



governmentattic.org

"Rummaging in the government's attic"

Description of document:	Department of Energy (DOE) Headquarters Facilities Master Security Plan (HQFMSP) 2013-2024
Requested date:	2025
Note:	No cover/release letter provided
Downloaded from:	See information on following two pages
Accessed:	11-August-2025
Posted date:	18-August-2025

The governmentattic.org web site ("the site") is a First Amendment free speech web site and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

Dept of Energy Headquarters Facilities Master Security Plan (HQFMSP)

CHAPTER 1

https://www.energy.gov/sites/prod/files/2013/12/f6/Chapter_1_Physical_Security.pdf

CHAPTER 2

https://www.energy.gov/sites/prod/files/2013/12/f6/Chapter_2_Limited_Areas_Vault-Type_Rooms_and_Temporary_Limited_Areas.pdf

CHAPTER 3

<https://www.energy.gov/sites/prod/files/2020/07/f76/HQFMSP-Chapter-3-Personnel-Security-June-2020.pdf>

CHAPTER 4

<https://www.energy.gov/ehss/articles/headquarters-facilities-master-security-plan-chapter-4-foci-facility-clearances-and>

CHAPTER 5

https://www.energy.gov/sites/prod/files/2013/12/f6/Chapter_5_Classified_Matter_Protection_and_Control.pdf

CHAPTER 6

<https://www.energy.gov/sites/default/files/2020/07/f76/HQFMSP-Chapter-6-Foreign-Interaction-2020.pdf>

CHAPTER 7

<https://www.energy.gov/sites/prod/files/2020/04/f73/HQFMSP%20Chapter%207%20-%204-1-2020.pdf>

CHAPTER 8

<https://www.energy.gov/sites/prod/files/2020/06/f76/HQFMSP-Chapter-8-Operations-Security-Program-June-2020.pdf>

CHAPTER 9

<https://www.energy.gov/sites/default/files/2024-07/Technical-Surveillance-Countermeasures.pdf>

CHAPTER 10

https://www.energy.gov/sites/prod/files/2013/12/f6/Chapter_10_Security_Awareness_Program.pdf

CHAPTER 11

<https://www.energy.gov/ehss/articles/headquarters-facilities-master-security-plan-chapter-11-incidents-security-concern>

CHAPTER 12

<https://www.energy.gov/sites/prod/files/2020/07/f76/HQFMSP-Chapter-12-Special-Access-Programs.pdf>

CHAPTER 13

https://www.energy.gov/sites/prod/files/2013/12/f6/Chapter_13_Controlled_Unclassified_Information.pdf

CHAPTER 14

<https://www.energy.gov/sites/prod/files/2020/07/f76/HQFMSP-Chapter-14-Cyber-Security.pdf>

CHAPTER 15

<https://www.energy.gov/sites/default/files/2020/07/f76/HQFMSP-Chapter-15-Outprocessing.pdf>

CHAPTER 16

<https://www.energy.gov/sites/prod/files/2020/07/f76/HQFMSP-Chapter-16-Equivalencies-and-Exemptions.pdf>

CHAPTER 17

<https://web.archive.org/web/20240506184344/https://www.energy.gov/sites/default/files/2024-04/Headquarters-Security-Officer-Program-Duties.pdf>

Acronyms List

https://www.energy.gov/sites/prod/files/2013/12/f6/Acronyms_List.pdf

Chapter 1

Physical Security

This chapter describes the security procedures adopted by DOE HQ to implement the requirements of the following DOE directives:

- Title 10 Code of Federal Regulations (CFR) Part 860.4
- Title 41 CFR Parts 101-19.3 and 102.74, Subpart C
- Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*
- DOE Order 473.3, *Protection Program Operations*
- DOE Order 471.6, *Information Security*
- DOE Order 580.1, Change 1, *DOE Personal Property Management Program*

The objective of these directives is to protect DOE sensitive and classified information, facilities, property, and employees from threats posed by intelligence collectors, terrorists, violent activists, criminals, psychotics, and disgruntled employees.

- Section 101 describes the procedures for acquiring the types of security badges used to control access to HQ facilities.
- Section 102 describes the procedures for requesting and obtaining a security credential (security badge) in accordance with the procedures required by HSPD-12. This section also covers Personal Identity Verification (PIV) procedures, which must be completed prior to receiving an HSPD-12 badge.
- Section 103 describes the procedures for preventing the introduction of Prohibited Articles into all HQ facilities.
- Section 104 discusses the procedures used to conduct inspections of personnel entering and exiting HQ facilities.
- Section 105 describes the general access control systems in place at HQ and procedures for gaining access to both public and secure areas within HQ.
- Section 106 discusses Security Hours, which identifies the days and times when certain physical security measures are implemented at HQ.

- Section 107 describes the controls established for US citizens who visit HQ. See Sections 601 and 602 for the controls established for visitors who are foreign nationals.
- Section 108 describes the controls adopted for the authorized removal of accountable government property and personally owned property from HQ facilities.
- Section 109 describes the lock and key control program in place at HQ.

Section 101

Headquarters Security Badges

The primary badge used to allow daily access to HQ facilities is the DOE security badge prescribed by DOE Order 473.3, *Protection Program Operations*. This badge is the common identification badge prescribed by HSPD-12.

NOTE: The common identification badge is known by several different names. DOE Order 473.3, Protection Program Operations, identifies it as the “DOE Security Badge.” Various DOE forms refer to it as the “HSPD-12 Credential,” and other official documents refer to it as a “PIV Credential.” Over time and by common usage, HQ personnel have adopted the term “HSPD-12 badge” to distinguish it from other types of security badges issued at DOE HQ. To more clearly communicate with HQ personnel, the term “HSPD-12 badge” will be used throughout the HQFMSP.

This section does not address the acquisition of HSPD-12 badges, which are discussed in Section 102 of the HQFMSP. This section discusses more general HQ policies and procedures for acquiring security badges, including those issued to:

- Those awaiting receipt of an HSPD-12 badge
- Those requiring access to an HQ facility but who do not meet the criteria for an HSPD-12 badge
- Those who have forgotten their regular badge
- Those awaiting replacement of a lost badge
- DOE field personnel visiting HQ
- Visitors who are U.S. citizens
- Visitors who are foreign nationals
- Those accessing Child Development Centers (CDCs)
- Commuters transiting an HQ facility.

The issuance of security badges at HQ is a collaborative effort between the Office of Physical Protection (HS-91) and the Office of HQ Personnel Security Operations (HS-93). All documents related to requests for security badges must first be submitted to HS-93 and that office, in turn, will forward the documentation to HS-91 for production and issuance of the badge.

HQ Implementation Procedures

General:

Security badges in use at HQ must be displayed above the waist and with the front (picture) side facing outward.

Security badges should be removed from view upon exiting an HQ facility.

The badge is government issued and the recipient is responsible to safeguard it and prevent its misuse, which includes allowing someone else to use it to enter the facility.

Security badges bear a photograph of the holder. HQ issues both HSPD-12 badges and Local Site-Specific Only (LSSO) badges out of the Forrestal or Germantown badge offices.

Personnel receiving an HSPD-12 or LSSO security badge for the first time must complete an Initial Security Briefing. Whenever an employee is granted a security clearance, that employee will be issued a badge reflecting the appropriate clearance level. Those receiving a security badge reflecting a security clearance must complete a Comprehensive Security Briefing (see Chapter 10, Security Awareness Program) and Standard Form (SF) 312, *Classified Information Nondisclosure Agreement*.

HSPD-12 Badges:

The HSPD-12 badge is accepted for access to all HQ facilities and can be encoded to operate HQ access control and intrusion detection systems. HSPD-12 badges bear expiration dates of 5 years from their issuance. Although contractor HSPD-12 badges have expiration dates of 5 years from their issuance, they will deny access to an HQ facility once the contract is fulfilled.

See Section 102, HSPD-12 and PIV Process, of the HQFMSP for complete details on the process for requesting HSPD-12 badges.

LSSO Badges:

LSSO badges are issued to DOE employees and contractors who are awaiting their HSPD-12 badge, lost their HSPD-12 badge, or fail to meet qualifications for issuance of an HSPD-12 badge (detailed to work at an HQ facility or other specialized need). These badges may be issued by the Forrestal or Germantown badge offices, by building receptionists, or by specially designated officials within each HQ facility. Both badge offices are open from 8 am to 4 pm Monday through Friday, excluding Federal holidays. Protective force personnel provide receptionist services at the main entrances to the Forrestal and Germantown facilities at all times. At other facilities, receptionists or designated officials are available to issue temporary security badges during normal working hours. Some, but not all, temporary security badges can be encoded to operate HQ access control systems.

The following types of LSSO badges are available:

1. Non-PIV Temporary Badge (Green) – This badge is issued to those awaiting issuance of an HSPD-12 badge and those requiring routine access to an HQ facility for six months or less (such as interns, temporary workers, and detailees). This badge can be encoded to operate automated access control points. The exact access points are determined by the holder's specific circumstances. All LSSO badges can be issued by the Forrestal and Germantown badge offices.

The most common use for the Green badge is to permit new employees awaiting issuance of an HSPD-12 badge to enter HQ facilities. For these employees, the Green badge is initially encoded to permit automated entry to HQ facilities for a period of 30 days. If the new employee completes the process for acquiring an HSPD-12 badge within the required 30-day time period, encoding of the Green badge continues up to six months total. If the new employee fails to complete the HSPD-12 process within the allotted 30-day time period, the encoding ends and the employee must sign into the HQ facility each day until the HSPD-12 processing is complete. See Section 102 of the HQFMSP for a complete discussion of HSPD-12 security badge processing.

A Green badge can also be issued to an HQ employee who has lost or damaged his/her HSPD-12 badge. Such Green badges are encoded to operate HQ access control systems in the same manner as the employee's HSPD-12 badge. When the employee receives his/her replacement HSPD-12 badge, the Green badge must be returned to the servicing badge office.

2. OGA/IPA Badge – Intergovernmental Personnel Act (IPA) personnel or Other Government Agency (OGA) detailees who may be assigned to HQ for a period of more than 1 year will have their badge encoded to the length of their detail up to 2 years. If the badge cannot be encoded the individual will be issued an HQ LSSO badge with an expiration date consistent with the duration of the assignment, not to exceed 2 years.

All IPAs and OGA detailees require the submission of a DOE Form (F) 473.2, *Security Badge Request*, from the HQ Security Officer (HSO) of the sponsoring element. DOE F 473.2 is the official request to process the badge application. General instructions for completing this form are presented in Attachment 101-1 at the end of this section.

All DOE Fs 473.2 are submitted to HS-93 for processing. In addition, other documents may be required to be attached to that form. These documents are:

- Requests for badges for IPA employees must be accompanied by a memorandum from the sponsoring Head of Element or the employee's servicing HSO or a copy of the IPA agreement specifying the dates of the assignments.
- Requests for badges for OGA detailees must be accompanied by a memorandum from the sponsoring Head of Element or the detailee's servicing HSO or a copy of the OGA agreement specifying the dates of the assignments.
- Requests for badges for other special cases, such as interns, temporary workers, and detailees from other DOE sites, must be accompanied by a memorandum from the sponsoring Head of Element or the employee's servicing HSO specifying the reason for requesting the DOE badge and the dates it is needed.

NOTE: If the DOE F 473.2 is submitted in association with a security clearance application, see Section 301, Acquiring New Q or L Security Clearances.

3. Forrestal Transit Badge – Non-DOE employees who are members of a van/carpool and park in the garage at the Forrestal building are eligible for a Forrestal Transit Badge. The badge allows the holder access (Monday through Friday only) to the garage through either the 12th Street entrance or the 9th Street entrance and entry/exit through the main lobby turnstiles. Badges expire according to the date authorized by the parking garage.

To acquire a Forrestal Transit Badge, the DOE employee sponsoring the individual who requires the badge must obtain a “DOE Transit Badge Form” from the Forrestal Badge Office or the Parking Office in Room GE-140, complete it, and hand-carry it to the Parking Office to be approved. The approved form must then be taken to the Forrestal Badge Office, where it is checked for the proper signatures. There must be two signatures on the form, the sponsor’s and an authorized parking official. When approval is obtained, badge office personnel contacts the sponsor and requests personal escort of the individual to the Forrestal Badge Office to present a government issued picture ID (e.g., driver’s license), have his/her photo taken, and receive the transit badge.

HQ employees who are foreign nationals are not authorized to sponsor a Forrestal Transit Badge.

Foreign nationals are issued transit badges only if they are in the Foreign Access Central Tracking System (FACTS).

4. Germantown Transit Badge – Non-DOE employees who transport DOE employees to and from the Germantown Facility are eligible for a Germantown Transit Badge. The badge allows the holder to enter and/or depart the facility immediately after bringing in or picking up the DOE employee. If the sponsor of the badge is a Federal employee, the badges are issued for 2 years and must then be renewed. If the sponsor of the badge is a contractor employee, the badges are issued for 1 year. These badges are not encoded to operate HQ access control systems.

To acquire a Germantown Transit Badge, the DOE employee sponsoring the individual who requires the badge must obtain a “DOE Transit Badge Form” from the Germantown Badge Office, complete it, and return it to the Badge Office. The Badge Office forwards it to the Germantown Facility Operations Manager for approval. After approval is obtained, a badge office staff member contacts the sponsor and requests personal escort of the individual to the Germantown Badge Office to present a government-issued picture ID (e.g., driver’s license), have his/her photo taken, and receive the transit badge.

HQ employees who are foreign nationals are not authorized to sponsor a Germantown Transit Badge.

Foreign nationals are not issued transit badges.

5. Forrestal and Germantown CDC Badges – Members of the public with a child enrolled at the Forrestal or Germantown CDC are authorized to request a “CDC ONLY” badge to deliver and pick up their child. These badges must be renewed annually. They are encoded to operate access control systems at either the Germantown or Forrestal CDC but not other HQ facilities. Procedures for the issuance of these badges are unique to the CDCs and HS-91. The CDC will inform parents of the actions required. Foreign nationals at Germantown must be in FACTS.

Forgotten DOE Security Badges:

Any DOE Federal or contractor permanent party employee who has been issued an HSPD-12 or LSSO security badge and does not have it in his/her possession must process through the receptionist desk in the Forrestal, 955 L’Enfant Plaza, or Germantown main lobby. The employee will be issued a temporary Passage Point paper badge and must then submit to inspection prior to entry.

Replacement of DOE Security Badges:

HSPD-12 and LSSO security badges may need to be replaced or reissued because of wear or damage, or if the individual’s physical characteristics have changed, such as the growth or removal of a beard or long hair that is cut short. Protective force officers may also direct individuals to replace their badges when they detect wear, damage, or changes in physical appearance. When the need arises, the individual should contact the Forrestal or Germantown badge office for assistance in obtaining a new badge.

Reporting Lost or Stolen DOE Security Badges:

Individuals whose HSPD-12 or LSSO badge has been lost, misplaced, or stolen must immediately notify their servicing badge office. The badge office requires the badge holder to complete an HQ F 473.1, *Lost or Stolen Badge Replacement*, which can be found here: <http://energy.gov/cio/downloads/doe-hq-f-4731-fillable-pdf>. Attachment 101-2 at the end of this section provides instructions for completing this form. The HQ F 473.1 must be completed by the individual, signed by the individual's supervisor, and submitted electronically to the badge office. Replacement of lost or missing badges normally takes at least 5 working days.

Termination of DOE Security Badges:

HSPD-12 and LSSO security badges are automatically terminated on the expiration date reflected on the badge. If the badge is still needed, the badge is renewed with a new expiration date.

A badge must be returned to DOE control for termination or revision whenever:

- The badge holder terminates employment.
- The badge holder no longer requires access to an HQ facility.

- A contractor employee becomes the employee of a different contractor.
- The badge holder is on a leave of absence, extended leave, or in another leave status for more than 90 days that does not involve official U.S. government business.
- The requirement for access is negated for any other reason.

The return of DOE security badges is also covered in Chapter 15, Outprocessing, of the HQFMSP. Chapter 15 contains detailed instructions on the collection and return of permanent security badges, termination of security clearances, etc.

Badge Office Locations and Operating Hours

There are two badge offices at HQ. The Forrestal Badge Office is located in Room 1E-090 and the Germantown Badge Office is located in Room B-106. Both badge offices are open from 8 am to 4 pm, Monday through Friday, excluding Federal holidays.

Points of Contact

For the names and contact information for those occupying the HS-91 positions identified in this chapter, call (202) 586-8075 or (301) 903-0145.

For the names and contact information for those occupying the HS-93 positions identified in this chapter, call (301) 903-5485 or (301) 903-1163.

Forms/Samples/Graphics

DOE F 473.2, *Security Badge Request* (go to <http://energy.gov/cio/downloads/security-badge-request> for a copy of this form)

General Instructions for Completing DOE F 473.2, *Security Badge Request* (see Attachment 101-1)

HQ F 473.1, *Lost or Stolen Badge Replacement* (go to <http://energy.gov/cio/downloads/doe-hq-f-4731-fillable-pdf> for a copy of this form)

General Instructions for Completing HQ F 473.1, *Lost or Stolen Badge Replacement* (see Attachment 101-2)

ATTACHMENT 101-1

General Instructions for Completing DOE F 473.2, *Security Badge Request*

Following are the instructions for completing the DOE F 473.2. The form can be found at <http://energy.gov/cio/downloads/security-badge-request>.

- a. Block A, From: Enter the name and signature of the Federal employee who is sponsoring the applicant for an HQ security badge. By signing this form, the sponsor certifies that the applicant needs to access an HQ facility for a period of at least six months. Do not use this form if the applicant needs access less than six months. The applicant can still be issued an LSSO badge to allow unescorted entry to an HQ facility as the need arises.
- b. Block B, Title: Enter the title and two-letter routing symbol (SC, NA, HS, etc.) of the Federal employee sponsoring the applicant for an HQ security badge.
- c. Block C, Telephone Number: Enter the office telephone number of the Federal employee sponsoring the applicant for an HQ security badge.
- d. Block D, Name of Applicant: Enter the last, first, and middle name of the applicant. *It is important to list the applicant's full, legal name and not nicknames, initials, or any other name.* The badge may be encoded to operate HQ access control systems. However, these systems do not operate properly unless the applicant's name is clearly recognizable and retrievable by the system.
- e. Block E, Social Security Number: Enter the applicant's nine digit Social Security Number. This number is needed to positively identify the applicant and distinguish him/her from others with the same name.
- f. Block F, Applicant's Employers Name: If a contractor, enter the name of the employing company. If an IPA, OGA detailee, or consultant, enter N/A.
- g. Block G, Employer Address: If a contractor, enter the address of the employing company. If an IPA, OGA detailee, or consultant, enter N/A.
- h. Block H, Employer Telephone Number: If a contractor, enter the telephone number for the employing company. If an IPA, OGA detailee, or consultant, enter N/A.
- i. Block I, Prime Contractor Name: List the name of the prime contractor responsible for the contract the applicant is supporting. If an IPA, OGA detailee, or consultant, enter N/A.
- j. Block J, Date: Enter the date the request is being made.
- k. Block K, U.S. Citizen: Check the appropriate block. Note that applicants who are not US citizens must be processed as foreign national assignees in accordance with Section

602, Unclassified Foreign Visits and Assignments, of the HQFMSP. There are extensive security requirements for foreign national assignees that must be satisfied before a security badge is issued.

- l. Block L, Request Applicant be Issued: Check the appropriate blocks.
- m. Block M, Badge At: Check the appropriate block. If a contractor, also enter the contract number and contract expiration date. Use of the full term contract ending date on HQ contractor/ subcontractor badges is permitted. Verification of this ending date is by the Contracting Officer's Representative (COR) with his/her signature in Section N of the form. If there is no indication of an ending date, the badge is issued with the expiration date as shown in the Procurement and Assistance Data System (PADS).

For IPAs, enter the expiration date of the IPA Agreement and attach a copy of the IPA Agreement page that contains this date. For OGAs enter the expiration date of the OGA assignment and attach a memorandum.

- n. Block N, Employer Certification: An official of the employing contractor must print and sign their name certifying that the applicant requires access to an HQ facility for a period of at least six months; that pre-employment checks were conducted in accordance with company policy; that the checks were favorable; and the individual was found to be suitable for employment. The contractor official then forwards the DOE F 473.2 to the COR.

The COR reviews the information on the form to ensure it is completed properly and that specific contract-related information, such as the contract number and contract expiration date, is accurate. After concluding this review, the COR completes the "COR Concurrence" portion of Section N and forwards the DOE F 473.2 to the cognizant HSO.

After verifying that the individual requires access, the HSO, or a Federal employee identified in writing to HS-91, signs the "Security Official Concurrence" portion of Section N and forwards the DOE F 473.2 to HS-93 for action.

ATTACHMENT 101-2

General Instructions for Completing HQ F 473.1, *Lost or Stolen Badge Replacement*

Obtain a copy of HQ F 473.1 at <http://energy.gov/cio/downloads/doe-hq-f-4731-fillable-pdf> and complete it as follows:

1. Name (Last, First, Middle) – Enter your name exactly as it appears on your badge. Do not use nicknames, abbreviations, or names you commonly use.
2. Telephone Number – Enter your work telephone number, including area code.
3. Today's Date – Enter the date you are completing the request.
4. Organization – Name and routing symbol of HQ Program Element.
5. Federal Manager or Supervisor's Name – If you are a Federal employee, enter your supervisor's name. If you are a contractor, enter the name of the Federal employee directing your work.
6. Type of Badge – If the badge to be replaced is an HSPD-12 credential, check HSPD-12; otherwise, check Local.
7. Reason for the Request – Check whether the badge was lost or stolen.
8. Explanation – Provide details about losing the badge and efforts to recover it. If the badge was stolen and a police report was filed, include the name of the law enforcement agency that took the report. Include information on where the badge may have been lost, when it was last seen, where it may have been lost, what steps have been taken to recover the badge, etc. Simply saying that you lost your badge and need a new one is unacceptable.
9. Employee's signature – Digitally sign the form, save the form, and e-mail it to the person listed in block 4.
10. Supervisor's signature – The supervisor should digitally sign the form, save the form, and e-mail it to the badge office (BadgeOffice@hq.doe.gov).

Once the badge office receives the completed form it is reviewed for completeness. The individual receives an e-mail from a member of the badge office staff when the replacement badge is ready for issue. In the meantime, the individual must obtain a temporary badge from the receptionist each day to gain access to the building.

This page intentionally left blank.

Section 102

HSPD-12 Badges and the PIV Process

On August 27, 2004, President George W. Bush issued HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*. HSPD-12 states that it is the “policy of the United States to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal government to its employees and contractors (including contractor employees).” In essence, HSPD-12 requires that all Executive branch agencies, including DOE, issue their Federal and contractor employees a common, secure, and reliable identification badge that can be used to grant access to Federally-controlled facilities. The identification badge also permits employees to access Federally-controlled information systems.

