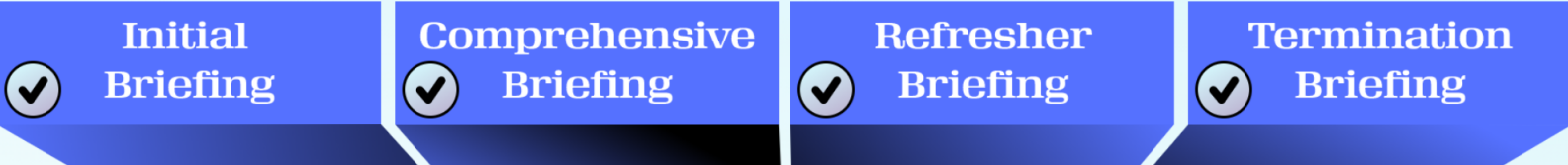
- information contained in the numbered items of the Security Termination Statement Form (DOE F 5631.29 or successor form)
- information contained in items 3, 4, 5, 7, and 8 of the SF 312
- penalties for unauthorized disclosure of classified information or matter as specified in the Atomic Energy Act and pertinent sections of 18 U.S.C.
- penalties for unauthorized disclosure of Unclassified Controlled Nuclear Information (UCNI).

Part 1

Part 2



Types of Briefings



The termination briefing must be conducted on the individual's last day of employment, the last day the individual possesses a security clearance, or the day it becomes known that the individual no longer requires access to classified information or matter, or SNM, whichever is sooner.

If the individual is not available for the termination briefing, the completed but unsigned security termination statement and an explanation of the circumstances surrounding the termination and why the signature could not be obtained must be submitted to the processing personnel security office.

Required notification: When an individual no longer requires a security clearance/access authorization, or when a clearance/access authorization is administratively terminated, the processing personnel security office must be notified electronically or verbally within two working days to be followed by submission to that office of a completed DOE F 5631.29, Security Termination Statement. Records documenting receipt of the termination briefing must be maintained.

This briefing must be documented by completing DOE F 5631.29 or by written notice.



True or False: After an access authorization is granted, an individual must be given a comprehensive security briefing before they are given access to classified matter or SNM.

- True
- False

True or False

Choose the correct answer, then select the Submit button.

Submit

Incidents of Security Concern

Infraction

Administrative
Inquiry

Criminal
Investigation

Select each activity to learn more

Incidents of Security Concern (IOSC) are events that are of concern to DOE S&S program that warrant preliminary inquiry and subsequent reporting. IOSCs at the time of occurrence are of enough concern to warrant immediate review, inquiry, assessment, and reporting.

The FSO may participate in some preliminary aspects of responding to IOSCs and may also be called upon to assist with the conduct of inquiries, as set forth in DOE directives such as DOE O 470.4B Chg 3, Safeguards and Security Program.



Incidents of Security Concern

Infraction

Administrative
Inquiry

Criminal
Investigation

Infraction

Infractions are any knowing, willful, or negligent action contrary to the requirements of Executive Order 13526, Classified National Security Information, as amended, or its implementing directives that does not constitute a violation.

An infraction is also the documentation of administrative and/or disciplinary actions assigned to an individual taken in response to an IOSC.

Part 1

Part 2



Incidents of Security Concern



Infraction

Administrative
Inquiry

Criminal
Investigation

Infraction

Types of Incidents that may result in infractions include the following:

- Failure to properly store and protect classified documents or matter
- Loss of a pass or badge due to negligence
- Failure to safeguard a computer access password
- Leaving an up-and-running computer workstation unattended at the close of business (or when the room is unattended) when it contains classified information or has access to a classified host computer
- Any attempt to obstruct justice



Part 1

Part 2



Incidents of Security Concern



Infraction



Administrative
Inquiry

Criminal
Investigation

Administrative Inquiry

An inquiry is a review of the circumstances surrounding an IOSC to compile all pertinent information and to determine whether an infraction, violation, or a compromise or potential compromise has occurred.

An inquiry does not indicate suspicion of intentional, criminal violation of law; it is simply a data-gathering exercise generally conducted by the contractor.

Inquiries are terminated immediately upon discovery of credible evidence that an intentional, criminal violation of law may have occurred. Inquiries must be kept separate from investigations.



Incidents of Security Concern



Infraction



Administrative
Inquiry



Criminal
Investigation

Criminal Investigation

In contrast to an inquiry, an investigation is a review by law enforcement entities of the circumstances surrounding an IOSC, which is a result of an inquiry's collection of facts and evidence about a suspected violation of law. It is used to support criminal prosecution generally conducted by Federal law enforcement.

An investigation is also a process used to gain an understanding of a Material Control & Accountability discrepancy, incident, or alarm, its cause(s), and if the situation is not satisfactorily resolved, the corrective action(s) necessary to prevent recurrence or remedy the problem. (DOE Policy Information Resource Glossary)



Potential Incidents of Security Concern

JANUARY						
SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Select each number below to learn more



Potential Incidents of Security Concern

JANUARY						
SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

The FSO in communication/coordination with applicable management and/or the Officially Designated Federal Security Officer (ODFSA) upon being informed/aware of a potential incident, must immediately examine and document all pertinent facts and circumstances to determine whether an incident occurred.

The preliminary inquiry and categorization is based on the subject policy and any additional criteria as documented in the site IOSC program plan.



Potential Incidents of Security Concern

JANUARY						
SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

The “clock starts” when a potential incident is brought to the attention of management.

At that point, the site has a maximum of 5 calendar days to conduct the preliminary inquiry, to make the initial categorization, and to perform the initial notification(s).



Potential Incidents of Security Concern

JANUARY						
SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Although a maximum of 5 calendar days are provided, sites are required to report the incident as soon as the incident is categorized.

The 5-day period provides flexibility for those incidents requiring additional fact-gathering, such as a classification review or an inventory check to locate a potentially lost/missing item.

If there is still uncertainty at the 5 calendar day mark, with respect to incident categorization, the incident must be reported as a Category A pending completion of the inquiry process.



Potential Incidents of Security Concern

JANUARY						
SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

If the final inquiry reveals additional details and facts, the incident can be recategorized.

If it is determined that an IOSC has occurred, DOE O 470.4B, Attachment 5 requirements for an IOSC must be followed.



Employee Responsibilities During an Inquiry

The FSO is responsible for raising employees' awareness of their responsibilities in the inquiry process. Employee responsibilities include the following:

Immediately upon discovery, report to the FSO that classified matter, SNM, or other departmental asset has been or may have been lost or compromised or is otherwise unaccounted for.