NOTE: The common identification badge is known by several different names. DOE Manual 473.3, Protection Program Operations, Attachment 2, identifies it as the “DOE Security Badge.” Various DOE forms refer to it as the “HSPD-12 Credential,” and other official documents refer to it as a “PIV Credential.” Over time and by common usage, HQ personnel have adopted the term “HSPD-12 badge” to distinguish it from other types of security badges issued at DOE HQ. To more clearly communicate with HQ personnel, the term “HSPD-12 badge” will be used throughout the HQFMSP.

In order to qualify for an HSPD-12 badge, the applicant must undergo a process known as PIV, which involves both verification of the applicant’s identity and a form of background investigation to ensure that the applicant is eligible for an HSPD-12 badge. The applicant’s identity is verified by submission of two official identification documents.¹ If the applicant does not provide two acceptable identification documents, an HSPD-12 badge cannot be issued.

HQ Implementation Procedures

Requesting an HSPD-12 Badge:

Processing individuals for an HSPD-12 badge involves the following steps:

1. Sponsorship – Every new HQ Federal or contractor employee requiring access to an HQ facility for six consecutive months or more must have an HSPD-12 badge. The HQ

¹ Acceptable identification documents consist of two categories. Primary forms of identification include an unexpired U.S. passport, driver’s license, state-issued ID card with photograph, military identification, military dependent identification, or Department of Defense Common Access Card. Secondary forms of identification can be an additional primary form of identification or a secondary form of identification, such as an unexpired U.S. Social Security card; birth certificate (original or certified copy); identification card issued by a Federal, state, or local government agency; school identification card with photograph; voter’s registration card; certificate of U.S. citizenship; Certificate of Naturalization; or other documents listed at <http://fedidcard.gov/viewdoc.aspx?id=109>.

element where the employee will work is responsible for sponsoring the employee for the HSPD-12 badge. The sponsor must be a Federal employee. For newly hired Federal employees, the sponsor is designated by the office that provides Human Resource (HR) services to the HQ element. In most cases, this is the Office of Human Capital (HC). For newly hired contractor employees, the sponsor is a COR within the HQ element or a Federal employee delegated the authority to act on behalf of the COR.

The newly hired employee is provided two forms to complete:

- DOE F 206.4, *Information Sheet for Sponsorship of HSPD-12 Credential*, and
- Optional Form (OF) 306, *Declaration for Federal Employment*. (Although this form appears to be for Federal employees, contractor employees must complete questions 1, 2, 8-13, 16, and 17a.)

DOE F 206.4 and OF 306 are provided to the employee/applicant either by the HQ element's HR sponsor or by the HSO. The applicant completes and returns both forms as instructed by the HSO or HR sponsor. The HSO or an elemental representative must supplement the information provided by the applicant on the DOE F 206.4, providing position-specific information in boxes 10 through 17.

The completed DOE F 206.4 (or a copy) is sent by the element's HSO to the HQ element-designated USAccess sponsor, who uses it to enter data about the applicant into USAccess, a database maintained by the General Services Administration.

2. Enrollment – After the sponsor enters the employee's information into USAccess, that system automatically contacts the applicant via e-mail with instructions for making an appointment to enroll at a USAccess Credentialing Center. More than 300 USAccess Credentialing Centers across the U.S. are available for enrollment and other HSPD-12 badge-related actions. The Forrestal and Germantown badge offices maintain credentialing centers, conveniently located for most HQ employees and contractors.

The applicant must report to the USAccess Credentialing Center of his/her choice at the scheduled time. The applicant must present two identity verification documents: one primary document, and one secondary document (which can be another primary document – see footnote on previous page).

At the USAccess Credentialing Center, operators review and record the applicant's two identification documents, and take the applicant's fingerprints and a photograph of the applicant.

3. Submission of HSPD-12 Badge Documentation – After the applicant is sponsored in USAccess, the HR sponsor or HSO forwards a copy of the form, either by fax or via e-mail encrypted to protect Personally Identifiable Information (PII), to the PIV team (PIV@hq.doe.gov or 301-903-0265) within HS-93. The OF-306 should be transmitted with the applicant's resume (required for Federal applicants only). The original OF-306 for Federal employees is maintained in the Official Personnel Folder (OPF); originals

need not be mailed. All documents should be handled in accordance with DOE directives on Official Use Only (OUO) documents and the Privacy Act.

For contractors seeking a “Building Access Only” (BAO) HSPD-12 badge, a DOE F 473.2, *Security Badge Request*, must be prepared by the contractor’s Facility Security Officer or servicing HSO and delivered to HS-93 in person or via the PIV mailbox (PIV@hq.doe.gov).

Federal and contractor employees applying for a security clearance and the associated HSPD-12 badge must provide additional documents (see Section 301, Acquiring New Security Clearances).

4. HQ PIV Team Review – The HQ PIV Team reviews the applicant’s documentation and USAccess records and searches for proof of a prior, favorably adjudicated background investigation. If the applicant possesses a documented background investigation, such as one conducted for a current or prior security clearance, the HSPD-12 badge can be approved for issuance without further documentation.

NOTE: The HQ PIV Team is authorized to refrain from taking action on HSPD-12 badge requests for persons currently awaiting a hearing or trial; convicted of a crime punishable by imprisonment of 6 months or longer; or awaiting or serving a form of pre-prosecution probation, suspended or deferred sentencing, probation, or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of 6 months or longer. In such cases, the applicant may be denied physical access to DOE facilities as a visitor, depending on the severity of the related charges. The Office of HQ Security Operations (HS-90) makes such access decisions on a case-by-case basis.

If the PIV Team identifies no prior background investigation for the applicant, a PIV Team analyst requests the sponsoring element’s HSO or HR sponsor to initiate the applicant into the Electronic Questionnaires for Investigations Processing (e-QIP) system to complete an SF-85, *Questionnaire for Non-Sensitive Positions* (or the SF-86, *Questionnaire for Sensitive Positions* for applicants seeking a security clearance). The e-QIP initiator is responsible for sending the applicant instructions on how to access the e-QIP system.

5. e-QIP Processing – See Section 304, e-QIP, in the HQFMSP for instructions on how to complete e-QIP processing.
6. Approval and Activation of HSPD-12 Badge – When the applicant completes the appropriate form in e-QIP, the Office of Personnel Management (OPM) conducts a background investigation and sends a report to DOE. For Federal new-hires who do not require a security clearance, the servicing HR office adjudicates the report for suitability. HS-93 adjudicates the report for Federal and contractor security clearance candidates to determine whether the applicant qualifies for a clearance and an HSPD-12 badge. HS-93 also adjudicates the reports for uncleared contractors to determine whether they

qualify for an HSPD-12 badge. The adjudication decision is recorded in USAccess and, if approved, an HSPD-12 badge is generated. The badge is sent to the Credentialing Center designated by the sponsor. An e-mail is sent to notify the applicant of the delivery.

The HSPD-12 badge must be activated at a USAccess Credentialing Center. Since part of the activation process prepares the badge for use in the unique HQ access control system, HSPD-12 badges do not operate properly unless registered at an HQ Credentialing Center, either at the Forrestal or Germantown badge office.

HSPD-12 *Badge* Renewal Process:

HSPD-12 badges automatically expire after 5 years. The expiration date is printed at the approximate midpoint along the right side of the face of the badge.

The renewal process begins without any action on the part of the individual badge holder. When the renewal process begins, the individual is sent a notification e-mail from USAccess, purely for information purposes. See the Certificate Renewal section, below, for information on e-mails generated by USAccess that advise individuals to update the *certificates* associated with their HSPD-12 badges.

In most cases, the individual receives a second e-mail from USAccess within two weeks informing him/her that the new badge has arrived and is available at either the Forrestal or Germantown badge office. If the individual does not receive this second e-mail within two weeks, he/she should ask the personnel in the element assigned to handle HSPD-12 badge renewals to check on the renewal status of the badge.

This second e-mail contains instructions on how to schedule an appointment to activate and pick up the new badge. During the appointment, the individual must present the special password included in the second e-mail, along with the expiring HSPD-12 badge. If an individual experiences difficulty in scheduling an appointment, he/she should report to the badge office for assistance.

HSPD-12 *Certificate* Renewal Process:

Although HSPD-12 badges are valid for 5 years after enrollment, the “certificates” stored on the chip expire after only 3 years. Certificates can be renewed (or “rekeyed”) at a USAccess Credentialing Center or at a desktop workstation enabled with a card reader and ActiveIdentity middleware. Instructions for certificate rekey are located on Powerpedia. Beginning 6 months before the expiration date, cardholders are notified of impending certificate expiration. E-mail messages are sent by USAccess, and “pop-up” messages appear to employees who use their cards for logical (computer) access at their desktops. If the certificates are not renewed at least 1 day before the expiration date, the entire card is terminated. The cardholder’s sponsor must request a replacement card, and the employee must schedule an appointment to re-enroll before a replacement HSPD-12 badge is issued.

Other Important Information:

- Individuals denied an HSPD-12 badge or have had an HSPD-12 badge revoked are ineligible for physical access to DOE property or access to information systems. The process for appealing denial of a PIV badge is described in DOE Order 206.2, *Identity, Credential and Access Management (ICAM)*.
- The applicant must record his/her name on DOE F 206.4 and OF 306 exactly as it appears on the two identity verification documents they present to the Credentialing Center. Nicknames, aliases, abbreviations, etc. are not permitted. The HSPD-12 badge is printed with the applicant's full first name, middle initial, and last name. If the person has no middle name, uses an initial only, is a senior, junior, etc., the name on the badge follows the conventions established by Federal Information Processing Standards (FIPS) 201, *PIV of Federal Employees and Contractors*. Requests for special name treatment cannot be granted by DOE and will not be processed by USAccess.
- The PIV investigation and HSPD-12 badge issuance processes may take several months, so HS-91 will issue a temporary security badge to new HQ employees and contractors. This badge is known as a LSSO badge. The LSSO badge is encoded to operate common HQ physical access control systems; however, even though the expiration date on the LSSO badge may indicate that it is good for 6 months, it will initially only operate physical control turnstiles for a 30-day period. During that time, the new employee or contractor is expected to enroll in USAccess and complete all required badge and security clearance paperwork. If the paperwork is completed within the first 30 days, physical access is extended up to 6 months, consistent with the date on the badge. If the employee or contractor fails to complete the required paperwork within 30 days, the LSSO badge is confiscated, and the employee is required to sign in as a "visitor" each day. LSSO badges can operate in the card readers or the desktops that provide access to DOE information technology systems.
- If the fingerprints taken during enrollment in USAccess are deemed "unclassifiable" (i.e., unreadable) by the Federal Bureau of Investigation (FBI), a Personnel Security employee contacts the applicant and the USAccess sponsor, sending a courtesy copy to the HSO, with instructions for "unlocking" the applicant's record in USAccess and scheduling an appointment to re-enroll. All fingers must be reprinted, even if the USAccess system considers some of the fingerprints adequate. The HSO is responsible for ensuring that the applicant re-enrolls and for notifying Personnel Security when re-enrollment is complete.
- Losing an HSPD-12 badge is a serious matter. Employees who lose their HSPD-12 badge must report the loss immediately to the servicing badge office, complete a Lost/Stolen Badge Report, have it signed by the supervisor, and return it to the badge office. The badge office waits 5 days before requesting a reenrollment to provide the employee an opportunity to locate the lost card.

- Element HSOs can check on the status of an HSPD-12 badge application by accessing the USAccess Reports Portal, which contains selected information on each applicant. HSOs may contact the HSO Program Manager for more information.
- DOE cannot process OGA employees and their contractors for an HSPD-12 badge. These employees must obtain an HSPD-12 badge from their employing agency. Exceptions to this rule can extend to employees from the Legislative or Judicial branches of the Federal government.
- Because the HSPD-12 initiative continues to evolve rapidly, Powerpedia (http://powerpedia.energy.gov/wiki/Welcome_to_Powerpedia) is highly recommended as a source that is frequently updated with new information. From the Powerpedia main page, search for “HSPD-12.”

Points of Contact

For the names and contact information for those occupying the positions identified in this section or more information about HSPD-12 badges, call (301) 903-4175 or (301) 903-1163.

Forms/Samples/Graphics

DOE F 206.4, *Information Sheet for Sponsorship of HSPD–12 Credential* (go to <http://energy.gov/cio/downloads/information-sheet-sponsorship-hspd-12-credential> for a copy of this form)

DOE F 473.2, *Security Badge Request* (go to <http://energy.gov/cio/downloads/security-badge-request> for a copy of this form)

OF 306, *Declaration for Federal Employment* (go to http://www.opm.gov/Forms/pdf_fill/of0306.pdf for a copy of this form)

Helpful Websites

<http://www.fedidcard.gov/viewdoc.aspx?id=109>

<http://www.hss.energy.gov/HSPD12/index.html>

http://powerpedia.energy.gov/wiki/Welcome_to_Powerpedia

Section 103

Prohibited Articles

All HQ facilities occupy space owned or leased by the General Services Administration (GSA); therefore, HQ is required to comply with the standard rules and regulations for all Federal properties administered by GSA. Rules pertaining to the introduction of firearms and dangerous materials onto Federal properties are described in 10 CFR 860.4 and the rules pertaining to alcohol and controlled substances are described in 41 CFR 102-74, Subpart C.

Prohibited Articles are generally not permitted in any HQ facility; however, there are a few exceptions to this general rule as described in the subsections, below.

HQ Implementation Procedures

Prohibited Articles:

Prohibited articles are:

- Dangerous weapons and explosives (including firearms and ammunition)
- 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)
- Alcoholic beverages
- Controlled substances (e.g., illegal drugs or paraphernalia, but not prescription medication)
- Dogs and other animals (identified in 41 CFR 101-20.311), except service dogs
- Other items prohibited by law.

Firearms Exception:

Lawfully armed DOE, Federal, civilian, or military police or investigative officers may remain armed while on DOE property if on official business. When such individuals arrive at an HQ facility, they must present their badges and/or credentials to the protective force supervisor stationed at the facility. They must declare that they are armed and on official business, and provide the name of the office/individual with which/whom they have business. The protective force supervisor must verify the provided information by referring to prior written notice or by speaking directly with the individual hosting the visit.

Alcoholic Beverage Exception:

Alcoholic beverages may be brought into an HQ facility with the approval of the Office of Management and Administration within the Office of Administration (MA-40). A sample memorandum for requesting authorization to bring alcoholic beverages on to HQ property is provided in Attachment 103-1. Once approval is granted, a copy of the approved memorandum must be delivered to HS-91 for information and dissemination.

Other Exceptions:

Other exceptions to the policy on Prohibited Articles may be requested via memorandum to the Director, HS-91. The memorandum should fully describe:

- The prohibited article(s)
- The reason for introduction
- How long the article(s) will be on HQ property
- Who will have custody of the article(s)
- How long the article(s) will be stored (if applicable)
- What HQ facility the article(s) will be introduced into
- Exactly which entrance(s) will be used to bring the article(s) into the facility.

If the request is approved, HS-91 notifies protective force officers stationed at the applicable entry control points to expedite processing of the prohibited article(s).

Points of Contact

For the names and contact information for those who can assist with the procedures described in this section, call (202) 586-8075 or (301) 903-0145.

Forms/Samples/Graphics

Sample Memorandum of Authorization for Alcoholic Beverages, (see Attachment 103-1)

ATTACHMENT 103-1

Sample Memorandum of Authorization for Alcoholic Beverages

MEMORANDUM TO (NAME)

DIRECTOR

OFFICE OF ADMINISTRATION

FROM:

(NAME)

TITLE (MUST BE FROM OFFICE DIRECTOR OR HIGHER)

OFFICE OF XXXXXXXXXX

SUBJECT:

Request Approval to Use Alcoholic Beverages within the Forrestal or Germantown Facilities.

The Office of XXXXXXXXXX has scheduled a (Event Type, i.e., holiday party) on (Month Day, Year) at the Forrestal Building in Rm. xx-xxx from x:xx to x:xx am/pm. I am therefore requesting approval to bring alcoholic beverages into the building on (Month Day, Year) for this occasion. Any alcoholic beverage not consumed will be removed from the building upon completion of the event.

I will monitor the consumption of these beverages in order to maintain appropriate conduct and ensure a safe and healthful environment.

Prior to bringing the alcoholic beverages into the building, a copy of the approved memorandum will be provided to the servicing Headquarters Physical Protection Team (Forrestal, Room 1G-042, or Germantown, Room E-333).

If you have any questions, please contact me at extension x-xxxx.

APPROVE: _____ DISAPPROVE: _____ DATE: _____

ACKNOWLEDGED BY HQ PHYSICAL PROTECTION TEAM: _____

This page intentionally left blank.

Section 104

Entry and Exit Inspections

This section describes the methods used to conduct entry and exit inspections of personnel entering and exiting DOE HQ facilities.

HS-91 is responsible for the implementation of entry and exit inspections at all HQ facilities.

HQ Implementation Procedures

Inspections:

Entry inspections are conducted to prevent the introduction of Prohibited Articles into HQ facilities. Exit inspections are conducted to prevent the unauthorized removal of classified information and government property.

The following procedures are used for conducting inspections at HQ facilities:

- All inspections are performed in a consistent and nondiscriminatory manner.
- Employees and contractors are subject to random inspections when entering and departing.
- During security hours (see Section 106), all badged DOE Federal and contractor employees are subject to random inspection.
- DOE Federal and contractor employees issued a temporary badge through the Passage Point system badge are not required to be inspected or have their hand carried items inspected when entering or exiting HQ facilities.
- All visitors and their hand carried articles are inspected upon entry and departure.
- Vehicles operated by Departmental employees and contractors may be subject to random vehicles inspections.
- Vehicles operated by visitors using the facilities are inspected at the vehicle access control point.
- All hand carried articles (i.e., briefcases, purses, parcels or other containers) are subject to inspection by protective force officers. Protective force officers do not open wrappers or packages containing classified material; however, when the contents of a classified package seem suspect, a member of HS-91 is contacted to inspect the package.

Prohibited Articles:

A sign identifying prohibited articles is posted at each HQ facility entrance. The methods for identifying Prohibited Articles are discussed in more detail in Section 103, Prohibited Articles.

Medical Implants:

Personnel with medical implants (pacemakers, artificial joints, etc.) that may cause false alarms or can be adversely affected by the inspection process should contact the appropriate Facility Security Manager – (202) 586-2680 at Forrestal or (301) 903-0145 at Germantown – to request modified screening.

Non-Consent to Inspections:

Individuals not consenting to an entrance inspection are denied entry into HQ facilities. DOE Federal employees or contractor personnel refusing to submit to an inspection may be issued a security infraction or other disciplinary action.

Individuals within an HQ facility who are suspected of engaging in criminal activity or who refuse to submit to an inspection may be detained by protective force officers.

Emergency Access by Response Personnel:

Emergency personnel can be granted immediate entry to HQ facilities, including Security Areas, in response to an emergency. Emergency personnel are not required to undergo an entrance inspection; however, any emergency personnel who are not escorted the entire time inside the facility may be subject to an exit inspection before leaving the facility.

Points of Contact

For the names and contact information for those occupying the positions identified in this section, call (202) 586-8075 or (301) 903-1163.

Section 105

Access Control

This section describes methods for controlling access to HQ facilities and detecting unauthorized intrusions into secure areas. HS-91 is responsible for implementing, operating, testing, and maintaining all HQ access control systems.

Access Control Systems

Entry to HQ facilities is controlled by HQ protective force officers, barriers and gates, various security policies and procedures, and four types of access control systems:

1. CCURE – The Physical Access Control System (PACS) at HQ uses encoded security badges to operate card readers. In most cases, a Personal Identification Number (PIN) is required to enter an area controlled by a card reader. Examples of PACS-controlled card readers include those at the pedestrian entrances to the Forrestal and Germantown buildings, entrances to Limited Areas and Vault-Type Rooms (VTRs), and some controlled access areas (where money, weapons, Controlled Unclassified Information, or high-value equipment may be stored). The PACS provides centralized auditing and monitoring of the card readers through a Central Alarm Station (CAS).
2. TESA Locks – A TESA lock is an electronic lock requiring an encoded security badge and PIN to operate. The locks may be used on doors to Limited and Exclusion Areas or rooms that require controlled access. Programming for TESA locks is arranged through HS-91.
3. Cipher Locks – A cipher lock is a mechanical lock consisting of five buttons that must be pushed in the proper sequence for the lock to open. Cipher lock combinations may be changed by any authorized person with the proper equipment. Cipher locks primarily control access to entrances where DOE property is stored or limited access is desirable. A cipher lock may be used on a door to a Limited Area, but not on a door to a VTR.
4. Keys – Keys are used on doors to rooms or buildings where privacy or property protection is required.

HQ Implementation Procedures

General Access Controls:

Access to HQ buildings is limited to DOE or DOE contractor employees and their authorized visitors. Additional information on specific controls is provided in Section 101, Acquiring HQ Security Badges; Section 102, HSPD-12 and the PIV Process; Section 104, Entry and Exit Inspections; Section 107, Visitor Control; Section 201, Establishing, Maintaining, and

Deactivating Limited Areas and VTRs; and Section 602, Foreign National Unclassified Visits and Assignments.

Every individual entering an HQ facility must obtain and display a security badge. The complete range of security badges in use at HQ is fully described in Section 101, Acquiring HQ Security Badges. DOE security badges contain indicators of the security clearance level (Q, L, or BAO) held by the badged individual. These indicators indicate the individual's authorization to access HQ facilities and/or the Limited Areas and VTRs within HQ.

Security badges shall be worn conspicuously, photograph side out, in a location above the waist and on the front of the body.

DOE reserves the right to deny access to its facilities to any individual who refuses to adhere to prescribed access requirements or when such denial is in the interest of maintaining the safety of its employees or the security of its facilities.

Access by Individuals with an HSPD-12 Badge Not Issued by DOE HQ:

HSPD-12 badges issued by DOE field sites or by OGAs can be registered to allow use of the CCURE system. HSPD-12 badges issued by DOE field sites are effective up to 1 year, while HSPD-12 badges issued by OGAs are effective up to 90 days. Individuals may register at kiosks located in the lobbies of the Forrestal and Germantown facilities.

Access by Individuals with an LSSO Badge Not Issued by DOE HQ:

LSSO badges issued by organizations other than DOE HQ, such as DOE field sites, do not allow entry into any HQ facility. Holders of such LSSO badges must process through the appropriate building reception desk, protective force officers, or other security point of contact responsible for the building.

VTR Access:

DOE Order 473.3 requires access controls at VTRs to include a log and record of all visitors. Occupants of VTRs are permitted to develop their own log, but it should contain spaces for the entrant's name, signature, office symbol or organizational affiliation, purpose of visit, arrival time, departure time, and name of escort (if applicable).

The Director, HS-90 is authorized to waive the requirement for repeated logging of personnel whose workspace is within the VTR. By Memorandum for the Record, dated November 2, 2007, HS-90 waived this requirement, provided that the worker logs in each day on initial entry and final departure.

Accessing Limited Areas and VTRs:

Authorized individuals entering a Limited Area or VTR where protective force personnel do not control access must ensure that unauthorized individuals do not enter the area. Authorized persons may admit an individual, provided that they inspect the individual's security badge to ensure that it bears the individual's photo and that he/she has the proper security clearance. Need to know must also be established before permitting entry into a VTR.

Access Authorization Memoranda:

Access authorization memoranda are not required for cipher lock or key-controlled areas.

When a Limited Area or VTR is first established (see Section 201, Establishing, Maintaining, and Deactivating Limited Areas and VTRs) or a TESA lock is newly installed on an area requiring controlled access, the responsible element HSO, Alternate HSO, or HSO Representative ensures that an Initial Access Authorization memorandum is submitted. The memorandum identifies who needs access to the area and provides contact information for them. The memorandum must be addressed to HS-91, and then sent as an attachment to an encrypted e-mail to the HQ Security Alarm and Access Control System (SAACS) Team. (The e-mail with an attached memorandum for areas with CCURE automated access control card readers should be addressed to "DL-HSS HQACCESS." The e-mail with an attached memorandum for areas with TESA locks should be sent to "DL-HSS HQTESA.") The memorandum authorizes the HQ SAACS Team to encode the security badges of individuals authorized to routinely enter the area. The encoding not only allows the security badge to unlock the doors, but may also allow designated persons to activate or deactivate the intrusion detection systems ("alarms") for the area. The initial access memorandum must contain the information specified in Attachment 105-1 at the end of this section.

NOTE: Pay close attention to the instructions included with the sample memorandum. Persons must be identified by last name, first name, and middle initial exactly as the names appear on their security badges. Do not use nicknames, initials, or any name other than what appears on the person's badge. Badge numbers are not required on access memoranda.

NOTE: Access memoranda for areas controlled by a CCURE card reader or TESA lock generally use the same format, except that memoranda for a CCURE card reader also require listing the "station or account number." The station/account number identifies a specific location monitored by the CAS. The station/account number is obtained by contacting the HQ Physical Security Systems Manager. Once the station/account number is known, the HSO should keep a record of it to simplify future submissions. Station or account numbers are not used for TESA locks, so access authorization memoranda for areas controlled by a TESA lock should not contain a station/account number.

Access authorization memoranda may need to be revised when:

- A new person needs added to the access list
- A person no longer needs access to the area
- Any change affects who can activate and deactivate the alarms
- The priority call list changes
- A person on the priority call list changes phone numbers
- Twelve months have passed since the last updated memo.

In any of these circumstances, a revised access authorization memorandum must be sent to the HQ SAACS Team via encrypted e-mail in the same manner as described above. The format for a changed access authorization memorandum is provided in Attachment 105-2 at the end of this section. Each revision of the access list must have an effective date and include the complete list of employees authorized to access the area.

Stop Access Request:

When a person poses a danger to supervisors or co-workers or is disruptive to the DOE mission, it may be necessary to revoke an individual's access to HQ facilities temporarily or permanently. To revoke a person's access, a Stop Access Request is sent to the Director, HS-91. The request must be sent and signed by a senior Federal official within the HQ element, the element's HSO or Alternate HSO, or the Director, HS-90. The request should properly identify the person to be denied access, briefly explain the reason for the request, and describe any special notifications that are desired if the person attempts to enter an HQ facility. The Director, HS-93 must be listed as a "cc" recipient of the request.

If an emergency situation arises, the request can be communicated in person or by phone to HS-91; however, a Stop Access Request must be provided within 1 work day. A Sample Stop Access Request is provided in Attachment 105-3 at the end of this section.

If the person is in an HQ facility at the time it becomes necessary to stop his/her access, the person should be escorted out of the facility by the HSO or other representative of the element and his/her security badge confiscated upon departure. HS-91 can arrange for protective force assistance during such actions. The confiscated badge is returned to the HQ Facility Security Manager.

Once a Stop Access Request is implemented, the Head of Element or HSO must advise HS-91 via formal memorandum or e-mail of the rescission status and whether it is temporary or permanent.

Individuals who are put on Administrative Leave must be put on a Stop Access memorandum for the duration of the leave.

Intrusion Alarms:

The HQ protective force must send an officer to investigate the cause of an activated alarm. Persons who set off door alarms must remain in place and provide information regarding the alarm to the responding officer. Individuals who create multiple false alarms can be subject to a security infraction.

Anyone noting an alarm should report it immediately to the CAS alarm console operator on extension 6-6900 (Forrestal) or 3-2403 (Germantown). If the alarm is determined to be malfunctioning and in need of repair, HS-91 will notify the element HSO of what repairs are required or how much downtime is anticipated.

Points of Contact

For the names and contact information for those who occupy the positions identified in this chapter, call (202) 586-8075 or (301) 903-1163.

CCURE Access Control Memoranda, encrypted e-mail to “DL-HSS HQACCESS”

TESA Lock Access Control Memoranda, encrypted e-mail to “DL-HSS HQTESA”

Forms/Samples/Graphics

Sample Initial Access Authorization Memorandum for New Areas (see Attachment 105-1)

Sample Updated Access Authorization Memorandum (see Attachment 105-2)

Sample Stop Access Request (see Attachment 105-3)

ATTACHMENT 105-1

Sample Initial Access Authorization Memorandum for New Areas

MEMORANDUM FOR (NAME), DIRECTOR
OFFICE OF PHYSICAL PROTECTION
OFFICE OF HEADQUARTERS SECURITY OPERATIONS

FROM: (NAME)
HEADQUARTERS SECURITY OFFICER
NAME OF ELEMENT

SUBJECT: Initial Access Authorization List for Room _____,
_____ Building, and Station/Account Number _____

This memorandum creates the initial Access Authorization list for the area identified above, effective (date). The following personnel require routine access to the room and will require the access level indicated.

Name	Routing Symbol	Employer	Home Phone	Access Level	Call Priority
Doe, Ralph K.	NS-4	DOE	(202) 555-1234 (U)	B	2
Law, John J.	NS-44	TPTT	(301) 555-9956	B	1
Public, Jane P.	NS-44	TPTT	(703) 555-1933	B	3
Sam, Uncle (NMI)	NS-21	DOE		A	
Train, Thomas T.	NS-21	Lionel Ind.		A	

If you have any questions, please contact me on (Phone Number).

Official Use Only Stamp

OFFICIAL USE ONLY (When filled in)

Instructions for Completing this Memorandum

"Memorandum for":	Must be addressed to the Director, HS-91
"From":	Must be from the element's HSO, Alternate HSO, or HSO Representative
"Subject":	The room number and building name are required for all access memoranda. The Station/Account Number is required only for rooms or areas secured by a CCURE-controlled card reader. Rooms/areas secured by a TESA lock do not require a Station/Account Number. <i>Use a separate memo for each room access list.</i> Do not cross reference other access lists.
Effective date:	Select a date several days in the future to allow HS-91 sufficient time to make the required changes. The longer the list of names, the more time will be required.
"Name":	The names must be in alphabetical order, in the format of last name, first name, and middle initial. Names must be exactly as they appear on the badges.
"Routing Symbol":	Organization code.
"Employer":	Briefly identify the person's employer. Federal employees must be listed as "DOE." If a contractor, list the name of the employer.
"Home Phone":	List home phone numbers for at least three people on the access list. Use a "(U)" to designate unlisted home phone numbers.
"Access Level":	Enter an "A" or "B." "A" means the individual can access the area only when the alarms are off. "B" means the individual has the authority to turn the alarms on and off.
"Call Priority":	The order in which people are to be contacted if the room is found to be unsecured or a problem has developed. At least three people should be designated with a call priority. This listing must match the SF 700 for areas with combination locks.

ATTACHMENT 105-2

Sample Updated Access Authorization Memorandum

MEMORANDUM FOR (NAME), DIRECTOR
OFFICE OF PHYSICAL PROTECTION
OFFICE OF HEADQUARTERS SECURITY OPERATIONS

FROM: (NAME)
HEADQUARTERS SECURITY OFFICER
NAME OF ELEMENT

SUBJECT: Changes to the Access Authorization List for Room _____,
_____ Building, and Station/Account Number _____

This memorandum updates the access authorization list for the area identified above, effective (date). The following personnel require routine access to the room and will require the access level indicated.

Name	Routing Symbol	Employer	Home Phone	Access Level	Call Priority
Box, Pandora S.	NS-19	Containers, Inc.		A	
Doe, Ralph K.	NS-4	DOE	(202) 555-1234 (U)	B	2
Law, John J.	NS-44	TPTT	(410) 555-1027	B	1
Public, Jane P.	NS-44	TPTT	(703) 555-1933	B	3
Sam, Uncle (NMI)	NS-21	DOE		A	

The following individual(s) was/were added to the list:

Pandora S. Box

The following individual(s) was/were deleted from the list:

Thomas T. Train

The phone number was changed for the following individual:

John J. Law; his new number is (410) 555-1027

If you have any questions, please contact me on (Phone Number).

Official Use Only Stamp

OFFICIAL USE ONLY (When filled in)

Instructions for Completing this Memorandum

"Memorandum for":	Must be addressed to the Director, HS-91
"From":	Must be from the element's HSO, Alternate HSO, or HSO Representative
"Subject":	The room number and building name are required for all access memoranda. The Station/Account Number is required only for rooms or areas secured by a CCURE-controlled card reader. Rooms/areas secured by a TESA lock do not require a Station/Account Number. <i>Use a separate memo for each room access list.</i> Do not cross reference other access lists.
Effective date:	Select a date several days in the future to allow HS-91 sufficient time to make the required changes. The longer the list of names, the more time will be required.
"Name":	The names must be in alphabetical order, in the format of last name, first name, and middle initial. Names must be exactly as they appear on the badges.
"Routing Symbol":	Organization code.
"Employer":	Briefly identify the person's employer. Federal employees must be listed as "DOE." If a contractor, list the name of the employer.
"Home Phone":	List home phone numbers for at least three people on the access list. Use a "(U)" to designate unlisted phone numbers.
"Access Level":	Enter an "A" or "B." "A" means the individual can access the area only when the alarms are off. "B" means the individual has the authority to turn the alarms on and off.
"Call Priority":	The order in which people are to be contacted if the room is found to be unsecured or a problem has developed. At least three people should be designated with a call priority. This listing must match the SF 700 for areas with combination locks.
"Additions":	Identify the name(s) of individuals added to the access list.
"Deletions":	Identify the name(s) of individuals removed from the access list.
"Phone Number":	Identify the name(s) of individuals whose phone numbers have changed and list the new numbers.

ATTACHMENT 105-3

Sample Stop Access Request

MEMORANDUM FOR (NAME), DIRECTOR
OFFICE OF PHYSICAL PROTECTION
OFFICE OF HEADQUARTERS SECURITY OPERATIONS

FROM: (NAME)
HEADQUARTERS SECURITY OFFICER
NAME OF ELEMENT

SUBJECT: Stop Access Request

This memorandum requests that a "Stop Access" order be issued for:

Name: Train, Thomas T.
Routing Symbol: NS-21
Employer: Lionel, Inc.

This request is effective immediately. Your office will be notified when the "Stop Access" can be discontinued.

The reason for this request is that Mr. Train poses a potential danger to his supervisor and co-workers in the Office of Nuclear Science (NS).

If Mr. Train attempts to enter any DOE HQ facility, please contact me immediately at (202) 586-5555 or notify the NS Alternate HSO at (202) 586-7777.

cc:
Director, HS-93

Official Use Only Stamp

OFFICIAL USE ONLY (When filled in)

Instructions for Completing a Stop Access Request

- "Memorandum for": Must be addressed to the Director, HS-91
- "From": Must be from the element's HSO, Alternate HSO, a senior Federal official within the program element, or the Director, HS-90
- "Subject": "Stop Access Request."
- "Name": Identify the person by last name, first name, and middle initial, exactly as it appears on the person's security badge.
- "Routing Symbol": Organization code.
- "Employer": Briefly identify the person's employer. Federal employees must be listed as "DOE." If a contractor, list the name of the employer.
- "Effective date": Usually a Stop Access is effective immediately, but a future date can be specified.
- "Reason for request": Briefly describe the justification for the Stop Access. The most frequent reason is because the person named poses a potential danger. Other reasons might include disciplinary actions, investigative requirements, or judicial directives.
- "Notifications": Identify who within the program element should be notified if the person named attempts to enter an HQ facility. A primary point of contact and an alternate is preferred. Include the work phone number of the person(s) to be notified.
- "cc": Always include the Director, HS-93 on a Stop Access Request, even if the person named does not have a security clearance.

This page intentionally left blank.

Section 106 Security Hours

This section identifies the times designated as Security Hours at HQ facilities. During Security Hours, the security posture of HQ facilities is increased. Additional security measures implemented during Security Hours include, but are not limited to:

- Closing certain entrances and exits
- Requiring all visitors to be under escort and inspected
- Requiring random inspections for all employees and contractors entering and departing the facility
- Inspecting all OGA individuals.

The Director, HS-90 designates Security Hours.

HQ Implementation Procedures

Security Hours are as follows

- Monday through Friday 7:00 P.M. until 6:00 A.M., each day
- All weekends beginning on Friday at 7:00 P.M. through Monday at 6:00A.M.
- All holidays and Administrative or Executive Order closings beginning at 7:00 P.M. on the evening preceding a non-Federal work day through 6:00 A.M. on the next Federal work day.

Points of Contact

For additional information on Security Hours, call (202) 586-8075 or (301) 903-0145.

This page intentionally left blank.

Section 107

Visitor Control

This section describes the security procedures for processing visitors to HQ facilities. Additional information about the types of badges issued to visitors, what inspections they undergo, when they must be escorted, and specific approvals required before foreign visitors are admitted are provided in Section 101, Security Badges; Section 104, Entry and Exit Inspections; Section 106, Security and Non-Security Hours; and Section 602, Unclassified Foreign Visits and Assignments.

HS-91 develops and implements visitor control procedures for all HQ facilities.

HQ Implementation Procedures

All DOE Federal, contractor employees, and visitors must provide a valid DOE security badge, driver's license, passport, or other form of government-issued photo identification to enter HQ facilities.

Once the inspection process is completed and access is granted, a visitor may travel throughout the facility without escort during non-security hours. If the visitor needs to enter a Limited Area, he/she must comply with the escort procedures set out in Attachment 107-1 at the end of this section.

If the visitor is unfamiliar with the facility, he/she may request assistance from the host office to locate the office or employee being visited. The office being visited must provide the requested escort. During Security Hours, an escort must be provided for all visitors who do not have an encoded DOE security badge.

A DOE HQ Federal or contractor employee with an HSPD-12, LSSO, or Passage Point badge may sponsor a visitor. A DOE HQ employee or contractor with a Green badge may not sponsor a visitor.

DOE Employees Visiting HQ Facilities:

DOE Federal and contractor employees who are visiting a HQ facility and have in their possession a DOE-issued HSPD-12 badge will be admitted to HQ facilities upon display of that badge. Before gaining turnstile access, such visitors must enroll their badges at the self-service kiosk. DOE visitors who cannot use the kiosk must proceed to the receptionist desk to receive a temporary Passage Point paper badge. If they still wish to obtain turnstile access, they will be directed to the badge office for enrollment.

Any DOE Federal or contractor employee who is visiting a HQ facility and does not have in his/her possession a DOE-issued HSPD-12 security badge must process through the receptionist

desk in the Forrestal, 955 L'Enfant Plaza, or Germantown main lobby and submit to inspection prior to entry.

Visitors from OGAs:

OGA employees holding an HSPD-12 security badge must process through the automated kiosk in the Forrestal and Germantown Main Lobby or see the receptionist/security officer. An OGA visitor with an HSPD-12 badge that is not currently encoded for turnstile access must submit to inspection prior to entry.

OGA Visitors Attending a Classified Meeting at DOE HQ:

When a visitor from an OGA has a security clearance and will be attending a classified meeting at HQ, that visitor must have his/her agency's security office pass the security clearance to HQ. See Section 306, Passing Security Clearances for Classified Meetings or Visits, for details on passing security clearances. Upon arrival the visitor must advise the receptionist that his/her agency has passed his/her security clearance to DOE. The receptionist verifies the visitor's clearance level and visit authorization, and issues a visitor badge indicating the appropriate access authorization.

U.S. Citizen Visitors:

Visitors must report to an authorized automated visitor registration system issuing point, typically the main lobbies in the Forrestal, 955 L'Enfant Plaza, or Germantown facilities. The visitor must identify who they intend to visit. The receptionist contacts the host to determine if the visitor can be admitted. The visitor must present a valid driver's license, passport, or other form of government-issued photo identification as personal identity verification, which is electronically entered into the automated visitor registration system. A temporary paper badge is then provided for the visitor to wear while in the HQ facility.

Pre-Announcements:

When an HQ employee expects a visitor, the employee can pre-announce the visit to HS-91 by sending an e-mail to the Forrestal or Germantown Facility Security Manager providing the name of the visitor, the company or agency he/she is affiliated with, the approximate arrival time, and the name and telephone number of the host. The pre-announcement expedites visitor processing, eliminating the need for a receptionist to locate the host before issuing a temporary security badge, and provides the receptionist with a phone number to notify the host of the visitor's arrival.

Group Visits:

Group visits (five or more individuals attending the same function) require a pre-announcement and an e-mail from the host to the Facility Security Manager stating where the visit will occur. The

e-mail must have two attachments: a Group Meeting Information Sheet and a Memorandum for Group Meeting Information (see Attachment 107-1 at the end of this section).

NOTE: If more than 15 visitors are attending the same function, the host organization must provide at least one person to meet the visitors upon their arrival and assist in the issuance of badges, so as to avoid unnecessary delays.

Uncleared Foreign National Visitors:

Foreign national visitors must report to the main lobby reception areas in the Forrestal, 955 L'Enfant Plaza, or Germantown facilities. The visitor must identify himself/herself as a foreign national and present his/her passport, visa, or any valid I-9 photo document. The receptionist queries the FACTS database to determine whether the foreign visit is approved. The host should also e-mail the servicing Facility Security Manager and designees an electronic copy of the memorandum approving the foreign visit. The memo must include the request number. The e-mail with memorandum eases processing and reduces delays. The visitor's passport or other acceptable documentation is electronically entered into the automated visitor registration system. The receptionist issues a temporary foreign national badge for the visitor to wear while in the HQ facility. The HQ element sponsoring the visit assigns a U.S. citizen with a permanent HQ badge to meet the foreign national at the reception desk.

When a foreign visit is not approved in FACTS or an electronic copy of the approval memorandum is not in place, a protective force supervisor or Federal member of HS-91 may allow the visit to continue. The host must be informed that the visitor's pertinent information must be approved within FACTS before the close of business on that day. Visitors approved under these circumstances must be escorted at all times by a U.S. citizen with a permanent HQ security badge.

A foreign national visiting the Office of the Secretary or other high-level HQ officials at the Forrestal Building qualifies as a "High Level Protocol Visitor." See Section 602, Unclassified Foreign Visits and Assignments, of the HQFMSP for more information.

Cleared Foreign National Visitors:

See Section 601, Classified Visits.

Visitors Attending Public Hearings:

HQ elements hosting public hearings or meetings are responsible for providing adequate staff to register members of the public who desire to attend such events.

When the public is notified of the hearing/meeting, the host organization must immediately notify by e-mail the Forrestal Facility Security Manager or Germantown Facility Security Manager of the date, time, and location of the event.

Congressional and State Visitors:

Impending visits to HQ facilities by members or employees of Congress or Congressional Committees or by Governors or their staffs must be coordinated through the Director of Congressional Affairs.

Very Important Person (VIP) Visitors:

VIP visitors are those visiting/meeting with the:

- Secretary
- Deputy Secretary
- Under Secretaries
- Administrator, National Nuclear Security Administration.

Receptionists issue special badges to VIPs at the Forrestal and Germantown facilities.

Distinguished Visitors (DVs):

DVs are those visiting/meeting with:

- Program Secretarial Officers
- Members of Secretarial Offices.

Receptionists issue special badges to DVs at the Forrestal and Germantown facilities.

Escort Procedures for Uncleared Visitors:

Escort responsibilities for visitors entering a Limited Area are described in Attachment 107-2.

Admission of Minors:

Minors may be admitted to HQ facilities, and the sponsoring adult must escort and maintain control over the minor at all times. Minors age 6 or under do not require badges. A child over 6 years of age is issued an appropriate temporary visitor badge.

Points of Contact

For the names and contact information for those who occupy the positions identified in this chapter, call (202) 586-8075 or (301) 903-0145.

Forms/Samples/Graphics

Escort Procedures for Uncleared Visitors to Limited Areas (see Attachment 107-1)

Memorandum for Group Meeting Information w/Group Meeting Information Sheet (see Attachment 107-2)

ATTACHMENT 107-1

Escort Procedures for Uncleared Visitors to Limited Areas

The following guidelines are intended for use by HQ personnel escorting an uncleared visitor entering a Limited Area.

Preparing for the Visit

Find out whether the uncleared visitor is a U.S. citizen or a foreign national.

Foreign national visitors will not be admitted into a DOE HQ facility unless their visit has been approved in FACTS and a memorandum specifically approving the visit has been furnished to protective force receptionists. The escort should ensure that these actions have occurred before attempting to escort the foreign visitor into the facility or a Limited Area.

The escort must have a security clearance, "L" or "Q," commensurate with the level of information handled within the Limited Area.

As a rule of thumb, one escort should not escort more than five visitors. If more than five visitors are expected, assign additional escorts. Even if there is only one visitor, arrange for at least one backup escort in case of contingencies during the visit.

Informing the Visitor Before His/Her Arrival

Tell the uncleared visitor that certain items are prohibited or controlled in the area to be visited:

- Firearms
- Knives
- Cameras
- Laptop computers
- Pagers
- Electronic toys.

Tell the visitor to leave extra time for security processing. He/she will need to check in at the facility reception desk, receive a special visitor's badge, and go through security screening.

Meeting the Visitor

Meet the visitor either in the lobby of the building or at the entrance to the Limited Area.

Direct the visitor to the reception desk to obtain a visitor badge if he/she does not already have one.

Instruct the visitor to display the visitor badge above his/her waist in an easily observable position. Caution the visitor about his/her responsibility to not lend or attempt to transfer the badge to anyone.

If the visitor brings a cell phone, pager, BlackBerry, or other electronic device(s) to the Limited Area, handle them as described in Section 202, Controlled Articles, of the HQFMSP.

Escorting the Visitor

Escort the visitor at all times while in the Limited Area.

Ensure that the visitor does not access classified information by overhearing classified conversations, reading or copying classified information, observing classified computer processing, or any other means.

Ensure that the visitor does not remove DOE property (unless an authorized person has issued him/her a Property Pass – see Section 108 of the HQFMSP).

If the visitor needs to use a restroom, accompany the visitor to the restroom door and remain outside the restroom door until the visitor is ready to return.

If there are multiple visitors and they need to go in different directions, arrange for additional escorts.

At the end of the visit, ensure that the visitor returns the badge to the protective force reception desk or any manned protective force post when the visit is completed.