1

2

3

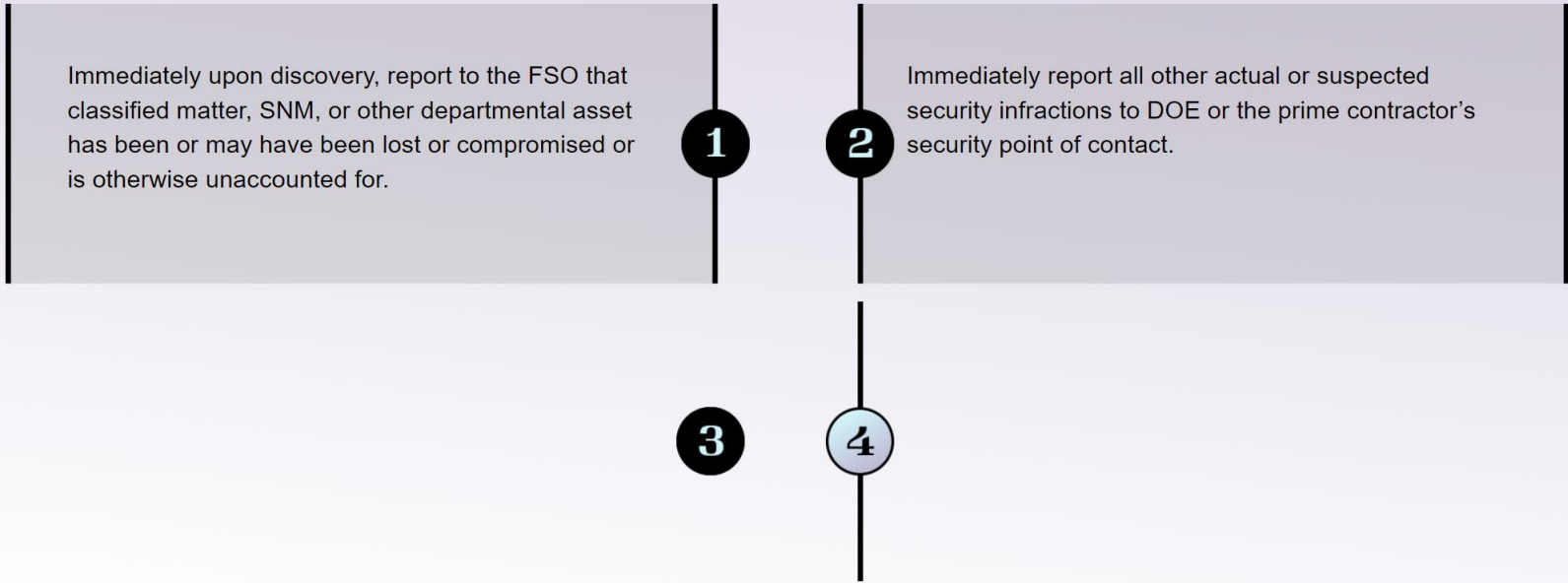
4

Select each number to learn more



Employee Responsibilities During an Inquiry

The FSO is responsible for raising employees' awareness of their responsibilities in the inquiry process. Employee responsibilities include the following:



Select each number to learn more



Employee Responsibilities During an Inquiry

The FSO is responsible for raising employees' awareness of their responsibilities in the inquiry process. Employee responsibilities include the following:

1
Immediately upon discovery, report to the FSO that classified matter, SNM, or other departmental asset has been or may have been lost or compromised or is otherwise unaccounted for.

2
Immediately report all other actual or suspected security infractions to DOE or the prime contractor's security point of contact.

3
Cooperate fully with the employer's inquiry into a work-related misconduct/concern, because they are legally entitled to interview an employee concerning a violation of policy or procedure.

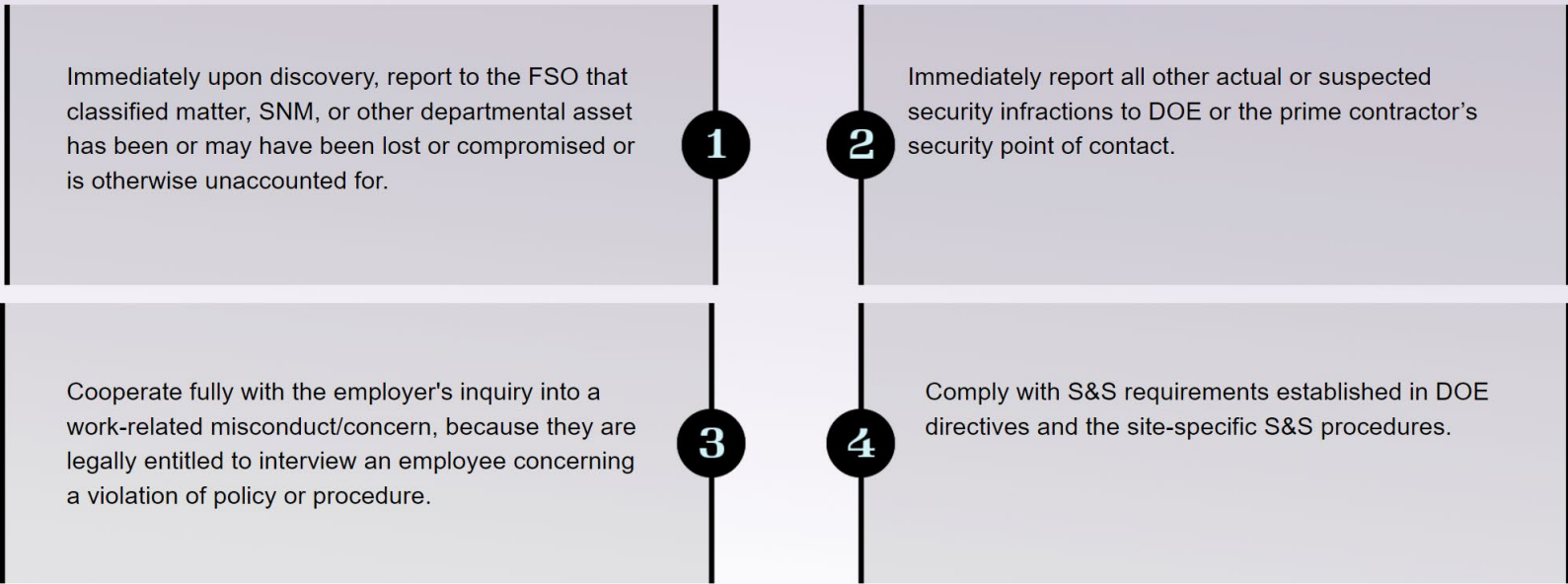
4

Select each number to learn more



Employee Responsibilities During an Inquiry

The FSO is responsible for raising employees' awareness of their responsibilities in the inquiry process. Employee responsibilities include the following:



Select each number to learn more



Purpose of Survey and Self-Assessment

Surveys

**Self-
Assessment**

Surveys and self-assessments are conducted to ensure S&S systems and processes at facilities/sites are operating in compliance with Departmental and national-level policies, requirements, and standards for the protection of security assets and interests.