Informing the Visitor Before His/Her Arrival

Tell the uncleared visitor that certain items are prohibited or controlled in the area to be visited:

- Firearms
- Knives
- Cameras
- Laptop computers
- Pagers
- Electronic toys.

Tell the visitor to leave extra time for security processing. He/she will need to check in at the facility reception desk, receive a special visitor's badge, and go through security screening.

Meeting the Visitor

Meet the visitor either in the lobby of the building or at the entrance to the Limited Area. Direct the visitor to the reception desk to obtain a visitor badge if he/she does not already have one.

Instruct the visitor to display the visitor badge above his/her waist in an easily observable position. Caution the visitor about his/her responsibility to not lend or attempt to transfer the badge to anyone.

If the visitor brings a cell phone, pager, BlackBerry, or other electronic device(s) to the Limited Area, handle them as described in Section 202, Controlled Articles, of the HQFMSP.

Escorting the Visitor

Escort the visitor at all times while in the Limited Area.

Ensure that the visitor does not access classified information by overhearing classified conversations, reading or copying classified information, observing classified computer processing, or any other means.

Ensure that the visitor does not remove DOE property (unless an authorized person has issued him/her a Property Pass – see Section 108 of the HQFMSP).

If the visitor needs to use a restroom, accompany the visitor to the restroom door and remain outside the restroom door until the visitor is ready to return.

If there are multiple visitors and they need to go in different directions, arrange for additional escorts.

At the end of the visit, ensure that the visitor returns the badge to the protective force reception desk or any manned protective force post when the visit is completed.

ATTACHMENT 107-2

Memorandum for Group Meeting Information w/Group Meeting Information Sheet

MEMORANDUM FOR (NAME), FACILITY SECURITY MANAGER
OFFICE OF PHYSICAL PROTECTION
OFFICE OF HEADQUARTERS SECURITY OPERATIONS

FROM: (NAME OF HOST)
(POSITION OF HOST)
NAME OF ELEMENT

SUBJECT: Notification of Group Meeting

The Office of _____ will host a group meeting in Room (number) on (date) at (time). We are expecting approximately (number) visitors who are listed on the attached *Group Meeting Information Sheet*. Please ensure this Group Meeting Information Sheet is distributed to facility receptionists and the appropriate types and numbers of visitor badges are prepared for signatures and issuance when they arrive.

(NOTE 1: If the meeting involves 15 or more visitors, include a statement that representatives from the hosting element will assist receptionists in issuing badges to the arriving visitors.)

(NOTE 2: For classified meetings or conferences please recognize that the time and location of a classified meeting may themselves be classified information. Coordinate with a Classification Official or your HSO before preparing or distributing any memorandum listing the date, time, and/or location of a classified meeting.)

(NOTE 3: DO NOT include foreign nationals on a Group Meeting Information Sheet. See Section 602, Unclassified Foreign Visits and Assignments, for information about processing foreign visitors. DO NOT fill in the citizenship block unless the visitor's U.S. citizenship has been confirmed. DO NOT ASSUME THAT A VISITOR IS A U.S. CITIZEN.)

Please contact (name of contact) from this office at (phone number) if you have any questions.

Attachment

GROUP MEETING INFORMATION

Meeting Title:	Meeting Location:
Date/Duration:	Time:
POC Name, Phone Number, and Routing Symbol:	

ATTENDEES

NOT including foreign nationals, except those attending a meeting open to the public.

Last Name, First Name, Middle Initial (Type or print neatly)	Citizenship	Company/Agency Represented	Office to Be Visited	This Section Completed by Security																																															
				Badge Information		Arrival Time In																																													
				Level	Number																																														
Print/Type:							1																																												
Signature:								Print/Type:							2	Signature:				Print/Type:							3	Signature:				Print/Type:							4	Signature:				Print/Type:							5
Print/Type:							2																																												
Signature:								Print/Type:							3	Signature:				Print/Type:							4	Signature:				Print/Type:							5	Signature:											
Print/Type:							3																																												
Signature:								Print/Type:							4	Signature:				Print/Type:							5	Signature:																							
Print/Type:							4																																												
Signature:								Print/Type:							5	Signature:																																			
Print/Type:							5																																												
Signature:																																																			

Section 108

Removal of Accountable Government Property and Employee Personal Property

Accountable government property consists of equipment or sensitive items, regardless of value, that require special control and accountability because of susceptibility to unusual rates of loss, theft, or misuse or due to national security and export control considerations. Examples of government property considered to be accountable at HQ are shown in Attachment 108-1 at the end of this section.

The Office of Project Integration and Logistics Operations (MA-432) is responsible for implementing property control procedures at HQ. Each HQ element has designated an Accountable Property Representative (APR) to act as an agent for MA-432. In addition, MA-432 has identified personnel within each HQ element who act as Property Pass Signers, who are authorized to provide Property Passes to element personnel who may need to remove accountable government property from an HQ facility.

NOTE: The terms “Authorized Issuing Officer” and “Property Pass Signer” are both acceptable. Because the term “Property Pass Signer” is more commonly used throughout HQ, that term will be used throughout this section.

NOTE: The official term for a “Property Pass” is a “Property Removal Authorization.” Because the term “Property Pass” is more commonly used throughout HQ, that term will be used throughout this section.

HQ Implementation Procedures

Becoming a Property Pass Signer:

Federal appointed APRs are authorized to sign property passes for their designated program element(s). Each HS element should have at least one Property Pass Signer to service elemental personnel at each HQ facility where it has offices (at least two at each facility is recommended). For example, if an HQ element has personnel at both the Forrestal and Germantown buildings, there should be at least one Property Pass Signer at each location.

Appointments of Property Pass Signers, other than APRs, are requested by an Office Director via a memorandum to the Property Management Office, MA-432, room GG-087, Forrestal, with the candidate’s name, organization title, and phone extension.

Upon approval, MA-432 furnishes HS-91 a current and complete electronic list of Property Pass Signers. HS-91 provides this information to protective force personnel assigned at each building entrance/exit.

A link to the current list of Property Pass Signers is included in the Helpful Websites subsection below. MA-432 will provide an updated listing the last Friday of every month (if applicable), with an effective date of the following Monday.

Issuance of Property Passes:

HQ F 580, *Certificate of Property/Property Removal Authorization (Property Pass)*, must be issued by a Property Pass Signer whenever an individual needs to remove accountable government property from an HQ facility.

To complete the Property Pass form, the following information is required:

- Name of the holder
- Holder's organization code
- Room number and facility name where the holder is assigned
- Holder's telephone number
- Description of the property being removed, including:
 - Nomenclature
 - DOE property tag number (if applicable)
 - Model number.
- Organization the property belongs to
- When the property will be removed
- When the property will be returned (The Property Pass can be issued for up to 3 years. Leaving the return date blank or writing "N/A" in this block is unacceptable).

Property Passes must be digitally signed by the authorized signer after the form has been completely filled out.

Removal of Accountable Government Property:

When an individual removes accountable government property, he/she must present the digitally signed Property Pass to the protective force officer posted at the exit. The officer:

- Ensures that the Property Pass is properly completed
- Verifies that the holder's identity matches that listed
- Verifies that the property matches that listed
- Verifies the authenticity of the signature of the Property Pass Signer/Authorized Issuing Officer
- Ensures that the property pass is current.

If these conditions are not met, the protective force officer may confiscate both the property and the Property Pass and notify the appropriate HSO or HS-91 representative.

Removal of Employee Owned Personal Property:

When an individual removes employee owned personal property from a HQ facility, he/she must follow the same rules as removing accountable government property, with one exception. That exception is that a DOE F 580.2, *Employee Personal Property Removal Authorization (Property Pass)*, is used to document the removal.

Visitor Temporary Property Passes:

If a visitor brings a personal or government laptop computer into an HQ building, protective force personnel issue him/her a Passage Point temporary property pass to help avoid unnecessary delays when the visitor departs the HQ facility.

The visitor is responsible for maintaining possession of the temporary property pass for the duration of his/her stay and returning the pass to protective force personnel upon departure.

Moving Boxes:

Government-purchased brown cardboard moving boxes are not to be removed from HQ facilities unless they are properly marked and identified as part of a scheduled move by MA-40.

Points of Contact

For the names and contact information for those who occupy the MA positions identified in this section, call (202) 287-5496.

Forms/Samples/Graphics

Examples of Government Owned or Leased Property Requiring a Property Pass (see Attachment 108-1)

HQ F 580, *Certificate of Property/Property Removal Authorization (Property Pass)*, (available from MA-432)

HQ F 580.2, *Employee Personal Property Removal Authorization (Property Pass)*, (available from MA-432)

Helpful Website

A current list of Authorized Issuing Officers/Property Pass Signers can be found at:
<http://energy.gov/management/office-management/employee-services/property-management>

ATTACHMENT 108-1

Examples of Government Owned or Leased Property Requiring a Property Pass

Desktop computers (central processing unit)

Laptop computers

Televisions (LCD and Plasma)

Monitors (LCD and Plasma)

Printers

Audiovisual equipment (projectors, video conferencing equipment)

Any furniture item

NOTE: Property Passes are not required for HQ property-tagged cellular telephones/BlackBerry-type devices or personal cell phones, including Personal Digital Assistants (PDAs), tablets, and iPads.

Section 109

Lock and Key Control

DOE Order 473.3, *Protection Program Operations*, Attachment 3, Section A, Chapter IV, establishes requirements for controlling keys and locks used for the protection of high-value government assets and classified matter. It establishes four levels of control based on the types of matter being protected, ranging from Level I, for locks and keys that secure nuclear weapons, to Level IV, for offices without open storage for classified matter. It also requires line management, based on site analysis, to determine the appropriate key and lock level for application to the site.

In August 2008, after a review of HQ assets and security strategies, the Director, HS-90 determined that Level IV controls are appropriate for all HQ facilities. Under Level IV, personnel must protect keys, pass cards, combinations, etc., from compromise, but formal accountability is not required.

HQ Implementation Procedures

Combinations to locks securing classified matter (i.e., in repositories or VTRs) must be changed when an employee leaves, no longer requires, or is no longer permitted access.

The classified matter custodian or the element's HSO may request combinations changes by telephoning the servicing badge office (Forrestal at x6-5764 or Germantown at x3-3330) or by sending an e-mail to “Badge Office” in the HQ Global Address List.

See Section 105, Access Control, for additional information on such matters as changing access lists, obtaining CCURE card readers, and TESA lock services.

Requests for commercial locksmith services, such as repairing or drilling broken locks, must be submitted to the servicing Building Facility Manager on a DOE F 4250.2, *Requisition for Supplies, Equipment, or Service*. The DOE F 4250.2 may be signed by the HQ element's HSO, APR, or Administrative Officer.

Points of Contact

For the names and contact information for those who occupy the positions identified in this chapter, call (202) 586-8075 or (301) 903-1163.

Forms/Samples/Graphics

DOE F 4250.2, *Requisition for Supplies, Equipment, or Service*, (for a copy of this form go to: <http://energy.gov/cio/downloads/requisition-supplies-equipment-or-service>)

This page intentionally left blank.

Chapter 2

Limited Areas, VTRs, and Temporary Limited Areas

Chapter 2 describes the security procedures adopted by DOE HQ to implement the requirements of the following DOE directives:

- DOE Order 473.3, *Protection Program Operations*
- DOE Order 471.6, Change 1, *Information Security*
- DOE Order 475.2A, *Identifying Classified Information*
- Classification Bulletin TNP-32, *Classification Guidance for Classified Meeting Locations at DOE/NNSA or DOE/NNSA Contractor Sites or Facilities*, dated May 27, 2010

DOE Manual 470.4-2A, *Physical Protection*, defines seven types of Security Areas that protect DOE employees, facilities, buildings, government property, classified information, nuclear materials and other security interests. Each type of Security Area has its own security requirements, such as access controls, alarms, vehicle controls, construction standards, operating procedures, etc. The seven types of Security Areas include:

- General Access Areas
- Property Protection Areas
- Limited Areas (LAs)
- Vault-Type Rooms (VTRs)
- Special Designated Security Areas
- Protected Areas
- Material Access Areas

All HQ facilities have General Access Areas and Property Protection Areas; however, only the Forrestal, Germantown, and 955 L'Enfant Plaza facilities have LAs, VTRs, and Special Designated Security Areas. At HQ, Special Designated Security Areas consist of Sensitive Compartmented Information Facilities (SCIFs) and Special Access Program (SAP) facilities. LAs, VTRs, and Special Designated Security Areas are not currently permitted in HQ facilities other than the Forrestal, Germantown, and 955 L'Enfant Plaza facilities. There are no Protected Areas or Material Access Areas at HQ.

DOE HQ has also established an LA sub-type area known as a Temporary Limited Area (TLA), which protects classified information for short periods of time. For example, a TLA may be established to allow a senior Departmental official to review classified information in his/ her office, or when an LA is undergoing renovation.

Because of common, local usage, the term “Security Area” at HQ has come to mean an LA, VTR, or TLA.

Chapter 2 describes the processes required to establish, operate, maintain, and deactivate LAs, VTRs, and TLAs at DOE HQ:

- Section 201 describes the procedures for establishing, maintaining, and deactivating LAs, VTRs, and TLAs.
- Section 202 identifies “Controlled Articles,” which are items that are not permitted (or that must remain under strict control) within an LA, TEMPEST Protected Area, or VTR.
- Section 203 describes the procedures for holding classified discussions and meetings in LAs and VTRs.
- Section 204 covers holding classified meetings in locations not pre-approved for classified discussions.
- Section 205 discusses how to obtain Secure Telecommunications Equipment (phones) and other Communications Security services.

HQ security procedures for Special Designated Security Areas (SCIFs and SAP facilities) are described in other security plans with a limited distribution and are not discussed in this HQFMSP.

Section 201

Establishing, Maintaining, and Deactivating LAs, VTRs, and TLAs

Classified matter must be processed, discussed, handled, or stored in designated LAs, VTRs, or TLAs. LAs, VTRs, and TLAs must have security measures in place to detect and deter unauthorized persons from gaining access to the classified matter. This includes measures to prevent unauthorized persons from seeing or hearing classified information. All LAs, VTRs, and TLAs at HQ must be approved by the Office of HQ Security Operations (HS-90) prior to the initiation of classified activities or the introduction of classified material or equipment.

Definitions of LA, VTR, and TLA:

1. Limited Area (LA) – An LA is a Security Area that protects classified matter. LAs are defined by physical barriers encompassing the designated space and have access controls to ensure only authorized personnel enter and exit the LA. A means must be provided to detect and deter unauthorized entry into the LA. In some instances, an LA may also be approved for processing, destroying, reproducing, transmitting or receiving, and discussing classified information.
2. Vault-Type Room (VTR) – A VTR is a DOE-approved room having combination-locked doors and protection provided by a Department-approved intrusion alarm system activated by any penetration of walls, floors, ceilings, or openings, or by motion in the room. Typically, VTRs are used for the open storage of classified materials, equipment, and components up to and including Secret/Restricted Data (S/RD). In some instances, they may also be approved for processing, destroying, reproducing, transmitting or receiving, and conducting amplified discussions of classified information.

NOTE: As a general rule, the open storage of TS/RD is not approved at HQ facilities.

3. Temporary Limited Area (TLA) – A TLA may be established when it is necessary to review classified information for a limited time period in a room that is not an already approved LA or VTR. Usually, TLAs are established while an LA or VTR undergoes construction or when a cleared employee needs to review classified information no higher than S/RD for a brief period of time. The security measures for a TLA are determined on a case-by-case basis and must be approved by the HQ Classified Matter Protection and Control (CMPC) Program Manager prior to any classified activities taking place in a TLA.

Documenting the Process:

The LA/VTR approval process is documented from initial visit through deactivation. A file for each LA or VTR is created and maintained by the HQ Survey Team within the Office of Information Security (HS-92). Each file contains all the documentation for the review, approval, changes, and deactivation for the LA or VTR. The HQ Survey Team maintains pertinent information about each LA and VTR in the HQ Security Area Database.

NOTE: The Director, HS-92, approves LAs and VTRs based upon the requirements set forth in DOE directives. In cases where all security requirements cannot be met, an Equivalency or Exemption may be requested (see Chapter 16, Equivalencies and Exemptions).

HQ Implementation Procedures

Establishing a New LA or VTR:

When an HQ element determines that a new LA or VTR is required, the following actions must be taken:

- The element HSO submits to HS-92 a Security Area Request Package requesting an Advice and Assistance visit to prepare for the establishment of a new LA or VTR. The Security Area Request Package consists of a memorandum requesting assistance in establishing a new LA or VTR along with two attachments: a Security Area Request/Facility Information Worksheet and a blueprint/drawing of the proposed LA or VTR. Attachments 201-1 and 201-2 provide a sample memorandum and the Security Area Request/Facility Information Worksheet. The drawing can be a copy of a blueprint or a simple, hand-written sketch of the area.
- HS-92 forwards the Security Area Request Package to the HQ Survey Team within HS-92. The HQ Survey Team conducts the appropriate physical security review and walk-through of the proposed LA or VTR before providing an Advice and Assistance Report to the element identifying the physical protection measures needed. It is the element's responsibility to arrange for and complete any needed construction or other physical changes to the proposed LA or VTR.
- Requirements for Technical Surveillance Countermeasures (TSCM) services are determined based upon the activities that will take place within the proposed area. If the area requires TSCM services, the HQ Survey Team coordinates with the HQ TSCM Program Manager to obtain those services.
- The HSO notifies the HQ Survey Team by e-mail when the physical security upgrades are complete. The HQ Survey Team inspects the LA or VTR to verify that all physical protection requirements are met. The HQ Survey Team then provides a Security Area approval memorandum and "Security Area Approval Certificate" to

the requesting HQ element. A sample Security Area Approval Certificate is shown in Attachment 201-3.

- When an LA or VTR has been accredited, the Security Area Approval Certificate must be prominently displayed inside the area, preferably near the main entrance.

Establishing TLAs:

Occasionally, an organization may request to review classified information on a limited basis in a location not yet approved as an LA or VTR. If the proposed location, classified activity, and alternative protection measures establish that the classified information can be protected as it would in an approved LA or VTR, the Program's HSO may request approval of a TLA to review classified information up to but no higher than S/RD.

To request approval for a TLA, an HSO must complete a Security Plan for the proposed area. Attachment 201-4 provides a Sample Security Plan for TLAs that is used as a template for requesting a TLA. The Security Plan must be signed by the employee(s) who will be working in the TLA and the requesting HSO, and submitted to HS-92 for approval by the HQ CMPC Program Manager.

The request for the TLA is approved by HS-92 on a case-by-case basis after careful analysis of the information described in the Security Plan. If the analysis determines that the classified information can be protected as it would be in an approved LA or VTR, approval may be granted.

Maintaining LAs, VTRs, and TLAs:

After an LA, VTR, or TLA has been approved, two situations may affect its continued ability to remain accredited:

- Physical changes, such as adding or rearranging large items of furniture or equipment, may affect the integrity of the space.
- LAs, VTRs, and TLAs are approved for specific classified activities at specific classification levels and categories. If different classified activities must be performed or there is a change in the classification level or category of the classified matter to be handled within the LA, VTR, or TLA, a new survey and *Security Area Approval Certificate* is required.

In either case, the element's HSO submits a new Security Area Request Package, as described above, to HS-92. The memorandum will briefly state the nature of the modification to the LA, VTR, or TLA and have a Security Area Request/Facility Information Worksheet attached. HS-92 forwards the Security Area Request Package to the HQ Survey Team for action.

The HQ Survey Team conducts the appropriate physical security review and takes one of the following actions:

- If the security posture of the area is unaffected by the physical changes, no further action is required and a memorandum stating this fact is transmitted to the HSO of the requesting HQ element.
- If the security posture of the area is affected by the proposed physical changes, an Advice and Assistance Report identifying the required physical protection measures is transmitted to the HSO of the requesting HQ element. Once the HSO determines all work necessary to bring the area into compliance has been satisfactorily completed, the HQ Survey Team is notified by e-mail. The HQ Survey Team conducts a follow-up review or walkthrough of the area and issues a new Security Area approval memorandum and Security Area Approval Certificate that are transmitted to the requesting HSO. Once reaccruited as an LA, VTR, or TLA, the new *Security Area Approval Certificate* must be prominently displayed inside the area, preferably near the main entrance, and all superseded certificates destroyed or returned to the HQ Survey Team.

NOTE: If the physical changes affect the ability of the area to continue classified activities and no compensatory measures are feasible, the LA, VTR, or TLA must be deactivated. All classified activities must cease or be relocated to an accredited Security Area until identified physical protection measures have been implemented and the area re-approved.

NOTE: If the change in activities requires the Security Area to become a TSCM serviced area, the HQ Survey Team forwards the request to the TSCM Operations Manager for appropriate action; this may require the element's TSCM Officer to submit a new request following the procedures established in Chapter 9, Technical Surveillance Countermeasures.

Deactivating LAs, VTRs, and TLAs:

When an LA, VTR, or TLA is no longer required, all classified matter must be destroyed or relocated to another approved LA, VTR, or TLA, and all classified activities must cease. The HSO of the element takes the following steps to complete the deactivation:

- Submit a new Security Area Request Package, as described above, to HS-92. The memorandum will briefly state that an existing LA, VTR, or TLA requires deactivation and have a Security Area Request/Facility Information Worksheet attached. HS-92 forwards the Request Package to the HQ Survey Team for action.
- The HQ Survey Team conducts a review of the LA, VTR, or TLA to ensure all classified matter has been removed and all classified activities have been terminated. When satisfied, the HQ Survey Team transmits a memorandum to the element's

HSO approving the deactivation of the LA, VTR, or TLA. A copy of this memorandum is provided to the Office of Physical Protection (HS-91).

- When the HSO receives the deactivation approval memorandum, all intrusion detection and access control equipment can be removed. The HSO must confirm that removal has been satisfactorily completed and then e-mail the HQ Survey Team advising of that completion. The HQ Survey Team updates the HQ Security Area Database to reflect the deactivation and notifies HS-91 of these actions.

NOTE: The HSO must ensure that all classified matter has been properly disposed of or relocated and that all other classified activities have been terminated prior to the removal or deactivation of any security equipment.

NOTE: If the HSO is unsure of the appropriate course of action to complete the deactivation, the HQ Survey Team completes an Advice and Assistance Report providing specific guidance.

Points of Contact

For the names and contact information for those assigned the positions identified in this section, call (301) 903-9990 or (301) 903-1163.

Forms/Samples/Graphics

Sample Security Area Request Memorandum (see Attachment 201-1)

Security Area Request/Facility Information Worksheet (see Attachment 201-2)

Sample Security Area Approval Certificate (see Attachment 201-3)

Sample Security Plan for Temporary Limited Areas (see Attachment 201-4)

ATTACHMENT 201-1

Sample Security Area Request Memorandum

MEMORANDUM FOR (NAME), DIRECTOR
OFFICE OF INFORMATION SECURITY
OFFICE OF HEADQUARTERS SECURITY OPERATIONS
OFFICE OF HEALTH, SAFETY AND SECURITY

FROM: (NAME), HEADQUARTERS SECURITY OFFICER
NAME OF ELEMENT

SUBJECT: Security Area Request

The Office of _____ is requesting your assistance in establishing a Security Area in Room _____ at the _____ Building. Attached is a Security Area Request/Facility Information Worksheet identifying the various activities that may need to be performed within the Security Area. Also attached is a diagram of Room _____ and the surrounding area.

If you have any questions on this matter or need assistance in examining the proposed area, please contact me on x3 or 6- _____.

Or

The Office of _____ is requesting your assistance in modifying the Security Area currently located in Room _____ at the _____ Building. Attached is a Security Area Request/Facility Information Worksheet identifying the nature of the proposed changes in activities in Room _____. Also attached is a diagram of Room _____ showing the proposed relocation of the existing _____.
(furniture, safes, filing cabinets, etc.)

If you have any questions on this matter or need assistance in examining the proposed area, please contact me on x3-_____ or 6- _____.

Or

The Office of _____ is requesting your assistance in deactivating the Security Area in Room _____ at the _____ Building. Attached is a Security Area Request/Facility Information Worksheet identifying the various activities to be deactivated.

If you have any questions on this matter or need assistance in examining the proposed area, please contact me on x3-_____ or 6- _____.

Official Use Only Stamp

Attachment(s)

OFFICIAL USE ONLY (When filled in)

ATTACHMENT 201-2



Security Area Request/Facility Information Worksheet

ITEM	ACTION

All applicable item numbers 1-7 must be completed and attached to the Security Area Request Memorandum.

1. DATE:
NAME (HSO):
ALTERNATE:
ORGANIZATION:
BLDG/ROOM #:
PHONE:
EMAIL:
2. What action is requested? (Select one) **(MUST ATTACH FLOOR PLAN)**
☐ Change in Activities. ☐ Approve Security Area. ☐ Decertify an existing Security Area.
☐ Modification to Area. ☐ Security Incident. ☐ Advice and Assistance. ☐ Other.
3. If a change to an existing Security Area is being requested, briefly describe the changes.
4. Provide the following information regarding the Security Area location:
BUILDING (GTN, FORS, etc.): ROOM NUMBER: POC:
5. What type of area is being requested? (Select one)
☐ Limited Area ☐ Vault-type Room

6. What classified activities will be conducted in this area? (Select all that apply) For each activity requested indicate the highest classification level, category, and caveats as applicable. **If this is a request to change classified activities, complete the blocks describing what activities are currently approved then complete section 7 describing the change.**

Activities

☐ Reproduction of Classified Matter

Level: ☐ Top Secret (TS) ☐ Secret (S) ☐ Confidential (C)
Category: ☐ Restricted Data (RD) ☐ Formerly Restricted Data (FRD) ☐ National Security Information (NSI)
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Destruction of Classified Matter

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Faxing of Classified Matter, Auto-answer: ☐ Yes ☐ No

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Closed Storage of Classified Matter

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Open Storage of Classified Matter

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Classified Computer Processing

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Classified Discussions

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Use of Secure Telephone (select all that apply) ☐ Amplified ☐ Nonamplified ☐ RG Encryptor

☐ Video Teleconferencing (select one) ☐ Classified ☐ Unclassified

☐ Other Classified Amplified Sound: Explain:

7. What classified activities will be changed in this area? (Select all that apply) For each activity requested, indicate the highest classification level, category, and caveats as applicable.

Activities

☐ Reproduction of Classified Matter

Level: ☐ Top Secret (TS) ☐ Secret (S) ☐ Confidential (C)
Category: ☐ Restricted Data (RD) ☐ Formerly Restricted Data (FRD) ☐ National Security Information (NSI)
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Destruction of Classified Matter

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Faxing of Classified Matter, Auto-answer: ☐ Yes ☐ No

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Closed Storage of Classified Matter

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Open Storage of Classified Matter

Level: ☐ TS ☐ S ☐ C

Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Classified Computer Processing

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Classified Discussions

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Use of Secure Telephone (select all that apply) ☐ Amplified ☐ Nonamplified ☐ RG Encryptor

☐ Video Teleconferencing (select one) ☐ Classified ☐ Unclassified

☐ Other Classified Amplified Sound: Explain:

8. Additional Comments:

ATTACHMENT 201-3

Sample Security Area Approval Certificate

**Headquarters Facility
Security Area
Approval Certificate**

The following area

Forrestal Building, Room

Has been approved by the DOE Office of Headquarters Security Operations as a:

Vault-type Room

For the following classified activity

Open storage, processing, reproduction and destruction
of classified matter

up to and including the following classification level/category

Secret/Restricted Data

Approving Authority

Date

ATTACHMENT 201-4

Sample Security Plan for Temporary Limited Areas

**SECURITY PLAN FOR THE
(INSERT OFFICE NAME)
TEMPORARY LIMITED AREA (TLA)
LOCATED IN (INSERT FORRESTAL OR
GERMANTOWN) ROOM (INSERT ROOM NUMBER)**

I. PURPOSE

Currently, all (insert Office symbol) classified activities must occur within its designated Limited Areas. However, in order to perform (his/her) assigned responsibilities, (insert individual's name) requires access to classified information outside of the designated (insert Office symbol) Limited Areas. As such, (insert HSO's name, title and Office symbol) has requested (insert individual's name) located in (insert Forrestal or Germantown room number), be designated as a Temporary Limited Area (TLA) so that (he/she) can access classified information within (his/her) office. Classified activities within the TLA are limited to reviewing classified documents at the (insert classification level and category) level and below. This Security Plan sets forth (insert individual's name) specific Classified Matter Protection and Control (CMPC) responsibilities while reviewing classified documents within the designated TLA. These specific responsibilities are in addition to the overall CMPC responsibilities contained in DOE Order 471.6, *Information Security*, and the HQFMSP.

II. RESPONSIBILITIES

A. (Insert Individual's Name) shall:

1. Ensure that all individuals (DOE employees and visitors) who do not have an appropriate security clearance are escorted while they are in the TLA to ensure that they are not allowed access to classified information.
2. Ensure that only personnel with the appropriate security clearance and need-to-know are present when classified documents are reviewed in the TLA.
3. Ensure that classified matter is constantly attended, is under control, and is never left unattended until it is returned for storage in an approved security repository within an approved Limited Area.
4. Shut office door(s) and hang "Please Knock before Entering" sign(s) on exterior door(s) whenever classified documents are reviewed in the TLA.

5. Ensure that classified documents transported between (insert Office symbol) Limited Areas and the TLA are transported in designated candy striped envelopes or other approved methods for transporting classified matter within Headquarters facilities.
6. Ensure that only documents classified as (insert classification level and category) but cannot be higher than S/RD level and below are viewed in the TLA.
7. Ensure that all Controlled Articles in the TLA are handled in accordance with the HQFMSP Section 202, Controlled Articles.
8. Ensure that all classified material is returned to one of (insert Office symbol) approved Limited Areas and properly stored within a GSA-approved safe when finished working with classified documents in the TLA.
9. Ensure that an SF-701, Security Area Checklist, is posted in the room and is initialed at the end of each day classified information is reviewed within it. Initialing the SF 701 will certify that all classified matter has been removed from the room and properly secured in an approved Limited Area.

I acknowledge that I have read this Security Plan and understand my responsibilities for protecting classified information:

_____	_____	_____
Printed Name	Signature	Date

I verify that I have reviewed this Security Plan with the occupants of the proposed TLA and that they fully understand their responsibilities for protecting the classified information entrusted to them.

_____	_____	_____
Headquarters Security Officer	Signature	Date

Approved By:

_____	_____	_____
HQ CMPC Program Manager	Signature	Date

cc:
HQ Survey Program Manager, HS-92
HQ Physical Protection Program Manager, HS-91

This page intentionally left blank.

Section 202

Controlled Articles

This section describes the implementation at HQ facilities of the DOE Order 473.3 requirements on Controlled Articles. Controlled Articles are Government, company, and personally-owned electronic devices that are capable of recording or transmitting data (e.g., audio, video, radio frequency, infrared, and/or data link electronic equipment). At HQ, the Director, HS-90, is the official responsible for establishing the procedures for bringing Controlled Articles into and/or using them within an LA, TEMPEST Protected Area, or VTR. The decisions made by HS-90 are based on risk assessments of the devices and the areas where they will be used.

Personnel Exempt from the LA, TEMPEST Protected Area, and VTR Controlled Article Policies

When performing official duties, the following categories of personnel and their equipment are exempt from the LA, TEMPEST Protected Area, and VTR policies and procedures on Controlled Articles:

- HQ TSCM personnel
- HQ security personnel installing, maintaining, testing, or removing access control and intrusion detection systems
- The HQ Incident Command Team
- The HQ Protective Force
- Special Agents performing personal protection or investigative duties
- Emergency responders, such as Emergency Medical Technicians, firefighters, and police officers
- Personnel and physical security personnel conducting official business.

HQ Implementation Procedures

DOE Owned Electronic Devices:

DOE owned electronic devices configured by the HQ Office of the Chief Information Officer (OCIO) for day-to-day operation in HQ LAs, TEMPEST Protected Areas, or VTRs are permitted as long as they are used and maintained in accordance with the OCIO approved User Agreement, which specifies applicable security precautions (see Attachment 202-1.)

NOTE: No changes to the OCIO installed configuration are permitted.

Controlled Articles:

Other electronic devices capable of recording or transmitting data, including devices from OGAs and other DOE sites, are controlled as follows.

DOE Headquarters Controlled Articles Matrix

Controlled Articles and Uses	Area Type		Controls Required
	S/RD and below but NOT TEMPEST and Protective Distributions System (PTS) protected areas	TS, SAP, Sigma 14 or above, TEMPEST and Protective Distributions System (PTS) protected areas	
Non-transmitting devices (one-way pagers, radios, etc.)	Allowed		None
Wireless mice	Allowed		None
Medical devices (hearing aids, pacemakers, insulin pumps, cardiac monitors, etc.)	Allowed		Notify the elemental HSO or the HQ TSCM Team. The HQ TSCM Team conducts a safety review to ensure the device will not be adversely affected by security systems installed within the area.
Non-user programmable remotes	Allowed		NOTE: User programmable devices may be recognized by having a USB or other port which allows them to be connected to a computer for programming. Refer questions about specific remotes to the TSCM Team
User programmable, TV/audio-visual remotes	Controlled		Requires HQ TSCM Team approval.
Dedicated telephone and video teleconferencing equipment (VOIP, POTS, ISDN, etc.)	Controlled		1. Requires HQ TSCM Team approval. 2. Must remain in the OCIO installed configuration and be used in accordance with User Agreements.
Mobile, wireless capable Personal Electronic Devices, including cell phones, smart phones and personal digital assistants, laptop computers, music players, e-book readers, tablets, bluetooth earpieces/headsets, etc.	Controlled	Prohibited	Must be secured during classified conversations or processing. Acceptable methods of securing include: 1) Placed in aircraft mode (RF functions turned off) 2) Batteries removed 3) Turned off and stored in approved RF bag 4) Removed from the area. These devices must NOT be operated as wireless access points or hotspots.
Infrared (IR) wireless keyboards	Controlled	Prohibited	1. Requires HQ TSCM Team approval. 2. Must remain in the OCIO installed configuration and be used in accordance with User Agreements
Radio Frequency (RF) wireless keyboards	Prohibited		Prohibited at all times.
Making audio/video recordings	Prohibited		Prohibited at all times.

NOTE: Personnel in an LA, TEMPEST Protected Area, or VTR where these devices have been introduced must be cognizant of their surroundings before using the devices. It is the individual's responsibility to take into consideration classified activities that are occurring in adjacent areas.

Unapproved Recording/Use:

If any Controlled Article, regardless of ownership, is used in an unapproved manner or for an unapproved activity, either intentionally or unintentionally within an LA, TEMPEST Protected Area, or VTR, that device and any associated media is subject to confiscation by the element HSO or an official under the supervision of HS-90. If the device and associated media are found to contain classified information or determined to have been used in an unapproved manner, a Security Inquiry will be initiated. The confiscated item may be sanitized and/or destroyed, in accordance with applicable policy.

Photography in LAs:

Photography is not permitted in VTRs; LAs where Top Secret (TS), Sensitive Compartmented Information (SCI), or Special Access Program (SAP) information is stored, processed, or discussed; or in LAs that are TEMPEST Protected Areas. If it becomes imperative to use a camera in one of these areas, see "Requesting Authorization for Additional Controlled Articles," below.

A still camera may be used to photograph personal events such as birthdays, promotions, award ceremonies, etc. within LAs where TS, SCI, and SAP information is not stored, processed, or discussed or in LAs not designated as TEMPEST Protected Areas. HS-90 has government-owned cameras available at both the Forrestal and Germantown facilities. HQ personnel are encouraged to use the HS-90 cameras instead of personally-owned devices because the HS-90 devices have already been approved for use in LAs. HSOs can instruct personnel within their element on how to obtain a camera from HS-90.

Written approval from the element HSO is required before using a camera. See Attachment 202-2, for a *Sample Request to Use a Camera in a Limited Area*. These procedures must be followed to obtain permission for use of a camera:

- The request for approval must be signed by a Federal employee in a supervisory position.
- A digital camera must be used.
- Personally-owned cameras must undergo a TSCM inspection prior to taking pictures.
- All classified and sensitive matter must be removed from the camera's view before taking pictures.
- All classified computing within the LA must cease and computer monitors turned off.

- Pictures must not show any security signs that are not visible to the general public.
- Pictures must not show any access control or intrusion detection equipment or sensors that are not visible to the general public.
- Pictures must not show any planning or project calendars.
- An authorized occupant of the LA must be present during all picture taking.
- At the conclusion of the photography, the camera and/or its media must be handled as a classified "working paper" until reviewed by a Derivative Classifier.
- Photographs containing classified or sensitive information must be removed from the camera and/or its media by the HQ TSCM Team.
- The sanitized camera/media is returned to the photographer for picture printing or distribution.

NOTE: The purpose of the review by a Derivative Classifier is to verify that the photographs do not inadvertently contain any of the items listed above.

TSCM Inspections of Controlled Articles:

HQ personnel who are unsure that a device meets the definition of a Controlled Article are encouraged to request a technical inspection before introducing the device into a LA, TEMPEST Protected Area, or VTR. The request must be made through the Technical Surveillance Countermeasures Officer (TSCMO) within the program element. See Chapter 9, Technical Surveillance Countermeasures, for instructions on contacting the HQ TSCM Team.

Requesting Authorization for Additional Controlled Articles:

The Office Director requesting authorization for additional Controlled Articles or the use of selected device features must submit the request via memorandum to the Director, HS-90. The HSO of the requesting organization must be copied on the memorandum. The memorandum describes in detail the controlled article, the reason for its introduction or use, how long it will be needed, mitigations, who will have custody of the article, and what HQ facility and LA, TEMPEST Protected Area, or VTR will be affected. The memorandum must also include a risk assessment for using the article and a statement that the Office Director accepts the risk.

The approved request is valid for the specified time period, not to exceed one year. Renewal requests must be submitted at least 90 days prior to the expiration of the current approval to permit proper review.

Periodic Technology Review

The HQ TSCM Team conducts an annual technological review of the authorized controlled articles and their features to determine whether the HQ Controlled Article policy needs revised.

Points of Contact

For the names and contact information for those assigned the positions identified in this chapter, call (202) 586-8075 or (301) 903-1163.

To determine if a particular room or area is a TEMPEST Protected Area, call (301) 903-3957.

Forms/Samples/Graphics

Sample User Agreement (see Attachment 202-1)

Sample Request to Use a Camera in a Limited Area (see Attachment 202-2)



Attachment 202-1

Sample DOE Headquarters Desktop Webcam User Agreement

This User Agreement outlines individual user's responsibilities when utilizing webcams while conducting desktop Video Teleconferencing (VTC) sessions in HQ Security Areas specifically approved for desktop VTC sessions. This User Agreement must be completed by each individual user prior to utilizing approved webcam equipment and/or conducting VTC sessions. Upon execution of this agreement (initials and signature), the user acknowledges the following requirements:

Initials:

- _____ Only DOE TSCM approved webcam equipment, software and hardwired desktop computer hardware may be utilized. The use of non-government owned/sponsored equipment for VTC sessions is not authorized.
- _____ Undocked laptops, integral laptop cameras and Personal Electronic Devices (i.e., Blackberry's, iPhones, IPADs or similar devices) are not authorized for video teleconferencing (VTC) within the Security Area.
- _____ Prior to connecting the VTC equipment, the environment where the VTC session will be taking place must be sanitized to ensure that sensitive and classified information will not be exposed during the VTC.
- _____ Wireless VTC session are not authorized within Security Areas.
- _____ Webcam users must notify occupants in the surrounding areas that an unclassified VTC session will be taking place within the Security Areas and that sensitive and classified information could be compromised if discussed or brought into view during the session.
- _____ Signs must be conspicuously posted to warn individuals that unclassified VTC is occurring and to restrict sensitive and classified information and activities in the immediate area.
- _____ Immediately upon completion of the VTC session, the software application must be terminated and the webcam and associated VTC specific equipment (headphone, microphones, etc.) must be physically disconnected (i.e, physically unplugged) from the network system.
- _____ User has received training in the use of VTC equipment and software associated with the devices.
- _____ When not in VTC session use, equipment must be stored in a manner to easily identify that it is physically disconnected.
- _____ Approved USB hubs may be utilized to facilitate easier physical disconnection.

- _____ Recording of desktop VTC sessions is not authorized.
- _____ VTC software automatic answer capability must be disabled.
- _____ Failure to follow these requirements outlined in this user agreement will result in a security incident.

ACKNOWLEDGEMENT:

I certify that I have read, understand and will comply with the User Agreement for the Use of Desktop VTC/Webcam Devices within specifically approved DOE Headquarters Security Areas.

(Printed User Name)

(User Signature)

(Date)

cc: User's HSO

Note: This User Agreement will be maintained in the Security Area Approval file for the area containing the webcam.

ATTACHMENT 202-2

Sample Request to Use a Camera in a Limited Area

MEMORANDUM FOR (ENTER NAME OF HEADQUARTERS SECURITY OFFICER)
NAME OF ORGANIZATIONAL ELEMENT

FROM: NAME OF FEDERAL SUPERVISOR MAKING REQUEST
TITLE
NAME OF ORGANIZATIONAL ELEMENT

SUBJECT: Request to Use Camera within a Limited Area of the
_____ Facility

I hereby request permission to use a camera to take photographs at the _____ Facility. The following information is submitted:

Date Camera Will Be Used: Enter Dates.

Person Using the Camera: Enter Name of Person Using Camera.

Purpose of Photography: Why photography is needed.

Location of Photography: Where the camera will be used. (This cannot be a Vault-Type Room or a Limited Area approved for Top Secret, Sensitive Compartmented Information, Special Access Program information, or a TEMPEST Protected Area).

Equipment to be Used: Preferably a Government-owned digital camera. If a personally-owned camera is to be used, there must be a statement that the camera has been inspected by the HQ TSCM Team and approved for use.

I understand and will comply with the following security rules pertaining to use of a camera in a Limited Area.

- The area will be sanitized before any photographs are taken. This includes covering up or removing from view all classified and sensitive documents or matter. This will include the total shutdown of any classified computer system.
- Only still photographs are authorized.
- I will not photograph any Security Area signs that are not visible to the general public.
- I will not photograph any access control or intrusion detection equipment such as card readers, PIN pads, door locks, secure telephone devices, sensors, motion detectors, etc., that are not visible to the general public.
- I will not photograph any planning or project calendars.
- An authorized occupant of the area will be present during the entire photography session.

- At the conclusion of the photography, the camera and/or its media will be handled as a classified "working paper" and submitted to a Derivative Classifier (DC) for review prior to being used for any purpose.
- The camera and/or its media will be stored as classified matter until a DC determines the photographs are unclassified.
- In the event classified matter appears in any photograph, the camera and/or its media will be sanitized by the HQ TSCM Team.

If you have any questions on this matter, please contact me at (phone number of person making request).

APPROVED: _____

DISAPPROVED: _____

DATE: _____

cc:
Facility Security Manager
User's HSO

This page intentionally left blank.

Section 203

Classified Meetings in LAs and VTRs Approved for Classified Discussions

It is HQ policy to conduct classified meetings (including conferences, presentations, etc.) within LAs and VTRs that have been specifically approved for classified discussions. Not all LAs and VTRs are approved for classified discussions, and there may be restrictions on the level or category of classified information that may be presented within an LA or VTR. There may also be restrictions on the use of audio amplification devices within an LA or VTR. It is incumbent upon the meeting host and all participants to ensure the Area has been approved for discussions at the equal to or higher classification level and category than the matter being discussed and to comply with other technical requirements.

On occasion, a classified meeting must be held in an area that has not been approved for classified discussions. For procedures see Section 204, Classified Meetings Outside of LAs and VTRs Approved for Classified Discussion.

HQ Implementation Procedures

Classified Meetings:

Prior to holding a classified meeting in an LA or VTR, the participants must ensure that the area is approved for classified discussion at the level and category of the information to be discussed. A Security Certificate sign must be posted within each LA and VTR clearly indicating that the area is approved for classified discussion, the level and category of the classified information, and whether the Area is approved for “amplified discussion.” Amplified discussion refers to the use of microphones, polycoms, and speaker phones to discuss classified information within the area.

NOTE: Classified meetings involving the discussion of SCI or SAP information must always be conducted in LAs or VTRs specifically approved for these discussions.

If the Area is not approved at the requisite level and category of the classified discussion, an alternate location must be found. For procedures see Section 204, Classified Meetings Outside of LAs and VTRs Approved for Classified Discussion.

When a classified meeting is scheduled within an LA or VTR approved for classified discussions, the date, time, location, discussion topic, and other details of the meeting can be openly announced.

If DOE field personnel or employees of OGAs are scheduled for a classified meeting at a HQ facility, they may need to pass their security clearances through the Office of HQ Personnel

Security Operations (HS-93). See Section 306, Passing Clearances for Classified Meetings and Visits, for instructions on how to pass security clearance information.

The host of the classified meeting must ensure that:

- All participants have the requisite security clearance and “need to know”.
- All Controlled Articles are removed beyond audible range and have their batteries removed, or must be turned off and placed in an approved Radio Frequency (RF) container (see Section 202, Controlled Articles).
- The classification level and category of the discussion are announced at the start of the meeting.
- A sign is visible to all participants indicating the classification level and category of the information presented during the meeting.
- All presentations given during the meeting bear the proper classification markings.
- Note taking is prohibited unless arrangements are made to protect all notes until they have undergone a classification review.
- All classified matter is properly protected during the meeting.

NOTE: Notify the TSCM Team when a Top Secret discussion or meeting is planned for an LA or VTR not approved for Top Secret discussions. The TSCM Team must be notified before such discussions occur.

Points of Contact

For names and contact information for those occupying the information security, personnel security, and TSCM positions identified in this section, call (301) 903-3510 or (301) 903-1163.