These programs provide the means for timely identification and correction of deficiencies and noncompliant conditions to prevent adverse events, and validating the effectiveness of corrective actions implemented to address identified deficiencies.

Select each button to learn more



Purpose of Survey and Self-Assessment

Surveys

Self-
Assessment

Survey

An integrated performance and compliance-based evaluation of all applicable topics to determine the overall status of the S&S program at a facility or site and ensure that S&S systems and processes at the location are operating in compliance with Departmental and national-level policies, requirements, and standards.

Surveys are conducted or supervised by Federal security personnel.

Select the forward button
below to learn more.



Purpose of Survey and Self-Assessment

Surveys

Self-
Assessment

Initial Survey

A comprehensive review of the security status at a facility which is a candidate for an FCL conducted to determine whether the facility in question meets established standards for the protection of the security interests and activities to be covered by the FCL.



Purpose of Survey and Self-Assessment

Surveys

Self-
Assessment

Periodic Survey

A survey conducted for all cleared facilities in accordance with established schedules and covering all applicable topics to meet the objectives of the S&S survey.



Purpose of Survey and Self-Assessment

Surveys

Self-
Assessment

Termination Survey

A survey of a cleared facility conducted to verify the termination of Departmental activities and the appropriate disposition of S&S interests at that facility.

The termination survey confirms that all S&S activities have been terminated or awarded to another contractor, that access authorizations have been properly terminated or dispositioned, and that no DOE property, classified information, or matter, and nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat remains.



Purpose of Survey and Self-Assessment



Surveys



Self-
Assessment

Self-Assessment

An internal integrated evaluation of all applicable S&S topical areas at a contractor facility or site, conducted by contractor security personnel at intervals consistent with risk management principles, to determine the overall status of the S&S program at that location and verify that S&S objectives are met.

The DOE cognizant security office may direct a specific self-assessment interval and may direct that self-assessment reports be provided to DOE.



FSO Responsibilities for Protection Levels

The graded protection approach categorizes Department assets into one of eight Protection Levels (PLs) based on consequence of loss.

There are 8 PLs identified in DOE requirements. A DOE facility can have one or more PL requirements and depending on the type of asset, there are certain physical protection requirements that need to be in place to protect the asset(s).

It is important to understand that most facilities will contain multiple PL assets that require protection. For example, a facility with PL-1 assets may also contain PL-2 assets, or facilities with PL-5 or PL-6 assets could possess PL-7 and PL-8 assets.

Protection programs must ensure that assets are provided protection commensurate with their PLs.

FSOs need to know what PL requirements the facilities/site they are responsible for, and are approved for.

The current approved security plan (SP), supported by either a vulnerability assessment or security risk assessment or both for the facilities/site the FSO is responsible for, is required to document how the facility/site meets the physical protection required for the applicable PLs.

The current DOE Order 470.3C, Design Basis Threat (DBT), and DOE Order 473.1A, Physical Protection Program, provide what is required for those 8 PLs, and a site/facility SP is required to capture how the facility and/or site is meeting applicable requirements depending on what PL(s) they have at their particular facilities/site.



Safeguards & Security Programs

1

2

3

4

5

6

7

Select each number to learn more about the S & S programs that may apply to your site/facility.

Interfaces and necessary interactions between S&S programs and other disciplines (e.g., safety, emergency management, classification, counterintelligence, facility operations, cyber security systems operations and security, and business and budget operations, including property management) must be identified and clearly defined.

These interfaces and interactions must be maintained throughout the lifecycle of protective measures to ensure that S&S planning and operations work together effectively with these disciplines.

Sensitive Compartmented Information is under the purview of the Office of Intelligence and Counterintelligence, and necessary interfaces and interactions between that office and S&S programs must also be identified, defined, and maintained.



Safeguards & Security Programs

1

2

3

4

5

6

7

Program Planning and Management

The following is a list of subtopic areas that FSOs need to know about their facilities:

- Protection program management
- Personnel development and training
- Management control
 - Surveys and self-Assessment programs
 - Performance assurance program
 - Resolution of findings
- S&S planning and procedures
- Incident reporting and management
- Program-wide support
- Facility approval and registration of activities
 - Foreign Ownership, Control, or Influence
 - Security management in contracting



Safeguards & Security Programs

✓

2

3

4

5

6

7

Protective Force

The following is a list of subtopic areas that FSOs need to know about their facilities:

- Management
- Training
- Duties
- Facilities and equipment



Safeguards & Security Programs

✓

✓

3

4

5

6

7

Physical Protection

The following is a list of subtopic areas that FSOs need to know about their facilities:

- Access controls
- Intrusion detection and assessment systems
- Barriers and delay mechanisms
- Testing and maintenance
- Communications



Safeguards & Security Programs

✓

✓

✓

4

5

6

7

Information Security

The following is a list of subtopic areas that FSOs need to know about their facilities:

- Basic requirements
- Technical surveillance
- Operations security
- Classification guidance
- Classified matter protection and control
- Control of classified matter
- Special access programs (SAP) and intelligence information



Safeguards & Security Programs

✓

✓

✓

✓

5

6

7

Personnel Security

The following is a list of subtopic areas that FSOs need to know about their facilities:

- Access authorizations
- Human reliability programs
- Control of classified visits
- S&S awareness



Safeguards & Security Programs



6

7

Materials Control & Accountability

The following is a list of subtopic areas that FSOs need to know about their facilities:

- Program administration
- Material accountability
- Materials control
- Measurement
- Physical inventory
- Nuclear Materials Management Safeguards System(NMMSS) reporting



Safeguards & Security Programs



Foreign Visit and Assignments

The following is a list of subtopic areas that FSOs need to know about their facilities:

- Sponsor program management & Admin
- Counterintelligence requirements
- Export controls/Tech transfer
- Security requirements
- Approvals and reporting



Lesson Summary

You should now be familiar with the following material:

1. The purpose of the Foreign Ownership, Control, or Influence (FOCI) program
2. Categorizing facility importance ratings
3. The document that formally registers a facility within DOE
4. Mandatory S&S awareness briefings
5. The definition of an infraction
6. Distinguishing between an administrative inquiry and a criminal investigation
7. Employee responsibilities during an inquiry



An exam based on the lesson objectives follows this slide. You may only review course material prior to beginning the exam.

Select NEXT button to begin the test



Test

You have reached the test section of this course. You will be asked 10 questions. Answer 80% of them correctly to complete the test.

Select the Start Test button to begin.

Start Test

Test

Question 1/10

What are the four types of S&S awareness briefings?

- Job-specific, comprehensive, refresher, and termination
- Initial, job-specific, comprehensive, and refresher
- Initial, comprehensive, refresher, and termination
- Job-specific, initial, comprehensive, and termination

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Test

Question 2/10

Which of the following statements is true in distinguishing an inquiry from an investigation?

- An inquiry does not indicate suspicion of intentional, criminal violation of law whereas an investigation is a review by law enforcement entities about a suspected violation of law.
- An investigation does not indicate suspicion of intentional, criminal violation of law whereas an inquiry is a review by law enforcement entities about a suspected violation of law.

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Test

Question 3/10

Interfaces and necessary interactions between S&S programs and other disciplines such as cyber security systems operations do not need to be identified or clearly defined.

- True
- False

True/False

Choose the correct answer, then select the Submit button.

Submit

Test

Question 4/10

Match each type of facility importance rating to its description.

Authorized to possess Top Secret matter or Category I quantities of SNM

Authorized to possess Secret Restricted Data and/or weapons data or Category II quantities of SNM

Authorized to possess Categories III and IV quantities of SNM or other nuclear materials requiring safeguard controls or special accounting practices

Assigned to activities and facilities that provide common carrier, commercial carrier, or mail service; not authorized to store classified matter or nuclear material

Matching Drop Down

Match each description to the correct answer, then select the Submit button.

Each drop down consists of the letters "A", "B", "C", or "D". Please chose a letter and fill it out next to the corresponding drop down.

Submit

Test

Question 5/10

Which of the following statements are true about the purpose of the Surveys and Self-Assessments? Select all that apply.

- Conducted to ensure that S&S systems and processes at facilities/sites are operating in compliance with departmental policies.
- Conducted to ensure that S&S systems and processes at facilities/sites are operating in compliance with national-level policies.
- Conducted to ensure systems and processes outside of S&S comply with requirements established in DOE directives and site-specific S&S procedures.

Multiple Response

Choose the correct answers, then select the Submit button.

Submit

Test

Question 6/10

**Which of the following are employee responsibilities during the inquiry process?
Select all that apply.**

- Immediately upon discovery, report to the FSO that classified matter has been or may have been lost or compromised or is otherwise unaccounted for.
- Immediately report all other actual or suspected security infractions to DOE or the prime contractor's security point of contact.
- Comply with S&S requirements established in DOE directives and site-specific S&S procedures.
- Cooperate fully with the employer's inquiry into a work-related misconduct/concern.

Multiple Response

Choose the correct answers, then select the Submit button.

Submit

Test

Question 7/10

What is the purpose of the FOCI program?

- To determine the Facility Importance Rating
- To determine the eligibility of a DOE facility to produce classified matter
- To determine any risk to security because of foreign interests with a U.S. company
- To determine the monetary value of DOE property

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Test

Question 8/10

Which of the following is a knowing, willful, or negligent act or omission that does not constitute a violation of law or result in actual compromise, but that could reasonably be expected to result in an unauthorized disclosure of classified information?

- Infraction
- Investigation
- Inquiry
- Incident

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Test

Question 9/10

Which of the following documents serves to formally register a facility with DOE?

- 32 CFR 2004, *National Industrial Security Program*
- Standard Form 312, *Classified Information Nondisclosure Agreement (SF-312)*
- 32 CFR 117, *National Industrial Security Program Operating Manual (NISPOM)*
- DOE Form 470.2, *Facility Data and Approval Record (FDAR)*

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Test

Question 10/10

Which of the following references would an FSO find Protection Level (PL) requirements that apply to their facility or site? Select all that apply.

- DOE Order 473.1A, *Physical Protection Program*
- DOE Order 470.3C, *Design Basis Threat*
- Industrial Security Standards
- DoD/National Requirements

Multiple Response

Choose the correct answers, then select the Submit button.

Submit

A man with a shaved head, wearing a blue polo shirt, stands in an office setting. The background is slightly blurred, showing office furniture and a whiteboard. On the left side of the image, there are three black boxes with white text, each containing a lesson title. The first two boxes have a white checkmark icon to their left. The third box does not.

✔ Lesson 1

✔ Lesson 2

Lesson 3

Select Lesson 3 to begin

Lesson Objectives

When you finish this lesson, you will have a better understanding of other security-related concepts for FSOs.

The lesson objectives are as follows:

1. Identify the purpose of graded protection
2. Identify types of DOE security areas
3. Identify security area controlled/prohibited articles
4. Identify security area privately owned prohibited articles
5. Identify the purpose of the Nuclear Materials Control and Accountability (NMC&A) Program
6. Identify materials designated as SNM
7. Identify SNM classifications



Review of DOE Security Areas

An FSO must have a clear understanding of other security-related concepts.

First, a thorough knowledge of facility security areas is required.

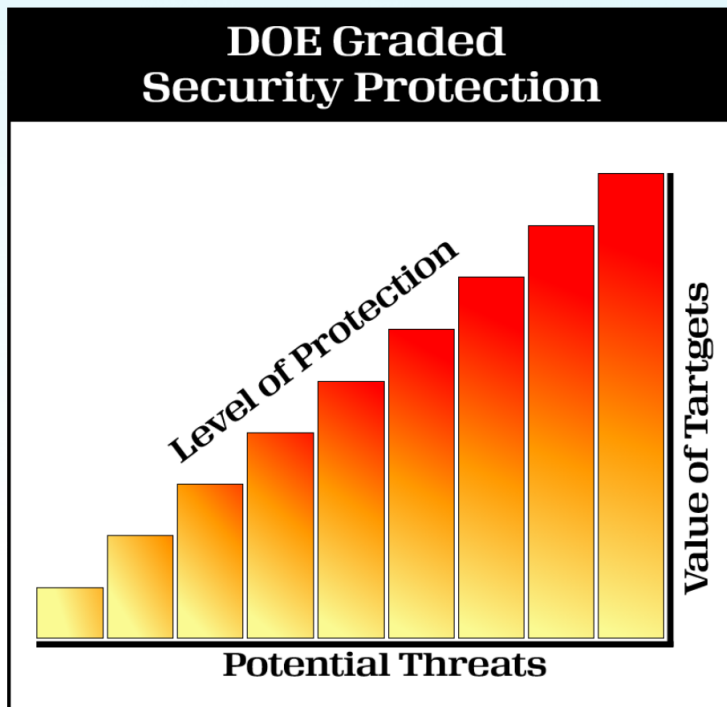
The term security area refers to any area containing DOE S&S interests that require physical protection measures.

DOE facilities typically include a series of physical spaces designated as security areas surrounding a designated S&S interest.

These security areas provide for the imposition of varying or graded protection measures that entail controlling access to and egress from the designated areas and security.



Graded Protection/Defense-in-Depth



Graded protection was developed by DOE to provide varying layers of S&S because the loss, theft, compromise, or unauthorized use of some DOE assets would have a serious impact on national security or the health and safety of DOE and contractor employees, the public, or the environment.