Section 204

Classified Meetings Outside of LAs and VTRs Approved for Classified Discussions

On occasion, the number of meeting participants exceeds the capacity of the approved area or there may not be an approved meeting area available. An unapproved area can be used for a classified meeting, providing certain security protection requirements and administrative measures are met. This section describes the procedures and security measures that must be met to ensure classified information is protected when discussed in an unapproved area.

This section does not apply to classified meetings held at the facilities of OGAs.

HQ Implementation Procedures

Classified meetings scheduled outside an LA or VTR must be approved by the TSCMO of the HQ element hosting the meeting. The TSCMO must contact the TSCM Operations Manager (TSCMOM) to identify the necessary protective measures.

TSCMOs can approve occasional classified discussions and meetings up to the S/RD level outside of approved LAs or VTRs within the Forrestal and Germantown buildings.

When scheduling a classified meeting outside of an approved LA or VTR, all publicity/notification documents, messages, or e-mails must be handled in accordance with *TNP-32, Classification Guidance for Classified Meeting Locations at DOE/NNSA or DOE/NNSA Contractor Sites or Facilities (U)*.

NOTE: TNP-32 is not included in HQFMSP because it is an Official Use Only document. A copy can be obtained by the element HSO through the HSO Program Manager. The HSO Program Manager can be contacted as indicated in the Points of Contact subsection at the end of this section.

If DOE field personnel or employees of OGAs will be attending a classified meeting at an HQ facility, they may need to pass their security clearances through HS-93. See Section 306, Passing Clearances for Classified Meetings and Visits, for instructions on how to pass security clearance information.

Once the meeting is approved, the TSCMO must coordinate with the host of the meeting to ensure that:

- All participants have the requisite security clearance and “need to know.”

- All Controlled Articles must be removed beyond audible range and have their batteries removed, or must be turned off and placed in an approved RF container (see Section 202, Controlled Articles).
- The area used to conduct the classified meeting must provide acoustical isolation in such a way that classified information is not advertently disclosed. Acoustical isolation can be addressed by a TSCM evaluation of the room, administrative procedures, or combination of both.
- The volume level of approved electronic equipment used in classified presentations (e.g., video cassette/DVD player/computer monitor volume, TSCMOM-approved portable public address systems using hardwired microphones, etc.) must be set so voices are not discernible outside the conference area.
- Public address systems (other than life-safety) permanently installed within the area of the classified discussion are not to be used without specific approval of the TSCMOM. If the TSCMOM does not approve use of these systems, they should be completely disconnected during the classified discussion. Wireless microphones must be disabled if stored within the conference area. The TSCMOM should verify that all these actions are completed.
- The room must have controlled access by the host, either through a locking mechanism or someone physically controlling access to the room.
- Information being presented must be visually protected so that no one outside the area or just entering the area can see it.
- The classification level and category of the discussion is announced at the start of the meeting.
- A sign must be visible only inside the room indicating the classification level and category of the information presented.
- All presentations must bear the proper classification markings.
- No discussions may take place within the hearing range of unauthorized persons.
- All doors and windows are closed and secured during classified presentations and discussions.
- Note taking is prohibited unless arrangements are made to protect all notes until they have undergone a classification review.
- All classified matter is properly protected during the meeting.
- All telephones, speaker phones, etc., must be physically disconnected from the telephone and electrical power removed.

- When classified meetings occur in an area with unclassified Video Teleconferencing (VTC) capabilities, all VTC connections must be (electric, data, etc.) physically disconnected from the network.
- All unclassified laptops must have microphones physically disabled.
- If the conference room is equipped with Wireless Access Point (WAP) or WiFi, those functions must be disabled prior to the start of the meeting.

The HQ element hosting the meeting is responsible for any costs incurred for these security requirements.

For multi-day meetings and conferences, the TSCMO must coordinate with the HQ protective force to seal all entrances and conduct security checks on the area used for the classified meeting. The TSCMO must also arrange for opening the area each day of the meeting or conference.

Points of Contact

For the names and contact information for those occupying the information security positions identified in this chapter, call (301) 903-9990.

For the names and contact information for those occupying the TSCM positions identified in this chapter, call (301) 903-3510.

To contact the HSO Program Manager, call (301) 903-1163 or (301) 903-2644.

This page intentionally left blank.

Section 205

Secure Telecommunications Equipment (Phones)

Secure Telecommunications Equipment (STE) and vIPER Universal Secure Phones (vIPERs) are Communications Security (COMSEC) equipment. HQ policies and procedures for their installation, configuration, use, and deactivation are governed by the National Security Agency (NSA). The HQ COMSEC Program, which includes all STE and vIPER services, guidance, and assistance, is managed by the Technical Security Program within the Office of Corporate Security Strategy, Analysis, and Special Operations (HS-1.2).

The COMSEC program ensures the secure transmission of classified and sensitive information. STEs and vIPERs encrypt telephonic and facsimile transmissions of classified information; therefore, these devices must be used when telephonically discussing classified information or transmitting classified information via a facsimile machine.

HQ Implementation Procedures

Requesting STE and vIPER Services:

STE and vIPER custodians may not connect, disconnect, reconfigure, transfer, or relocate these devices on their own. These actions may only be performed by authorized personnel affiliated with the HQ Secure Phone Group. The HSO within each HQ element must be advised when STE service is needed. All service requests, which include requests for installation, reconfiguration, relocation, transferring to another user, troubleshooting, and deactivation, must be prepared by the elemental HSO and transmitted via email to the HQ Secure Phone Group for action.

To take the requested action, the HQ Secure Phone Group needs (at a minimum) the following information:

1. For installation of a STE or vIPER for a new user:
 - a. New user's name.
 - b. Room number and name of HQ Building. Attach a scanned copy of the document showing that the room where the STE or vIPER will be located is approved for classified discussions (preferably the Security Area Approval Certificate provided by the Headquarters Survey Team). Note that COMSEC personnel do not install a STE or vIPER in a room that is not approved for classified discussions.
See the sub-section Residential Installation of STEs and vIPERs, below, for instructions for installing a STE or vIPER in a private residence.
 - c. Contact number for new user.
 - d. Organizational routing symbol for new user.

- e. Key level required and any special needs, such as the need to talk to North Atlantic Treaty Organization (NATO) countries, other countries via the Combined Communications Electronic Board (CCEB), or SCI.
 - f. If the request is for a STE to be connected to a facsimile machine or computer, the HSO must provide documentation of all approvals in place for a secure fax.
 - g. When the new installation needs to be done (date or range of dates and best time of day).
2. For transfer of a STE or vIPER to a different user, the e-mail should include:
- a. Previous user's name.
 - b. New user's name.
 - c. Contact numbers for previous and new users.
 - d. Organizational routing symbol for new users.
 - e. Room number and building location of previous and new users. If the transfer will be made to a different room, attach a scanned copy of the document showing that the room where the STE or vIPER will be located is approved for classified discussions (preferably the Security Area Approval Certificate provided by the HQ Survey Team). Note that COMSEC personnel will not install an STE or vIPER in a room not approved for classified discussions.
 - f. STE or vIPER serial number. The STE serial number is found on the back of the STE and starts with the letters "STE A" or "STE B" followed by a 10 digit number; the vIPER serial number is also on the back of the phone, but starts with the letters "GSN: FNBE", the numbers "21," and then an additional 8 digit number.
 - g. The new key level required and any special requirements, such as need to discuss NATO, CCEB, or SCI information.
 - h. When the transfer needs to take place (date or range of dates).
3. For removal of a STE or vIPER, the e-mail should include:
- a. Username
 - b. Room number
 - c. Contact number
 - d. STE or vIPER serial number (refer to item 2f, above)
 - e. When the removal needs to take place (date or range of dates).

Once the e-mail is prepared, it should be sent to: HQSecurePhone@hq.doe.gov.

Residential Installation of STEs and vIPERs:

If an HQ element identifies the need, an employee may have a STE or vIPER installed at his/her private residence *for the purpose of listening only*. ***Discussing classified information on a STE or vIPER at a residence is strictly prohibited.***

The HQ element where the user is assigned must pay for a vIPER installed at a private residence.

To request the installation of a STE or vIPER at a private residence, the HSO must send an e-mail to the HQ Secure Phone Group at HQSecurePhone@hq.doe.gov and have the user complete a Residential vIPER Telephone Equipment Security Plan (see Attachment 205-1). The HSO must then submit the completed plan to HS-92 by:

- Intra-office mail to HS-92, Attention: HQ Survey Team, Room F-316, Germantown, or
- Scan it electronically, attach it to an encrypted e-mail, and transmit it to “HS-92 Operations” in the Microsoft Outlook Global Address List.

Once HS -92 receives the signed user agreement they provide a copy to the HQ Secure Phone Group to make arrangements to install the STE or vIPER. A file of current Residential STE/vIPER user agreements is maintained by the HS-92 Survey Team.

Points of Contact

For the names and contact information for the HQ Secure Phone Group, call (301) 903-5062.

To contact the HQ Secure Phone Group by e-mail, use HQSecurePhone@hq.doe.gov.

To contact HS-92 by phone, call (301) 903-9990.

To contact HS-92 by e-mail, use the title “HS-92 Operations” in the Microsoft Outlook Global Address List.

Forms/Samples/Graphics

Residential vIPER Telephone Equipment Security Plan (see Attachment 205-1)

ATTACHMENT 205-1

Residential vPer Telephone Equipment Security Plan

The following security requirements are in effect for any residential installed vPer.

_____The purpose for the vPer instrument in a residential installation is to enable the authorized residential user to receive audible classified information in an **Emergency Situation**. Conversations on the vPer telephone at the residential site should be limited to brief, **UNCLASSIFIED** responses, e.g., yes/no answers, by the authorized residential user. The risk associated with passively listening to classified information at the residence is minimal; the risk associated with actively discussing classified information at the residence is very high, especially for that of senior management personnel. As such, the discussion of classified information is strictly prohibited and is in direct contravention to DOE Orders and National directives. Authorized discussion of classified information must be accomplished within, approved security areas located in U.S. Government facilities.

_____Maintenance on your residential vPer by anyone other than authorized DOE personnel is strictly prohibited. All installations, changes, removals, and maintenance will be performed only by the COMSEC Custodian.

_____The vPer instrument must be installed in a room in which the user can be isolated by physical means from other occupants in the residence while using the vPer telephone equipment. When the terminal is in use in the encrypted mode, the doors and windows to the room shall be closed and only individuals with the appropriate clearances and need-to-know shall be allowed within and/or in close proximity to the room.

_____No other type telephone instrument may be located in the same room as the vPer instrument. The vPer instrument must be separated from other electronic devices in accordance with the approved TEMPEST Plan for the residence.

_____The PIN number for the vPer must be memorized (it cannot be written down).

_____The vPer instrument must not be moved within the residence or transported out of the residence without the approval of the Headquarters Security Officer and the Communications Security Custodian.

_____, The classification level to which the vPer instrument is keyed should not be disseminated to anyone within the residence or to anyone without the need-to-know.

_____As communication with another Secure Telephone is established, the residential vPer authorized user can identify the distant end user and the authorized classification level on the instrument's liquid crystal display (LCD). The distant end user will see "Residence, USDOE, DOE Official" scroll on its vPer screen followed by "Residence" and a classification level. The LCD on the residential vPer instruments will display the lower of the two classification levels to which the secure communication instruments are authorized to transmit.

_____Any notes taken during classified use of the vPer instrument should be unclassified. However, any and all notes taken concerning the substance of the secure communication must be protected as classified until reviewed by a Derivative Classifier. If determined to contain classified information the notes must be appropriately marked and protected, or properly destroyed as classified matter.

Acknowledgement by the vPer authorized user:

(printed name)

(signature)

(date)

OFFICIAL USE ONLY

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 712), exemption number category: Exemption 7 - Law Enforcement.
Department of Energy review required before public release.
Name/Org: _____
Date: _____

OFFICIAL USE ONLY

Chapter 3 Revision History: Revisions by date (Newest to oldest):**May 7, 2020:**

- Added language that Chapter 3 only applies to Headquarters
- Added applicable Federal Regulations
- Update Clearance Request and Processing section to include new requirements
- Added the utilization of eCAR and CATS
- Updated Applicant Tracking System
- Updated Reporting Requirements
- Updated Classified Visits
- Added HSPD-12 processing (information transferred from Chapter 1 and updated to include new requirements)
- Removed Badge Processing (SF-312)
- Updated and changed links
- Updated and changed contacts and related contact information

Chapter 3

Personnel Security

This chapter covers the security procedures adopted by DOE HQ to implement the requirements of the following Federal regulations and DOE directives:

- Privacy Act of 1974
- Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*
- DOE Order 206.2, *Identity, Credential, and access Management (ICAM)*
- U.S. Office of Personnel Management memorandum, dated July 31, 2008, from Linda M. Springer, subject: Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12
- Title 10, Code of Federal Regulations, Part 707
- Title 10, Code of Federal Regulations, Part 710
- Title 48, Code of Federal Regulations, Part 952.204-2
- Security Executive Agent Directive (SEAD) 4, *National Security Adjudicative Guidelines*
- SEAD 7, *Reciprocity of Background Investigations and National Security Adjudications*
- DOE Order 470.4B, *Safeguards and Security Program*
- DOE Order 472.2, *Personnel Security*
- DOE Order 475.1, *Counterintelligence Program*

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

- Section 301 covers the procedures for acquiring new security clearances.
- Section 302 covers other actions that affect security clearances such as transfers, extensions, upgrades, downgrades, and cancellations.

- Section 303 covers the requirements for reporting information that may affect the retention of a security clearance.
- Section 304 covers the procedures for accessing the Electronic Questionnaire for Investigations Processing (e-QIP) and completing the e-QIP process required for those seeking a security clearance and an HSPD-12 security badge.
- Section 305 covers the annual process that HSOs must complete to ensure cleared personnel in their element are reinvestigated at the proper interval to verify the continued need for their security clearances.
- Section 306 covers procedures for passing security clearance information to organizations hosting classified meetings.
- Section 307 covers the process for obtaining a HSPD-12 credential for employees who do not require a security clearance. If a security clearance is required, follow the guidance in Section 301.

Please note there are a total of seven Cognizant Personnel Security Offices (CPSO) across the DOE complex that handle security clearance related matters. The CPSO for HQ is the Office of Headquarters Personnel Security Operations (AU-43). The information in this Chapter applies only to security clearance requests that will be processed by AU-43 as well as security clearances that have been granted by AU-43. It does not apply to DOE Federal or contractor employees physically located at a HQ facility whose security clearance is being processed by or has been granted by another CPSO.

Section 301

Acquiring New Security Clearances

Certain HQ Federal and contractor employees must have security clearances because their jobs require them to have access to classified matter. A security clearance is a determination by the United States Government that a person is eligible for access to classified matter. To obtain a security clearance, a Federal investigative agency must conduct background investigations before employees or contractors are issued security clearances.

NOTE: An equivalent term for “security clearance” is “access authorization;” however, the term “access authorization” has several different meanings at DOE HQ. To avoid confusion, the term “security clearance” is used throughout this section instead of “access authorization.”

Five types of security clearances exist at DOE: a Q clearance, L clearance, TS clearance, S clearance, and C clearance. An employee’s security clearance is determined by the work he/she will perform, his/her position description (if a Federal employee), or the terms of the contract (if a contractor employee).

Security classification is cast into three levels:

- **Confidential:** The unauthorized disclosure of Confidential information or material can cause measurable damage to national security. The vast majority of military personnel are given this very basic level of clearance. This level is reinvestigated every 15 years.
- **Secret:** The unauthorized disclosure of Secret information can cause serious damage to national security. This level is reinvestigated every 10 years.
- **Top Secret:** The unauthorized disclosure of TS information or material can cause grave damage to national security. This level is reinvestigated every 5 years.

In addition, three categories of classified matter are identified: Restricted Data (RD), Formerly Restricted Data (FRD), and National Security Information (NSI). The employee must have a security level clearance consistent with his/her assignment. Common combinations are reflected in the table, below:

Employee Accesses Authorized Based on DOE-Issued Security Clearances

Q	Top Secret	L	Secret	Confidential
TSRD				
SRD				
CRD		CRD		
SNM CAT I - III		SNM CAT II & III		
TSNSI	TSNSI			
SNSI	SNSI	SNSI	SNSI	
CNSI	CNSI	CNSI	CNSI	CNSI
TSFRD	TSFRD			
SFRD	SFRD	SFRD	SFRD	
CFRD	CFRD	CFRD	CFRD	CFRD

This section covers many of the possible variations, but requires close and continuing coordination between those responsible for sponsoring and requesting security clearances and AU-43 to ensure that clearance requests are processed in an effective and timely manner.

HQ Implementation Procedures

Preliminary Considerations:

Before an individual is processed for a security clearance, proper documentation must be in place.

1. Federal Employees – The Position Description (PD) of Federal employees must specify the proper security clearance level to be processed for the assignment. If the employee's PD does not specifically state that a security clearance is required, then that employee cannot be processed for a security clearance.
2. Contractors – The company employing contractors who require a security clearance must possess a Facility Clearance issued by DOE and a contract requiring the proper security clearances for its employees. AU-43 personnel verify that the employers of

contractors have the necessary background documentation in place. If not, the application cannot be processed.

NOTE: The procedures for a contract company to acquire a DOE Facility Clearance are described in Chapter 4, Foreign Ownership, Control or Influence; Facility Clearance; and Classified Contract Registration.

Who Does What?

The individual's status as a Federal or contractor employee and other considerations determine who is responsible for security clearance application assistance:

1. Newly Hired or Existing Federal Employees – Each HQ element has established its own procedure for assisting Federal employees requiring a security clearance. In some elements, a Human Capital (HC) specialist assists the employee; in other elements, it is the HSO. The proper official contacts the employee when it is time to apply for a clearance.
2. Other Government Agency Detailees – Federal employees employed by another department or agency, such as the Department of Defense, who are detailed to work at DOE must work with the HSO of their sponsoring element to complete the required paperwork for a security clearance.
3. Intergovernmental Personnel Act (IPA) Employees – A person employed by DOE under an IPA agreement is in a unique category. He/she is hired under a contract-like agreement administered by HC. When hired, he/she has the authority of a Federal employee. For the purpose of security clearance processing, IPA employees are treated the same as contractor employees, except HC arranges for a drug test and furnishes a copy of the IPA Agreement (prepared by HC) to include in the security clearance request package. Consequently, HSOs should consult with AU-43 to specify what other documentation may be needed.
4. Newly Hired or Existing Contractor Employees – New or existing HQ contractor employees requiring security clearances must work with their Facility Security Officer (FSO). The FSO coordinates with the element's HSO to obtain the required signatures and submit the security clearance request package.
5. Key Management Personnel (KMPs) – KMPs are top officials with the authority to affect the organization's policies or practices in security activities of a contract performing classified work for DOE. At a minimum, KMPs must include the senior management official responsible for all aspects of contract performance and the designated facility security officer (FSO). KMPs must have a DOE security clearance, commensurate with the classified work being done by their company, in accordance with the DOE Foreign Ownership, Control, or Influence (FOCI) Program. KMPs that do not access classified information may be excluded (exclusion resolution).

AU-42 provides the names of the KMPs to the HSO of the HQ element that is using the company to perform the classified work. AU-42 also notifies the company's FSO of the security clearance their KMPs require and the HSO who will process their security clearance documentation. For contractors holding multiple contracts with other organizations, AU-42 determines the contract requiring the highest security access level via the Safeguards and Security Information Management System (SSIMS). The HQ element with the contract requiring the highest security access level becomes the element responsible for sponsoring KMP clearances.

6. All Others – There are other categories of people who might require a DOE security clearance. In the past, these have included Federal or local law enforcement agency personnel participating in joint task forces, members of Presidential or Congressional commissions, U.S. Congressmen/women representing districts with DOE facilities, governors and/or lieutenant governors of states with DOE facilities, and other government agency employees. When these special situations occur, the HSO of the affected HQ element must consult with AU-43 to determine the required documentation and who will sponsor the security clearance.

Requesting a Security Clearance:

Processing an application for a security clearance involves several steps and multiple officials:

1. Determining Sponsorship – All applicants for a security clearance must have a sponsor. The sponsor is the HQ element assigning the classified work. The Federal employee's PD must include the need for the work specified, as well as the proper security clearance level. For contractors, the contract between the HQ element and the contractor must detail the need for the classified work. The assigned sponsor is responsible for initiating all clearance related actions including reinvestigations, security refresher briefings, etc.
2. Sponsorship in USAccess
 - a. **Federal and IPA Employees:** The HC specialist sponsors and enrolls the applicant in USAccess. See Section 307, "Requesting a HSPD-12 Credential," items 1 and 2 for more information.
 - b. **Contractor Employees:** The HSO coordinates with the designated person in his/her element to sponsor and enroll the contractor into USAccess. See Section 307, "Requesting a HSPD-12 Credential," items 1 and 2 for more information.

The applicant must enroll in USAccess to have fingerprints captured before the clearance request is submitted to AU-43. For information on how to locate a USAccess Credentialing Center, how to schedule an appointment, and the required documents for enrollment, go to <https://www.fedidcard.gov/>

3. Obtaining Documentation from the Applicant

- a. **Federal Employees:** The element's HC specialist or HSO must acquire the necessary documents from the applicant, including:
 - DOE F 5631.18, *Security Acknowledgement*
 - OF-306, *Declaration for Federal Employment* (HC collects this form)
 - A copy of the applicant's current resume
- b. **Contractor Employees:** The contractor's FSO must obtain and prepare the required application documentation from the employee, including:
 - DOE F 5631.18, *Security Acknowledgement*
 - DOE F 473.2, *Security Badge Request* (if applicable)

4. Contractor Pre-employment Screening – The contracting company is required to conduct pre-employment screenings and evaluate the results in accordance with their personnel policies. This requirement, as well as the drug testing requirement described below, is defined in 48 CFR 904.

The pre-employment screening must include:

- Verifying the applicant's educational background, including a high school diploma obtained within the past 5 years, and degrees or diplomas granted by an institution of higher learning
- Contacting the applicant's employer(s) of the past 3 years
- Contacting the applicant's listed personal references
- Conducting local law enforcement checks when such checks are not prohibited by state or local law or regulation
- Conducting a credit check
- Conducting other checks appropriate for the applicant.

The FSO assembling the applicant's security clearance application package must provide the pre-employment screening results in a letter (see Attachment 301-1) to AU-43 stating that:

- A pre-employment review was conducted
- The date(s) the review was conducted
- The identity of each entity providing information about the applicant
- Certification that the information was reviewed by the employing contractor in accordance with all applicable laws, regulations, and Executive Orders,

including those governing the processing and privacy of an applicant's information collected during the review

- Certification that all information collected during the review was reviewed and evaluated in accordance with the contractor's personnel policies.

DOE can reimburse contractors for the cost of pre-employment screening of security clearance applicants.

5. Drug Testing – Both Federal and contractor employees applying for a security clearance must undergo a urinalysis drug screening for the use of illegal substances. Drug test results must be dated within 60 calendar days of the date the applicant certifies his/her SF-86.