In keeping with the graded safeguards concept, facilities may operate under varying safeguards requirements due to different material types, forms, and quantities.

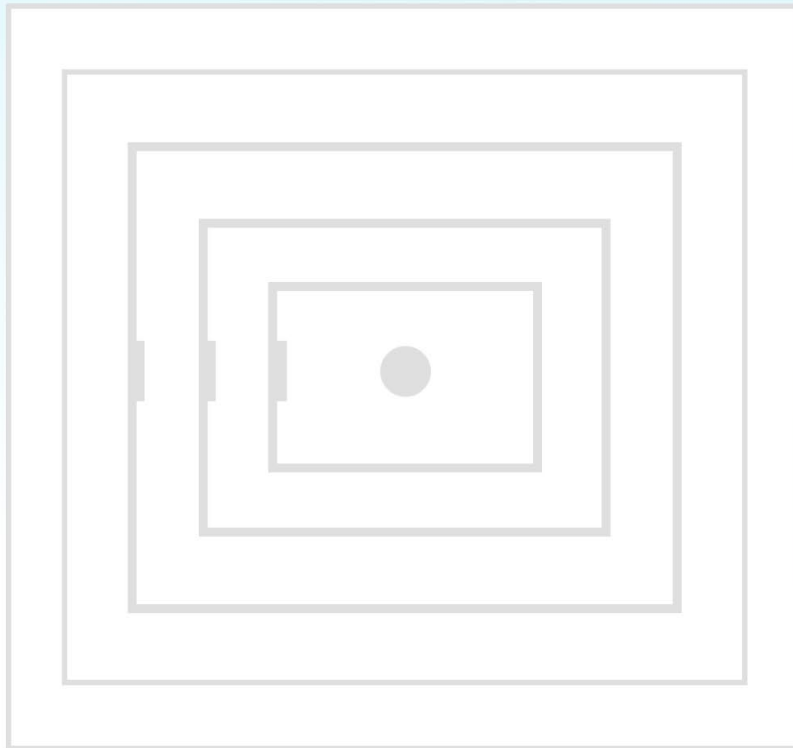
To comply with the DOE graded protection concept, the facility must have controls to assure a system that provides varying degrees of physical protection, accountability, and material control to different types, quantities, physical forms, and compositions of nuclear materials consistent with the risks and consequences associated with threat scenarios.



More details related to graded protection can be found in DOE Orders 473.1A, *Physical Protection Program*; DOE O 470.4B, *Safeguards and Security Program*; DOE O 474.2, *Nuclear Material Control and Accountability* and DOE O 470.3C, *Design Basis Threat (DBT)*.



DOE Security Areas



GAA

PPA

LA

PA

MAA

**Select each level of security
to add it to the map**

**For a full description of each
DOE Security Area, select the
DOE O 473.1A, Physical Protection
link found in the Resources.**



DOE Security Areas



GAA

PPA

LA

PA

MAA

**Select each level of security
to add it to the map**

General Access Area (GAA)

GAA's may be designated by the ODSA to allow access to certain areas with minimum-security requirements.

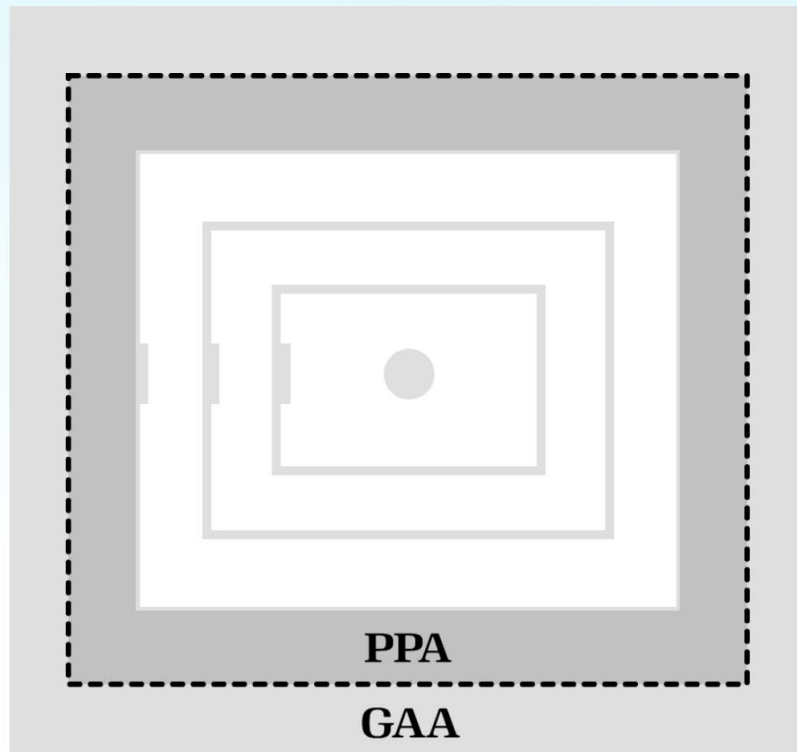
The ODFSA must approve security requirements for those areas designated as GAA's based on a risk management process.

Security requirements and the identification of GAA locations must be documented in SPs approved by the ODFSA.

The security requirements must be posted to inform all personnel, including the public, that entry into these areas subjects them to requirements.



DOE Security Areas



GAA

PPA

LA

PA

MAA

**Select each level of security
to add it to the map**

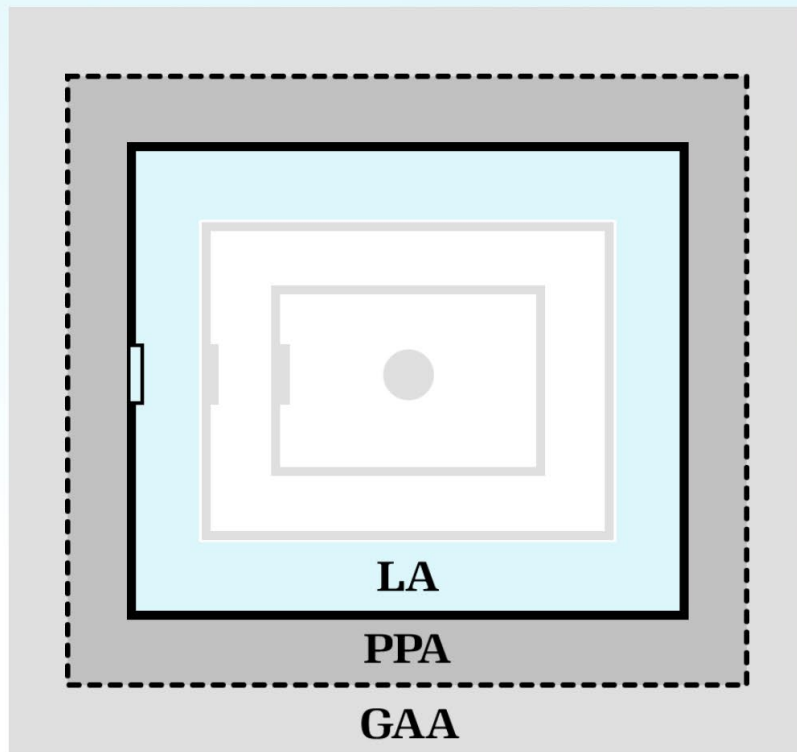
Property Protection Area (PPA)

PPAs are established areas having defined boundaries and access controls for the protection of DOE property.

Protection measures shall be adequate to give reasonable assurance of protection for the assets and Departmental property.



DOE Security Areas



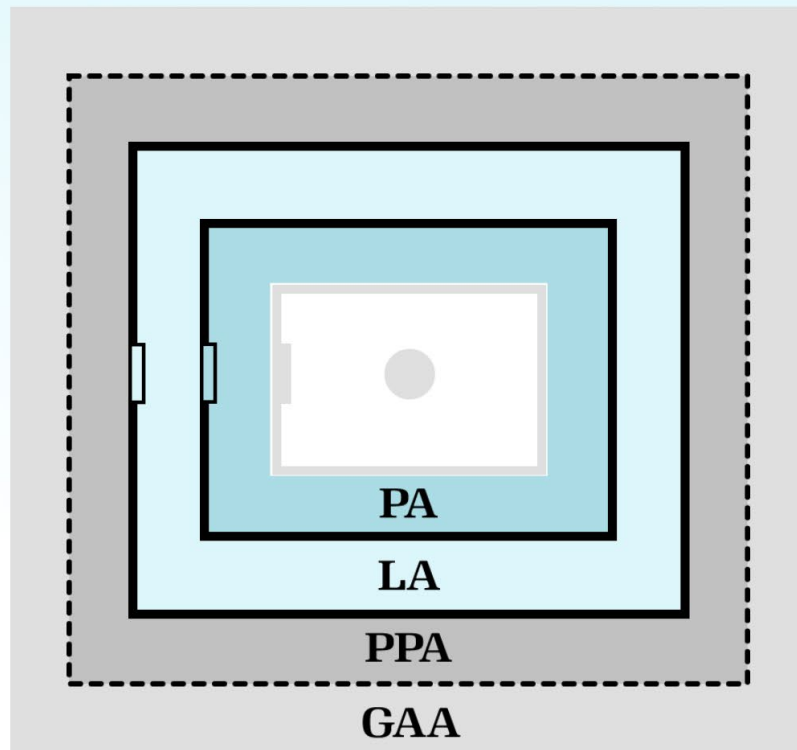
GAA PPA LA PA MAA

Select each level of security to add it to the map

Limited Area (LA)

LAs are security areas having boundaries defined by physical barriers, used for the protection of classified matter and/or Category III quantities of SNM, where protective personnel or other internal controls can prevent access by unauthorized people to classified matter or SNM. Security officers, security police officers, or other internal security measures provide the necessary means to control access.

DOE Security Areas



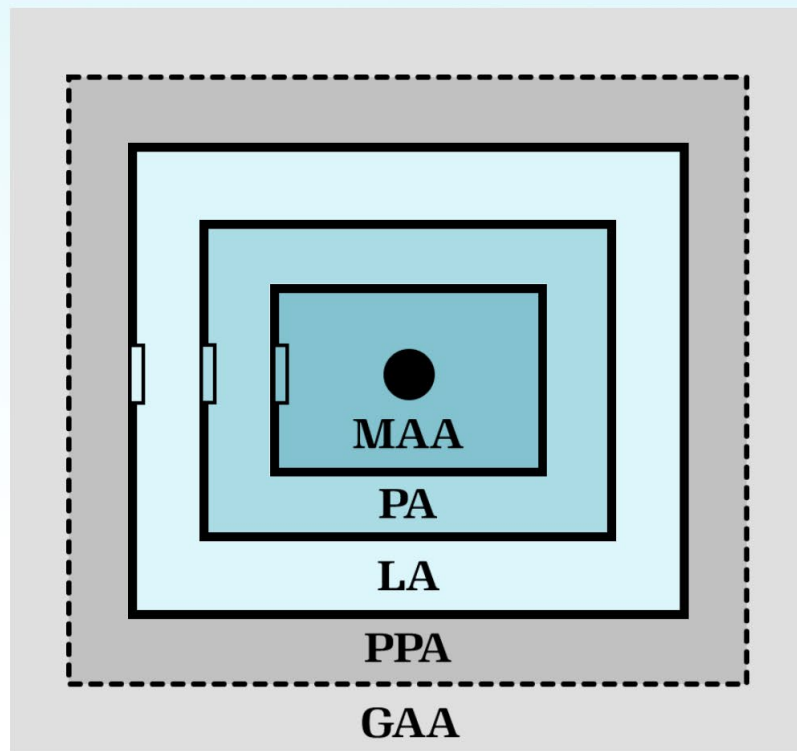
GAA PPA LA PA MAA

Select each level of security to add it to the map

Protected Area (PA)

PAs are security areas defined by physical barriers such as walls or fences and surrounded by intrusion detection and assessment systems, to which access is controlled, used to protect Category II SNM and classified matter and/or to provide a concentric security zone surrounding a material access area.

DOE Security Areas



- GAA
- PPA
- LA
- PA
- MAA

Select each level of security to add it to the map

Material Access Area (MAA)

MAAs are security areas that are approved for the use, processing, and/or storage of a Category I quantity or other quantities of SNM that can credibly roll up to a Category I quantity and which has specifically defined physical barriers, located within a protected area, and is subject to specific access controls.



Next



Which security area has specifically defined physical barriers, is located within a protected area, is subject to specific access controls, and is approved for the use, processing, and or storing of Category 1 SNM?

- Protected area (PA)
- Limited area (LA)
- Material access area (MAA)

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Controlled/Prohibited Articles

[Controlled Articles](#)

[Prohibited Articles](#)

Sites are responsible for developing procedures to deter the introduction of prohibited and controlled articles. These procedures must be documented in a SP approved by the ODFSA.

Select each button above to learn more



Controlled/Prohibited Articles

✓ Controlled Articles

Controlled articles such as portable electronic devices (PED), both government and personally owned, capable of recording information or transmitting data (for example audio, video, radio frequency, infrared, and/or data link electronic equipment) are not permitted in limited areas (LAs), vault type rooms (VTRs), protected areas (PAs), and material access areas (MAAs), without prior written approval.

i

Additional information covering prohibited items may be found under the provisions of 18 USC § 930, 21 USC 841 et. seq, 10 CFR Part 860 and 41 CFR Chapter 102-74 Subpart C.