- a. **Federal and IPA Employees:** The HC Specialist coordinates the drug test for applicants and receives the results which are included in the applicant's security clearance request package.
- b. **Contractor Employees:** Contractors must establish their own drug testing programs, as required by 10 CFR 707, *Workplace Substance Abuse Programs at DOE Sites*. The contractor must arrange for the security clearance applicant to take a drug test and must also provide the results to the FSO who is preparing the applicant's security clearance request package.

Drug test results must be included in a letter to AU-43. Results of the contractor's drug screening are reported in one of two ways: an attached copy of the laboratory report showing the results of the drug test, or a statement within the letter attesting to the date, location, and results. The sample letter in Attachment 301-1 may be used to report drug test results.

DOE can reimburse contractors for the cost of drug testing security clearance applicants.

NOTE: DOE does not process security clearance requests from any applicant who tested "positive" for illegal drugs. The applicant/sponsor must wait at least one year before resubmitting a security clearance application.

6. Other Documentation Required

- a. **Federal Employees:** A copy of the employee's PD and the Position Designation Record (PDR) must be obtained from HC and included with the clearance request. The PDR must be signed.

- b. **Contractor Employees:** A copy of the PDR must be included with the clearance request. The PDR does not have to be signed at this time. This may change in the future.
7. Justification for the Security Clearance – The element’s HC specialist or HSO must ensure that the need for the security clearance is satisfactorily justified. The justification must specify the highest classification level and category of matter to be accessed and detail the duties requiring access at that level. PDs will not be accepted as justification for a security clearance.

NOTE: A justification such as “The applicant is a rocket scientist and will need a Q in order to perform her duties” is inadequate and will not be accepted by AU-43. A proper justification would be: “The applicant will support the Office of Energy Science in the development of cold nuclear fusion. This will require unescorted access to LAs, where applicant will come in contact with classified information or materials up to the S/RD level.”

8. e-Clearance Action Request (eCAR) system – eCAR is a part of the NNSA developed Clearance Action Tracking System (CATS). All DOE CPSOs use CATS to process security clearance requests. All requests for security clearances must be submitted to AU-43 via eCAR. Access to eCAR is attained by completing PERSEC F 5630.27, *Clearance Action Tracking System* (see Attachment 301-2). A copy of the form can be obtained by emailing AU-43 at personnelsecurity@hq.doe.gov. Return the completed and signed PERSEC F 5630.27 to AU-43 at the same email address for review and approval. AU-43 forwards the approved form to the CATS Support team for processing. When the account is created, a representative from the CATS Support team will contact the requester with instructions for logging into eCAR.
8. Submitting a Request for a Security Clearance – Once all of the requirements in the paragraphs above have been met, the HC Specialist or HSO creates a request in eCAR. As information is entered into eCAR, the system automatically populates PERSEC F 5633.33, *Clearance Action Request* form with the data. A template of this form (see Attachment 301-3) is available that matches the fields in eCAR so that individuals entering data into the system will have all of the information required. Contact AU-43 at personnelsecurity@hq.doe.gov for a copy of the fillable template. AU-43 will accept either a signed and completed PERSEC F 5633.33 or Template 5633.33. The completed form should be uploaded as an attachment along with the rest of the required documents which are listed below:

Federal Employees:

DOE F 5631.18, *Security Acknowledgement*
PD and OF-8
PDR
Drug Test Results

Current resume

Contractor Employee:

DOE F 5631.18, *Security Acknowledgement*

PDR

Drug Test Results

Pre-employment checks/letter

DOE F 473.2, *Security Badge Request* (if applicable)

8. AU-43 Review of Documentation Submitted – AU-43 reviews the documents to verify they are complete. If the documents are filled out incorrectly, information is missing or discrepant, or the required documentation is not attached, AU-43 rejects the eCAR request and sends an email to the submitter explaining the corrections needed. When the corrections are made, the documents are resubmitted to AU-43 via eCAR.

NOTE: AU-43 is authorized to refrain from taking action on security clearance requests involving persons on parole or probation for a felony offense until they have completed their period of parole or probation.

When the documents are complete, the applicant will complete the SF-86, Questionnaire for National Security Positions via e-QIP.

9. e-QIP Processing – See Section 304 of HQFMSP for information regarding e-QIP processing.
10. Preliminary Approval – AU-43 will Preliminary Approve an employee if both the fingerprints and the SF-86 are clear of any derogatory information. USAccess will be updated to reflect the Preliminary Approval and the HSPD-12 credential will print at that time. If AU-43 is unable to Preliminary Approve, the employee will continue to use the Local Site Specific Only (LSSO) badge unless otherwise directed. An email will be sent to employee, HSO, and the Badge Office informing all parties of the Preliminary Approval and extension of either the LSSO badge or HSPD-12 credential. Please refer to Chapter 1, Physical Security, for additional information on badges.
11. Background Investigation – Once the e-QIP process is completed, the applicant's information is automatically forwarded to the Defense Counterintelligence and Security Agency (DCSA). DCSA provides the results of the background investigation to AU-43 for review.
12. Grant of Security Clearance & Badging – AU-43 reviews the applicant's investigative report and provides unbiased adjudication in accordance with SEAD 4, *National Security Adjudicative Guidelines*. If the background investigation is favorable, AU-43 grants the security clearance and updates CATS which in turn updates the Central Personnel Clearance Index (CPCI) database. Notification of the clearance grant is made to the HQ badge office, HC for Federal employees, and the HSO for contractor employees. If a

badge card is included for the contractor employee, AU-43 forwards it to the badge office. USAccess will be updated with the appropriate clearance level and a new HSPD-12 badge will be printed. Please refer to Chapter 1, Physical Security, for additional information on badges.

AU-43 cannot approve applicants with unresolved security concerns as identified by the National Security Adjudicative Guidelines. Instead, the application must be processed through the Administrative Review procedures contained in 10 CFR 710, as described in the subsection below.

Reciprocity:

A security clearance can be granted reciprocally when an applicant has an active security clearance granted by another Federal agency, or the applicant has been determined eligible for a security clearance by another Federal agency. In addition, the applicant must have a favorably adjudicated background investigation completed at the level to support the security clearance requested and within the required timeframe.

Reciprocity does not apply if an existing security clearance or eligibility cannot be verified, the applicant's most recent favorably adjudicated background investigation is out of scope or does not support the level of clearance requested, or AU-43 is in possession of derogatory information that has not been covered by the applicant's most recent background investigation.

Interim Access Authorization (IAA):

Under exceptional circumstances and when such action is clearly consistent with Departmental and national interests, an uncleared applicant may, pending completion of the appropriate background investigation, be permitted to have an interim security clearance. The Federal Head of Element must prepare a memorandum request to the Director, AU-40, that includes a detailed justification explaining why:

- A serious delay of, or interference in, to an operation or project essential to a DOE program will occur unless the person for whom the IAA is requested is granted access to classified information or Special Nuclear Material (SNM) before completion of the normal security clearance process, and
- The services of a qualified person who is currently cleared to access the necessary classified information or SNM cannot be obtained.

The applicant must complete all the steps required for a security clearance as noted above before an interim security clearance request will be processed by AU-43. Requests submitted with justifications that do not meet the requirements as specified above will be returned with no action taken by AU-43.

It is important to note that the submission of a request for an interim clearance does not guarantee the applicant will be granted one. All interim clearance requests undergo a rigorous review process. Both the applicant and Federal Head of Element will be notified in writing of the final decision.

NOTE: Interim security clearances may be extended or transferred for another purpose within the DOE complex only.

Administrative Review (AR) Processing:

AU-43 initiates the AR process, as outlined in 10 CFR 710, when an individual's eligibility for a security clearance has been suspended or cannot be granted because of unresolved security concerns. Individuals being processed under 10 CFR 710 are provided a notification letter from AU-43, which includes a summary of the security concerns. The individuals are also provided written instructions by AU-43 on the information they need to provide in order to resolve the security concerns. At this point, the individual has the option to have the substantial doubt regarding eligibility for access resolved in one of two ways: a decision by the Manager, without a hearing, on the basis of the existing information in the case; or by personal appearance before an Administrative Judge.

When an individual's security clearance is denied or revoked following AR, granting or reinstating security clearance eligibility is reconsidered only under the following circumstances:

- When a minimum of one year has elapsed since the date of the Manager's, Administrative Judge's or Secretary's final decision, or of a previous denial of a reconsideration request.
- When requested by the individual
- When a bona fide offer of employment exists requiring access to RD, NSI, or SNM
- When either: (1) material and relevant new evidence exists, or (2) convincing evidence of rehabilitation or reformation exists.

The request for reconsideration must be submitted in writing to the Director, Office of Departmental Personnel Security (AU-53), and accompanied by an affidavit detailing the new evidence or evidence of rehabilitation or reformation. AU-53 notifies the individual if his/her security clearance eligibility will be reconsidered, and what actions will need to be taken before the decision regarding eligibility for a security clearance can be made.

Protection of Personnel Security Information:

Because security clearance forms contain Personally Identifiable Information (PII), the forms must be protected in accordance with the Privacy Act of 1974. PII is considered Official Use Only and is included within the meaning of controlled Unclassified

Information. PII must be stored in a locked drawer, file cabinet, or a GSA-approved container, and may be discussed only with authorized persons in connection with the processing or adjudication of a security clearance, Federal employment suitability determination, security inquiry, or criminal investigation.

Refer to Chapter 13, Controlled Unclassified Information, for specific guidance on the transmission and destruction of PII.

Applicant Tracking System (ATS):

Applicants may use the ATS to check the general status of their security clearance requests if a new investigation has been requested from the DCSA. The *Applicant Tracking System Quick Reference Guide* describes how to access ATS (see Attachment 301-4). The Helpful Website subsection below provides the ATS website link. ATS offers three items of information:

- The Investigation Requested Date (the date AU-43 submitted the request for the applicant's security clearance to the DCSA)
- The Investigation Results Received Date (the date AU-43 received the applicant's background investigation report from the DCSA)
- The Clearance Action Date (the date AU-43 acted on the applicant's security clearance request).

Points of Contact

For the names and contact information for those occupying the AU-40 positions identified in this chapter, call (301) 903-9990.

For the names and contact information for those occupying the AU-43 positions identified in this chapter, call (301) 903-4175.

For the names and contact information for those occupying the AU-53 positions identified in this chapter, call (202) 586-3249.

Forms/Samples/Graphics

DOE F 206.4, *Information Sheet for Sponsorship of HSPD-12 Credential* (go to <http://energy.gov/cio/downloads/information-sheet-sponsorship-hspd-12-credential> for a copy of this form)

OF-306, *Declaration for Federal Employment* (go to http://www.opm.gov/forms/pdf_fill/of0306.pdf for a copy of this form)

DOE F 473.2, *Security Badge Request* (go to <https://www.energy.gov/sites/prod/files/2013/07/f2/DOE%20F%20473%20%28security%20badge%20request%29%20FORM%20FINAL%205-15-13.pdf> for a copy of this form)

DOE F 5631.18, *Security Acknowledgement* (go to <http://energy.gov/cio/downloads/security-acknowledgement-0> for a copy of this form)

Sample Letter Reporting Results of Contractor Pre-employment Checks and Drug Testing (see Attachment 301-1)

Sample PERSEC F 5630.27, Clearance Action Tracking System (see Attachment 301-2)

Sample of Template 5633.33, Personnel Security Clearance Action Request & Instructions (see Attachment 301-3)

Applicant Tracking System Quick Reference Guide (see Attachment 301-4)

Helpful Website

To access ATS, go to: <https://ats.doe.gov/>

ATTACHMENT 301-1**Sample Letter Reporting Results of Contractor Pre-employment Checks and Drug Testing****Contractor Letterhead**

Date

Director, Office of Headquarters Personnel Security Operations
Office of Headquarters Security Operations
Office of Environment, Health, Safety and Security
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

Dear Sir/Madam:

This letter is to inform you that (name of person) is an employee of this company and is applying for a Department of Energy security clearance. He/she has successfully completed pre-employment screening and drug testing requirements described in Title 10, Code of Federal Regulations (CFR), Part 707, and Title 48, CFR, Part 952.204-2.

The pre-employment checks were conducted by (name of company providing pre-employment screening services) and included verification of the employee's educational background, contact with his/her employer(s) for the past 3 years, contact with listed personal references, permissible local law enforcement checks, a credit check, and other checks routinely performed by our company. These checks were conducted in accordance with all applicable laws, regulations, and Executive Orders, including those governing the processing and privacy of the employee's information collected during the review. The results of these checks were reviewed on (date of review) and evaluated in accordance with our company personnel policies. (Name of person) was determined to be eligible for employment in a position that would require a security clearance.

(Name of person) was tested for the use of illegal substances. A copy of the laboratory report with favorable test results is enclosed with this letter.

If you have any questions concerning these matters, please call me at (202) 555-5555.

Sincerely,

Name
Facility Security Officer (or other official)
Name of company

Enclosure (drug testing laboratory report)

ATTACHMENT 301-2

PERSEC F 5630.27
05/01/2019

Page 1 of 2

CLEARANCE ACTION TRACKING SYSTEM

Unclassified Account Access Request

This form is required for all new user accounts, access changes, and terminations. CATS administrators must complete the NNSA Computer Application Security Training and provide a copy of their training certificate prior to being granted initial access to administrator permissions, and on an annual basis thereafter.

In an effort to reduce paperwork, please use electronic signatures and email the completed request by using the "Submit" button above. For assistance completing this request, contact the CATS Support Desk at (505) 845-6228 or CATSSupport@nnsa.doe.gov

Request Type: ☐ New User ☐ Termination ☐ Access Change ☐ Temporary Access	Employee Type: ☐ Federal ☐ Contractor	Clearance Level: 	PIV Badge: ☐ Yes ☐ No	Citizenship: ☐ U.S Citizen ☐ Non-U.S. Citizen
Name of User (Last, First, MI): 	Title: 	Cognizant Personnel Security Office: 		
Email Address: 	Phone: 	Date of Last Cyber Training: 		

CPSO Access Required (Select All That Apply): ☐ AB ☐ CH ☐ ID ☐ NR ☐ OR ☐ RL ☐ SR ☒ WA

Role(s): ☐ Adjudicator I ☐ Adjudicator II ☐ Supervisor/Assigner ☐ Processor ☐ Vault Worker

Select All
That Apply

☐ Administrative Review ☐ Administrator ☐ CI Officer ☒ eCAR Only ☐ Read Only

Adjudication

☐ Adjudicative Assigner	☐ Grant Authority
☐ Adjudicator	☐ HRP Analyst
☐ Adjudicator Self-Assign	☐ HRP Assigner
☐ AR Analyst	☐ IR Analyst
☐ AR Assigner	☐ IR Assigner
☐ AR HQ Approver	☐ Limited Grant Authority
☐ AR LDS Approver	☐ Review Action Ignore C/F
☐ AR Manager Approver	☐ Review Action Self-Assign
☐ CE Analyst	☐ Super Trusted Contractor
☐ CE Assigner	☐ Trusted Contractor
☐ CI Assigner	
☐ CI Officer	

Processing

- | |
|---|
| ☒ eCAR Admin |
| ☒ eCAR User |
| ☐ Employer Code Book Manager |
| ☐ Fed Oversight |
| ☐ Fed Processor (IFQ) |
| ☐ Processing Assigner |
| ☐ Processor |
| ☐ Vault Worker |
| ☐ Vault Worker- Safe Files |

Other

- | |
|---|
| ☐ Action/Doc Admin |
| ☐ Case (PSF) Admin |
| ☐ CATS Administrator |
| ☐ CATS Reports |
| ☐ CPCI Error Admin |
| ☐ DIF Reject Queue |
| ☐ Investigations Admin |
| ☐ PSI Librarian |
| ☐ Safe File Custodian |
| ☐ Reconsideration Analyst |
| ☐ Reconsideration Assigner |

Justification (describe the supporting program or activities that require the above permissions/CPSO access):

All users require signature authorization from their CPSO Approver and the CATS Approving Official prior to account creation / update.

CPSO Approver:		Approval Date:	
By signature, I certify the above-named individual's security clearance is as stated, and s/he has an official need for the CATS access/resources requested. Additionally, continued need for the specified access will be monitored and if/when access to CATS and/or certain permissions are no longer a necessity, an updated Authorization Request will be provided to the CATS Approving Official or CATS Administrator.			
CATS Approving Official:		Approval Date:	
CATS Administrator:		Completion Date:	

PERSEC F 5630.27
05/01/2019

Page 2 of 2

CLEARANCE ACTION TRACKING SYSTEM

User Code of Conduct

As a new CATS application user, I am required to read and understand the information contained within this user Code of Conduct. This User Code of Conduct applies to all federal and contractor employees approved for access to the CATS application (i.e., Personnel Security, Counterintelligence, etc.) and all related applications (i.e. eCAR Portal).

1. I understand that CATS access is granted to Department of Energy (DOE) employees, contractors, or customers currently performing duties that require access to DOE personnel security information, and that I am responsible for notifying the CATS Support Team of any changes in my position, roles, responsibilities, etc. so that account access and/or permissions can be adjusted.
2. I understand that CATS contains electronic Personnel Security Files (ePSF), and that per DOE O 472.2, *Personnel Security*, I must have an active Q/Top Secret security clearance (or an equivalent background investigation that has been favorably adjudicated and is within scope) to access this information.
3. I understand that I am responsible for maintaining the confidentiality and integrity of the data accessed within the CATS application; that all data processed within the CATS application is considered Sensitive Unclassified Information; and that I am not authorized to share any of the information with individuals that do not have a legitimate need-to-know and Q/Top Secret security clearance (or an equivalent background investigation that has been favorably adjudicated and is within scope).
4. I understand that I am required to protect my CATS account password/PIN at all times and I am prohibited from sharing my password/PIN with anyone.
5. In addition to complying with local reporting requirements, I understand that I must immediately report all suspected cyber security incidents (i.e. viruses, spyware, unusual computer behavior, suspected password compromise, etc.), to the CATS Support Team and the National Nuclear Security Administration (NNSA) Albuquerque Complex Incident of Security Concern (IOSC) Inquiry Official (see IOSC Procedures on the CATS Customer Service Portal for details).
6. I understand that I may only process CATS information on an authorized DOE unclassified computer system/network (VPN, Citrix, etc.), and only at the appropriate classification level (i.e. no classified or Unclassified Controlled Nuclear Information (UNCI) processing can occur within CATS). If classified information is inadvertently processed in CATS, reporting requirements in the paragraph above will be followed.
7. I understand that I must encrypt all data extracts and reports containing PII using encryption methods and tools approved by the NNSA Office of the Associate Administrator for Information Management and Chief Information Officer (NA-IM) and that I must store printed documents and removable media containing sensitive unclassified information in a locked room, drawer, cabinet, or area when unattended.
8. I understand that I am required to 'lock' my computer system (by pressing Ctrl + Alt + Del and selecting the "Lock Computer" option) anytime that I am not in direct line-of-sight of my computer system.
9. I understand that use of the CATS application is for DOE "Official Use Only."
10. I acknowledge that failure to comply with the CATS application security rules and guidelines may result in a security infraction being issued and/or possible revocation of my CATS application access.

CATS User Acknowledgement

I have read and understand my responsibilities as an authorized user of the CATS Application. I agree to comply with the security controls and responsibilities outlined in this CATS User Code of Conduct. I understand that I may never knowingly fabricate, manipulate, delete, or insert data that compromises (or potentially compromises) CATS application data integrity. I have received a copy of this document for my records. If any computer security related incidents or questions arise at any time while using the CATS application, I understand that I must immediately inform the CATS Support Team at (505) 845-6228, and the NNSA Albuquerque Complex IOSC Inquiry Official.

Employee Signature:

Date:

ATTACHMENT 301-3

TEMPLATE 5633.33
(June 2020)

**PERSONNEL SECURITY
CLEARANCE ACTION REQUEST**

SUBJECT INFORMATION			
Subject Type: Please select		Routing Symbol:	DOB:
SSN:			
Name (Last Suffix, First Middle):		Job Title:	
Place of Birth (City, State/Country):	Foreign National ☐ Yes ☐ No	Multiple Citizenship ☐ Yes ☐ No	Citizenship Country:
Physical Home Address (Street Address, City, State, Country, Zip Code):			
Mailing Address (Street Address, City, State, Country, Zip Code):			
Personal Email Address:		Personal Phone #:	
Work Email Address:		Work Phone #:	
Submitter Name:	Submitter Email Address:		Submitter Phone #:
SUBJECT WORK LOCATION / BILLING			
Owning CPSO: HEADQUARTERS	Work Site: Please Select	SOI: DN11	SON: Please Select
EMPLOYER INFORMATION			
Employer (Legal Name):			
Employer Code: NOT NEEDED	Facility Code:	Facility Classification Level: NOT NEEDED	Facility Primary Interest Site: NOT NEEDED
Contract Number:		Primary Contract Number:	
Contract Clearance Access Level: Please Select		Contract Classification Level: Please Select	
ACTION REQUESTED			
Clearance Action Requested: Please select	Clearance Access Level: Select	Classification Level: Please select	Frequency of Access: Please select
Special Request		Justification for Clearance Request:	
Special Access Program ☐ Yes ☐ No			
Interim PIV ☐ Yes ☐ No			
Prior Security Clearance? ☐ Yes ☐ No			

CERTIFICATION FOR PERSONNEL SECURITY CLEARANCE ACTION REQUEST		
<i>"I certify the above individual requires access to the types/level(s) of classified information, matter, or category of SNM to perform official duties as described."</i>		
HC Rep or Hiring Manager Name or Contracting Officer Representative (Last, First, Middle):		Title:
Email Address:	Organization:	Phone #:
Signature and Date:		
<i>"I certify this clearance has been properly justified per all applicable laws, rules, and regulations."</i>		
Headquarters Security Officer Name (Last, First, Middle):		Title:
Email Address:	Organization:	Phone #:
Signature and Date:		
SUBMITTING OFFICE USE BLOCK		
OFFICIAL USE ONLY (When Completed) May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), Exemption number and category: <u>6 - Personal Privacy</u>, Department of Energy review required before public release. Name/Organization: _____ Date: _____, Guidance (if applicable): <u>N/A</u>		
PRIVACY STATEMENT: Collection of information requested is authorized by the Atomic Energy Act of 1954, as amended, and by Executive Orders 10865 and 12356. This form will become part of the individual's Personnel Security File. Disclosure of the information requested on this form is voluntary. However, if the information is not provided, the request for DOE security clearance or access authorization cannot be processed. Access to the information provided is permitted only to authorized Federal Government agencies and to DOE personnel directly involved in the processing for the determination of the eligibility of the individual for a security clearance or access authorization. PERSEC Form 5633.33 or Template 5633.33 is required to request a security clearance action for individuals that require access to classified materials. NOTE: The term "Security Clearance" is being used synonymously with "Access Authorization" as referenced in Department of Energy (DOE) Order 472.2.		