✓ Prohibited Articles



Controlled/Prohibited Articles

Controlled Articles



Prohibited Articles

Prohibited articles must not be permitted onto DOE property without appropriate authorization. Prohibited articles include but are not limited to:

- Explosives
- Dangerous weapons, as defined by 18 USC § 930
- Instruments or material likely to produce substantial injury to persons or damage to persons or property
- Controlled substances (for example, illegal drugs and associated paraphernalia but not prescription medicine)
- Other items prohibited by law



Nuclear Materials Control and Accountability

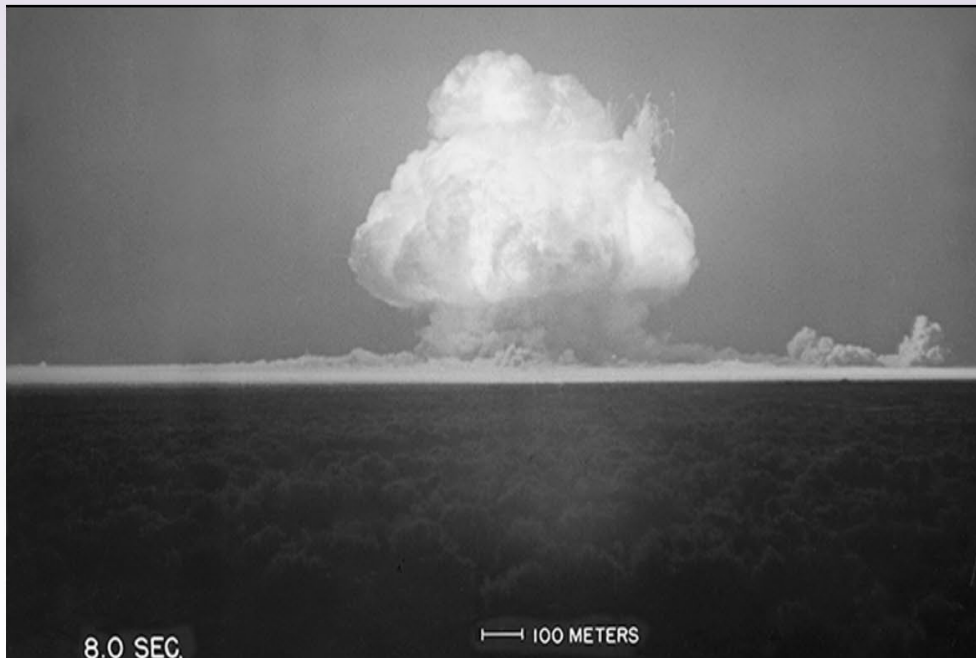
Nuclear Materials Control and Accountability (NMC&A) is another important element of the S&S Program.

The purpose of NMC&A is to control and account for nuclear materials that are important to national security.

Before a facility is allowed to handle nuclear materials, it must first meet certain DOE standards and be approved as a nuclear facility. Each site is required to develop its NMC&A Program procedures according to DOE requirements such as those found in DOE O 474.2, *Nuclear Material Control and Accountability*.



Nuclear Materials Control and Accountability



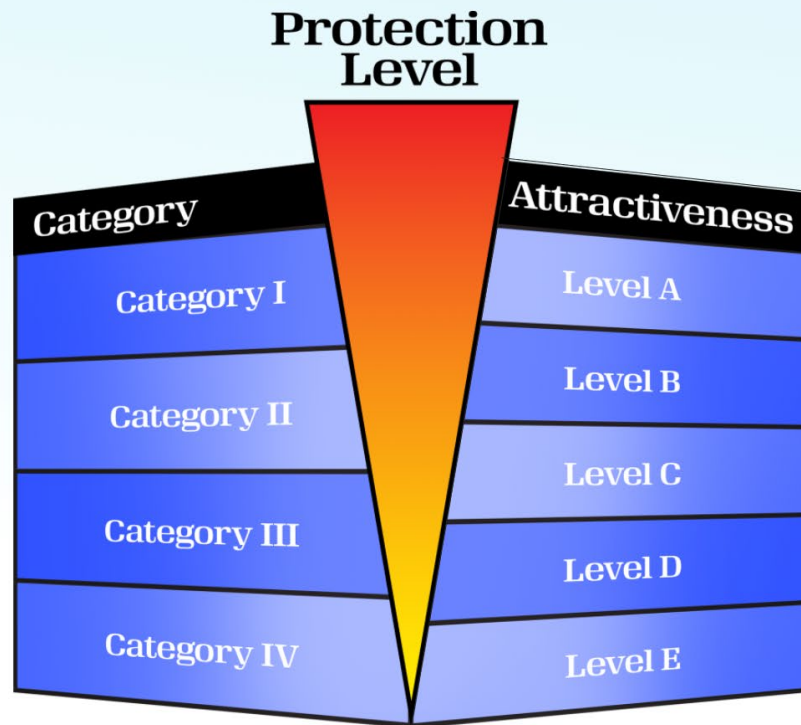
Nuclear materials must be maintained and safeguarded.

SNM is of particular concern to DOE because SNM can be used to produce nuclear weapons. DOE has specifically identified three materials as SNM because they can be used to produce a nuclear device:

- Plutonium
- Uranium-233
- Uranium enriched in the isotope 235



SNM Classifications



SNM is classified into categories such as Category I, Category II, Category III, Category IV, and attractiveness levels A to E.

A primary purpose of the NMC&A program is to minimize the threat of proliferation of nuclear weapons by tracking and controlling materials used in their manufacture.

Protecting SNM, therefore, is a high priority in DOE.

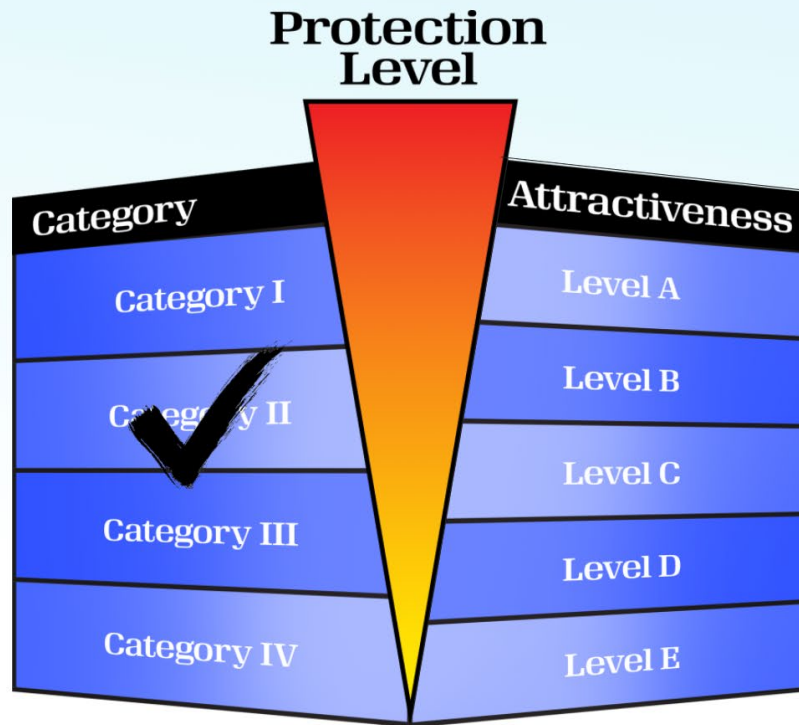
Select Category or Attractiveness to learn more



Back



SNM Classifications



Category

For SNM, the greatest protection is given to Category I materials, with lesser protection required for Categories II and III, and only minimal protection for Category IV materials.

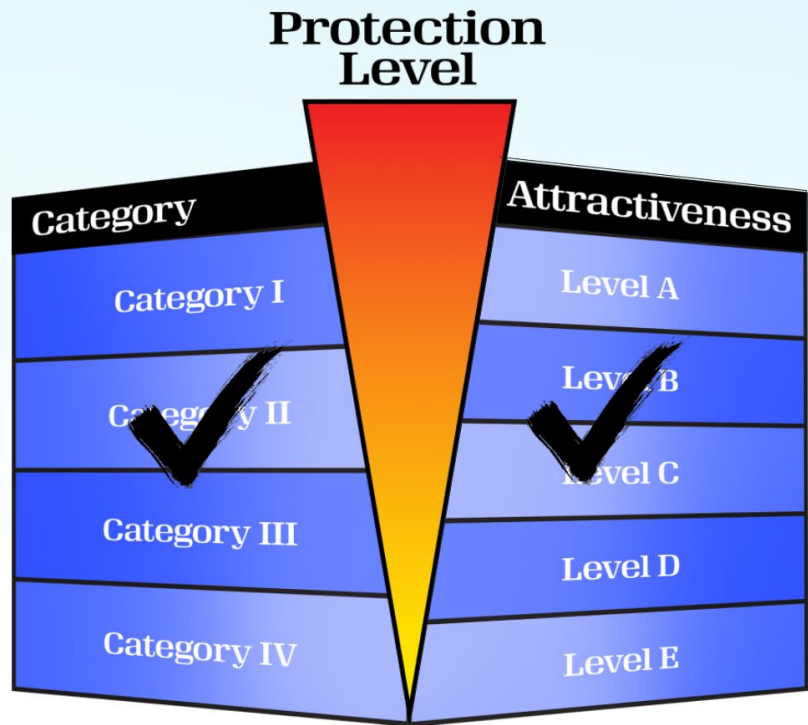
In general, the category is based on the quantity of material present.



Back



SNM Classifications



Attractiveness

Greater protection is given to Attractiveness Level A materials than to Attractiveness Level E materials.

The attractiveness level is determined by the effort required to convert that material into an improvised nuclear device.



Back



Lesson Summary

You should now be familiar with the following material:

1. The purpose of graded protection
2. Types of DOE security areas
3. Security area controlled/prohibited articles
4. Security area privately owned prohibited articles
5. The purpose of the NMC&A Program
6. Materials designated as SNM
7. SNM classifications



An exam based on the lesson objectives follows this slide. You may only review course material prior to beginning the exam.

Select NEXT button to begin the test



Test

You have reached the test section of this course. You will be asked 10 questions.
Answer 80% of them correctly to complete the test.

Select the Start Test button to begin.

Start Test

Test

Question 1/10

Which of the following articles are prohibited in all DOE security areas? Select all that apply.

- Dangerous weapons
- Explosives
- Instruments or material likely to produce substantial injury or damage to persons or property
- Controlled substances, such as illegal drugs and associated paraphernalia
- Prescription medicines

Multiple Response

Choose the correct answers, then select the Submit button.

Submit

Test

Question 2/10

Which security area is approved for the use, processing, and/or storage of a Category I quantity or other quantities of SNM that can credibly roll up to a Category I quantity and which have specifically defined physical barriers, located within a protected area, and is subject to specific access controls?

- Materials Access Area (MAA)
- Property Protected Area (PPA)

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Test

Question 3/10

Which of the following are SNM classifications? Select all that apply.

- Category I
- Category II
- Category V
- Category VI

Multiple Response

Choose the correct answers, then select the Submit button.

Submit

Test

Question 4/10

Which of the following privately owned articles are prohibited in LAs, PAs, or MAAs without prior authorization? Select all that apply.

- Recording equipment (audio, video, optical, or data)
- Portable electronic devices equipment capable of data recording or transmission
- Cellular telephones and radio frequency transmitting equipment
- Computers and associated media
- Alcohol

Multiple Response

Choose the correct answers, then select the Submit button.

Submit

Test

Question 5/10

Which of the following materials are identified as SNM because they can be used to produce a nuclear device? Select all that apply.

- Plutonium
- Uranium-233
- Uranium enriched in isotope 235
- Tritium
- Lithium

Multiple Response

Choose the correct answers, then select the Submit button.

Submit

Test

Question 6/10

Which security area is defined by physical barriers, used for the protection of classified matter and/or Category III quantities of SNM?

- Limited Area (LA)
- Property Protected Area (PPA)

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Test

Question 7/10

Which of the following statements is true about the purpose of Nuclear Material Control & Accountability?

- The purpose of NMC&A is to control and account for nuclear materials that are important to national security.
- The purpose of NMC&A is to pass the accountability of nuclear materials to sources outside of national security.

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Test

Question 8/10

Which security area may be designated by the ODSA to allow access to certain areas with minimum security requirements?

- Protected Area (PA)
- General Access Area (GAA)

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Test

Question 9/10

Which security area is defined by physical barriers such as walls or fences and surrounded by intrusion detection and assessment systems, to which access is controlled, used to protect Category II SNM and classified matter?

- Protected Area (PA)
- Limited Area (LA)

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

Test

Question 10/10

Which security area has an established area that has a defined boundary, has access controls for the protection of DOE property, and protection measures shall be adequate to give reasonable assurance of protection for the assets and Departmental property?

- Property Protection Area (PPA)
- General Access Area (GAA)

Multiple Choice

Choose the correct answer, then select the Submit button.

Submit

PMC-110DE

Facility Security Officer Overview

**You have successfully completed
PMC-110DE, Facility Security Officer Overview.
Please select exit if you wish to exit to end the course or
return if you would like to return to the course for review.**

Return

Exit