Instructions for Template
*Required Fields

SUBJECT INFORMATION

***Subject type:** Use the drop-down list to select type of employment

***Routing Symbol:** Enter applicant's routing symbol

***DOB:** Enter applicant's date of birth (MM/DD/YYYY)

***SSN:** Enter applicant's full social security number

***Name:** Enter applicant's full legal name, including full middle name or NMN if there is no middle name, and Suffix, if applicable

***Job title:** Enter the applicant's job title

***Place of Birth:** Enter City, State/Country

***Foreign National:** Either "Yes" or "No"

***Multiple Citizenship:** Either "Yes" or "No"

***Citizenship Country:** Type in where the individual holds citizenship

***Physical home Address:** Type in applicant's address, if known; if not, type in DOE facility address

***Mailing Address:** Check "Same as Physical Address," if appropriate, or type in mailing address

***Personal email address:** Provide e-mail address for applicant

Personal phone number: Provide number, if known

Work email: Provide work email, if known

Work phone: Provide phone number, if known

***Submitter name:** Name of individual filling out this form

***Submitter email address:** Provide e-mail address of individual filling out this form

***Submitter Phone #:** Phone number of submitter

SUBJECT WORK LOCATION / BILLING

Owning CPSO: Populated with Headquarters

***Work Site:** Select from the drop-down list

SOI: Populated with DN11

***SON:** Enter Submitting Office Number from drop-down list

EMPLOYER INFORMATION

***Employer:** Enter name of employer (in e-CAR, select from drop-down list)

Employer Code: Populated with Not Needed

***Facility Code:** Enter the employing company's code (this code is on the Contact Security Classification Specification (CSCS form))

Facility Classification Level: Populated with Not Needed

Facility Primary Interest Site: Populated with Not Needed

***Contract Number:** Enter subcontract number, if applicable

***Primary Contract Number:** Enter primary contract number

***Contract Clearance Access Level:** Select from drop-down list

***Contract Classification Level:** Select from dropdown list (this information is on the CSCS form)

ACTION REQUESTED

***Clearance Action Requested:** Select from drop-down list

***Clearance Access Level:** Select from drop-down list

***Frequency of access:** Select either continuous or periodic

***Special Request:** Select any, if appropriate

***Justification:** Enter justification for clearance request (a detailed description of why the individual requires access to classified matter including a statement on the classification level of access required)

CERTIFICATION***Certifications:**

- **Signatories are:** The Human Capital Representative (for Federal employees); or the Contracting Officer Representative (for contractors) with their title, e-mail address, organizational code and phone number
- **Contractor Certifying Office Name:** This is for the Headquarters Security Officer signature, with his/her title, email address, organizational code, and phone number

Documents:

- Upload documents to support the type of clearance request to include this e-CAR form with signatures

ATTACHMENT 301-4**Applicant Tracking System Quick Reference Guide****What is ATS**

The Applicant Tracking System (ATS) is a secure web page that allows a clearance applicant to see when the clearance investigation was scheduled, when DOE received the investigation results, and when a determination was made concerning the clearance request. This system will only track the status of an investigation that was requested by DOE. It will not show a status for an investigation that was requested by any other Federal agency or Department.

Getting Started

There are three basic steps in using ATS:

1. Open Internet Explorer (the web browser)
2. Create an ATS account
3. View the investigation date data

Step 1: Opening Internet Explorer

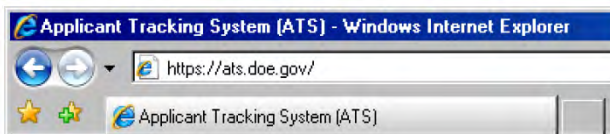
Start Internet Explorer by double clicking its icon. The browser home page opens.



Step 2: Creating an ATS Account

In the **Address** field, type <https://ats.doe.gov> and then press the **Enter** button.

*Note: Make sure that you type the **s** in **https**:*



The ATS Log In page opens.



Click on the **New User** button. The logon page changes to the new user registration page. Fill in the following data on the page:

- Your first and last name
- Last 4 digits of your SSN
- Your Email address
- Your user ID – there are no restrictions; you can enter whatever you want
- Your password – the restrictions are listed at the bottom of the page

Click on the **Submit** button. A message appears on the registration page stating that your account was created. You also will receive a confirmation email that contains your user ID and the ATS URL.

Click on the **Back to Login** button. The ATS Logon page opens.

Enter the user ID and password you created, and then click on the **Login** button.

The **Rules of Behavior** window opens.



Click on the I Agree button. The Clearance Status window opens. _____

Step 3: Viewing Investigation Dates



Step 3: Viewing Investigation Dates

The **Clearance Status** window lists your name and three date fields:

- **Investigation Requested Date:** This is the date DOE has asked the investigating agency to start the investigation.
- **Investigation Results Received Date:** This is the date DOE received all investigation results from the investigating agency.
- **Clearance Action Date:** This is the date DOE made a determination on your clearance request (granted/reinstated L or Q access, upgraded L access to Q, canceled/terminated the request).

If the **Investigation Results Received Date** or the **Clearance Action Date** is blank, that stage of the process has not occurred.

You can see the information shown in this window during the following time frame:
from 1 day after the **Investigation Requested Date** is entered into DOE's Personnel
Security Database (PSDB) through 30 days after the **ClearanceAction Date**.

The **Clearance Status** window contains three drop-down menus:

- **File:** Select **File/Exit** (or click on the icon) to close the Clearance Status window and return to the ATS Logon window.
- **File:** Select **File/Print Screen** (or click on the icon) to print the Clearance Status window.
- **Tools:** Select **Tools/Change Password** to change your password.
- **Help:** Select **Help/Content** (or click on the icon) to view the help file.
Select **Help/Rules** to view the ATS Rules of Behavior.
Select **Help/About** to view the current version number and release date of the ATS software.

Additional Information

If you have specific questions about the investigation process or time frame, contact the security officer who has been handling your clearance request.

For questions or problems concerning this web site, contact the eDISS+ Help Desk.

1. Our phone number is (301) 903-8790.
 - Our fax number is (301) 903-8724.
 - Our e-mail address is diss-helpdesk@hq.doe.gov

Section 302

Other Security Clearance Actions

A DOE security clearance is granted based upon the individual's need to perform certain classified duties. Over time, the individual may change jobs, need a different level of security clearance, or no longer require a security clearance. These situations directly impact the individual's security clearance. The servicing HSO must assist the individual in maintaining the integrity of his/her security clearance.

Many possible variations can occur because of the complicated nature of security clearance actions. To ensure that the transactions are processed in an effective and timely manner, AU-43 must coordinate with those responsible for requesting security clearance actions.

HQ Implementation Procedures

When circumstances affecting an individual's security clearance change, the servicing HSO must notify AU-43 and submit certain documentation. In some circumstances, an eCAR request must be submitted; in others, the documentation is emailed directly to AU-43.

1. The Individual Accepted a Job in a Different HQ Element – The losing element must terminate the individual's security clearance because he/she is no longer performing duties requiring such a clearance. The HSO of the losing organization should outprocess the individual (see Chapter 15, Outprocessing); have the individual complete a DOE F 5631.29, *Security Termination Statement*; and annotate "This individual is transferring to (Name of Element)" on the DOE F 5631.29. If the HSO is aware that the individual will be performing classified work in his/her new position, the completed DOE F 5631.29 should be provided to the gaining element's HSO. Otherwise, the DOE F 5631.29 should be emailed to AU-43 at personnelsecurity@hq.doe.gov.

If the gaining HQ element requires the individual to perform classified work, the HSO of the gaining element must create and submit a Transfer request in eCAR. A new justification is required as well as the DOE F 5631.29 referred to in the paragraph above, the PDR, and the PD if a Federal employee. If the individual who is transferring is a badged contractor employee, the HSO must also prepare a new DOE F 473.2, *Security Badge Request*, and add it to the eCAR request.

The HSOs of the two organizations should coordinate and work together so that the clearance is not terminated by AU-43 before the transfer paperwork is received.

If the gaining HQ element does not require the individual to perform classified work, please refer to paragraph 3.

2. An Individual with a Security Clearance is Departing DOE – The individual's security clearance must be terminated. The HSO should outprocess the individual (see Chapter

15, Outprocessing) and have the individual complete DOE F 5631.29. The completed form must be emailed to AU-43 at personnelsecurity@hq.doe.gov.

3. An Individual No Longer Requires Access to Classified Information but Requires Regular Access to a HQ Facility – The servicing HSO must have the individual complete a DOE F 5631.29. In addition, the HSO must submit Template 5633.33 with “Downgrade to BAO” selected as the Clearance Action Requested. For contractor employees, the HSO must also complete and submit to AU-43 a new DOE F 473.2. AU-43 will contact the HSO if any additional paperwork is needed. All documents should be emailed to personnelsecurity@hq.doe.gov.
4. An Individual Had a Clearance that Was Terminated and Now Needs to be Reinstated – The sponsoring HSO of the element should submit a Reinstatement eCAR request. A valid justification is required along with DOE F 5631.18, the PDR, and negative drug test results. For Federal employees, the PD is also required. If the individual is a contractor, the HSO must verify through a SSIMS check that the employing company has a facility clearance and that the classified contract with the sponsoring HQ element is registered. The HSO must also complete a new DOE F 473.2 for contractor employees only, and add it to the eCAR request.
5. An Individual Has a DOE L, S, or C Clearance but Requires a Q or TS Clearance – The presumption is that the individual now has a need for access up to TS/RD or TS/NSI. The HSO servicing the individual must submit an Upgrade eCAR request. An acceptable justification is required along with the PDR. The PD is required if the individual is a Federal employee. When a contractor seeks the upgrade, the HSO must also complete a new DOE F 473.2 and add it to the eCAR request.
6. An Individual Has a Q or TS Clearance but Requires an L, S, or C Clearance – The individual no longer requires access up to TS/RD or TS/NSI, but requires access up to C/RD, S/NSI, or C/NSI. The servicing HSO must submit a Downgrade eCAR request. A valid justification is required along with the PDR. If the individual is a Federal employee, the PD is also required. For contractor employees, the HSO must also complete a new DOE F 473.2 and add it to the eCAR request.
7. An Individual with a Security Clearance Needs to Support an Additional HQ Element – The HSO of the element requiring the individual’s new services must submit a request for Extension in eCAR. The extension allows AU-43 to identify all the HQ elements that may have an interest in maintaining the individual’s security clearance. Unless the individual will be working for more than one contractor, a security clearance extension is unnecessary if the individual is taking on additional duties within his/her sponsoring element.
8. An Individual No Longer Requires a Security Clearance after the Request was Submitted to AU-43 – The servicing HSO of an individual who is being processed for a security clearance but no longer needs it must submit Template 5633.33 with “Cancellation” selected as the Clearance Action Requested. The justification should explain why the

clearance is no longer needed (i.e., employee resigned, job duties changed, etc.). The completed form must be emailed to AU-43 at personnelsecurity@hq.doe.gov.

Once a DOE security clearance is granted, the individual must undergo a background reinvestigation every 5 years. Section 305, Security Clearance Reinvestigations and Verifications, contains details on processing reinvestigation requests.

Actions related to the termination of security clearances are described in Chapter 15, Outprocessing, of the HQFMSP.

Points of Contact

For the names and contact information for those occupying the AU-43 positions identified in this chapter, call (301) 903-5499 or (301) 903-4175.

Forms/Samples/Graphics

DOE F 473.2, *Security Badge Request* (go to <https://www.energy.gov/sites/prod/files/2013/07/f2/DOE%20F%20473%20%28security%20badge%20request%29%20FORM%20FINAL%205-15-13.pdf> for a copy of this form)

DOE Form 5631.29, *Security Termination Statement* (go to <http://energy.gov/cio/downloads/security-termination-statement> for a copy of this form)

Sample of Template 5633.33, Personnel Security Clearance Action Request (see Attachment 301-3)

This page intentionally left blank.

Section 303

Reporting Requirements for Personnel Holding Security Clearances

This section sets forth HQ procedures for reporting significant matters affecting a person's security clearance. Information that may affect a person's continued eligibility for access to DOE facilities, material, or classified information must be reported to AU-43.

HQ Implementation Procedures

Reportable Information:

All individuals have a specific obligation to report personnel security-related matters as they occur, whether related to themselves or to other individuals applying for or holding a DOE security clearance. Such matters, listed below, must be reported verbally and directly to AU-43 immediately upon the individual becoming aware of the situation or incident, and in no event later than two (2) working days after the event. Thereafter, written confirmation of the information must be provided by the individual to AU-43 within three (3) additional working days.

NOTE: Federal management officials must report any condition affecting the status of an applicant's or employee's security clearance, including death, employment termination, or change in need for access to classified information. Contractors must report an employee who declines an offer of employment, fails to report to duty, is terminated, dies, no longer requires access to classified information, or has his/her access restricted or withdrawn.

Other reportable information includes, but is not limited to:

1. Legal action effected for a name change – AU-43 must be notified, in writing, to ensure that the appropriate change is made to the security clearance record. AU-43 coordinates with the individual's servicing badge office and HSO to obtain a corrected security badge.
2. Change in citizenship.
3. Any use of an illegal drug, or use of a legal drug in a manner that deviates from approved medical direction.
4. Parent(s), brother(s), sister(s), spouse, or offspring assuming residence in a sensitive country. See the Sensitive Countries List, which is OUO, available from the Office of Counterintelligence (IN-20).

5. Observing or having knowledge of the presence of a situation or incident involving an individual holding or applying for a DOE security clearance that involves any of the matters identified in this section.
6. Any arrests, criminal charges (including charges that are dismissed), citations, tickets, summons or detentions by Federal, State, or other law enforcement authorities for violations of law within or outside of the U.S. Traffic violations for which a fine of up to \$300 (per the SF-86 form) was imposed need not be reported, unless the violation was alcohol or drug-related.
7. Hospitalization for mental health reasons or treatment for drug or alcohol abuse.
8. Employment by, representation of, or other business-related association with a foreign or foreign-owned interest or non-U.S. citizen or other individual who is both a U.S. citizen and a citizen of a foreign country.
9. Personal or business-related filing for bankruptcy.
10. Garnishment of wages.
11. Any contact with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information or SNM.
12. Any unofficial contact with a foreign national from a sensitive country, as well as any association with any foreign national that is close and continuing, or more than casual in nature, whether in a business or social setting, or in any way raises a security concern. This includes a belief that a foreign national is inappropriately trying to obtain sensitive or classified information from the DOE cleared individual.
13. Suspension or termination of accesses either administratively or for cause.
14. Marriage or cohabitation – DOE F 5631.34, *Data Report on Spouse/Cohabitant*, must be used to make the report to AU-43 and submitted within 45 days of the marriage or cohabitation. A National Agency Check (without fingerprints) is conducted on the spouse or cohabitant if he/she is not a U.S. citizen.
15. Foreign nationals who share living quarters with the cleared individual.
16. Proposed travel to a sensitive country must be reported to the Office of Intelligence and Counterintelligence in accordance with the requirements of that office.

Reporting 90 Day Absences:

Cleared personnel must report a leave of absence or extended leave lasting 90 days or more. The individual's access authorization may be terminated during the time he/she does not require

access to classified information. The report must be made directly to AU-43 using the *Sample 90 Day Absence Report* (see Attachment 303-1).

Points of Contact

For the names and contact information for those occupying the AU-43 positions identified in this chapter, call (301) 903-5499 or (301) 903-4175.

To acquire a copy of the Sensitive Countries List, call (202) 586-5275.

Forms/Samples/Graphics

DOE F 5631.34, *Data Report on Spouse/Cohabitant* (go to <http://energy.gov/cio/downloads/data-report-spousecohabitant> for a copy of this form)

Sample 90-Day Absence Report (see Attachment 303-1)

ATTACHMENT 303-1**Sample 90-Day Absence Report**

MEMORANDUM FOR (NAME), DIRECTOR
OFFICE OF HEADQUARTERS PERSONNEL SECURITY OPERATIONS
OFFICE OF HEADQUARTERS SECURITY OPERATIONS

FROM: (NAME)
DIRECTOR OR HEADQUARTERS SECURITY OFFICER
NAME OF ELEMENT

SUBJECT: Reporting 90-Day Absence

In accordance with 4.r.(2), of DOE Order 470.2.2, PERSONNEL SECURITY our office is reporting that (Subject's name) will be absent from duty in excess of 90 days or more and will not require access to classified material or information during this absence. Your office will be notified when he/she returns to duty.

If you have any questions regarding the above, please contact me at _____.

Section 304

Electronic Questionnaires for Investigations Processing

This section supplements the procedures described in Section 307, HSPD-12 Credential for Personal Identity Verification (PIV), and Section 301, Acquiring New Security Clearances, and the process for data collection for background investigations.

DOE uses the e-QIP web application to collect, review, and coordinate the information required by the Federal government to conduct background investigations. The Defense Counterintelligence and Security Agency (DCSA) manages the e-QIP system on behalf of all Federal agencies, including DOE. e-QIP must be used by every DOE Federal or contractor employee applying for an HSPD-12 security badge and/or a security clearance.

e-QIP is a database application located on a secure website. As with all secure websites, several authentication actions are required before an applicant can use e-QIP. These actions ensure that only authorized personnel can gain access to e-QIP and the applicant's personal information. The procedures described in this section must be followed to access e-QIP, properly complete the appropriate security questionnaire, and ensure protection of the applicant's privacy.

The e-QIP system has several advantages over the former paper process for gathering and retaining the information required for background investigations. These advantages include:

- The applicant can access his/her security questionnaire at the e-QIP website from any computer, thereby allowing the applicant to work from home, while travelling, etc.
- Once the applicant completes his/her security questionnaire, most of the information remains in the system. When the applicant has been initiated again at a future date he/she has access to the information previously provided and only needs to update it.
- The data is available to the applicant wherever his/her career places him/her in the Federal government, whether as a Federal employee or as a contractor.
- e-QIP contains automatic audit features that reduce the opportunity for errors in the security questionnaire to go undetected.
- An applicant can save his/her work and take the time needed to properly complete the security questionnaire.
- Information from an applicant's security questionnaire is transmitted electronically, which reduces processing time.

AU-43 is responsible for managing e-QIP activities for all DOE security clearances processed at HQ.

HQ Implementation Procedures

What Must Be Done:

An applicant or employee needing to complete the SF-85, SF-85P, or SF-86 form will have an e-QIP request initiated which allows him/her to access the e-QIP system. The individual will receive a notification email containing important instructions about registration, the link to the e-QIP website, and a due date for when the form must be completed and transmitted to AU-43 for review. Applicants should be given no more than 2 weeks to complete the form. It is the applicant's responsibility to make every effort to complete the form by the due date given in the notification email. However, if more time is needed due to extenuating circumstances (i.e., medical emergency, death in the family, extended travel, etc.), he/she should contact the individual who sent the notification email to request more time and explain the reason. Otherwise, applicants are expected to comply and have the form completed by the due date. Reminders will not be sent.

Applicants who fail to comply and allow the e-QIP request to expire must contact the individual who sent the notification email and provide an explanation for the noncompliance. If the explanation is plausible, another e-QIP request will be initiated for the applicant allowing him/her an additional opportunity to complete the form. If the applicant fails to comply a second time, the HSO and the HC specialist (for Federal applicants) will be contacted and AU-43 will discontinue processing the clearance request.

e-QIP Registration:

Most applicants will need to register for an e-QIP username and password. The registration process requires the applicant to answer three "golden questions," which include the applicant's last name, year of birth, and city of birth, and enter a 14 digit registration code. The applicant receives this registration code via email from DCSA or within the notification email. If the "golden questions" and registration code are entered correctly, the applicant will be prompted to create a username and password. Passwords must be at least 14 characters in length and contain a mixture of special characters, upper and lowercase letters, and numbers. If the username and password created are acceptable, the applicant will be prompted to select three "challenge" questions and answers. The "challenge questions" allow the applicant to reset his/her password should it be forgotten. The applicant is encouraged to view the answers as he/she types them to catch typing or spelling errors.

Some applicants who have recently accessed e-QIP will have a username and password. If the individual cannot remember their password, he/she should enter the username and click on the "Forgot Password" link. The individual's challenge questions created during registration will appear. If the individual answers the questions correctly, he/she will be prompted to create a new password. If the individual cannot remember the answers to the challenge questions or

cannot remember the username, he/she should contact the person who sent the notification email and ask for assistance.

Completing the SF-85, SF-85P, or SF-86 form in e-QIP:

After logging in, the applicant is automatically directed to either the SF-85, SF-85P, or SF-86 form. The applicant must enter his/her personal data into the proper form. The data can be saved if the applicant cannot complete it all at one time. To save the data, the applicant must click on the “logout” button at the top, right-hand corner of the screen. The process continues until the form is completed. e-QIP detects some, but not all, errors as they occur. If a required field is not completed, e-QIP stops the applicant from proceeding to the next section. All errors must be corrected and all warnings must contain an explanation before the system will allow the applicant to certify their form.

When all data is entered and all validation errors corrected, the applicant certifies that his/her answers are correct, prints a copy of the form for his/her records, digitally signs the signature pages, and releases the form to AU-43 for review. AU-43 reviews the form for completeness and accuracy. If corrections are needed, AU-43 will return the form directly to the applicant and send an email with a detailed explanation of the corrections/clarifications needed. The HSO will also be informed of this action, if possible. AU-43 gives the applicant up to 5 days to make the corrections in e-QIP, certify the form, digitally sign the signature pages, and release the form for AU-43 to review. AU-43 reviews the form for completeness and accuracy again. If acceptable, AU-43 releases the form to DCSA to start the background investigation. AU-43 has 14 days from the time the applicant certifies the form to submit to DCSA.

AU-43 will return forms for corrections/clarifications two times. After the second time, the HSO and/or HC Specialist will be notified for assistance.

Notification of Completion:

It is the responsibility of the applicant to notify AU-43 when he/she has completed the form and released it for review. There is no automatic notification in e-QIP that alerts AU-43 when an e-QIP request is waiting for review. If an applicant fails to notify AU-43, it is possible that the form could sit in a waiting state in e-QIP for longer than 14 days resulting in AU-43 not meeting the required submission goal. If this happens, AU-43 will return the form to the applicant who will then be required to review the entire form, make any updates needed, certify the form, digitally sign the signature pages, release the form, and notify AU-43 that these actions are complete.

Continuation of HSPD-12 Badge or Security Clearance Processing:

Completing the e-QIP process is just one of many steps required to obtain an HSPD-12 badge or a security clearance. For those applying for an HSPD-12 badge, refer to Section 307 for required additional processing actions. For those applying for a security clearance, refer to Section 301 for required additional actions.

Points of Contact

For the names and contact information for those occupying the positions identified in this chapter or more information about HSPD-12 badges, call (301) 903-5499 or (301) 903-4175.

Helpful Website

<https://nbib.opm.gov/e-qip-background-investigations/>

This page intentionally left blank.

Section 305

Security Clearance Reinvestigations and Verifications

Each fiscal year, AU-43 sends a list of all clearance holders due for reinvestigation to the HSO of the HQ element sponsoring the security clearances. The list is transmitted via memorandum and contains processing instructions. The majority of the packages are scanned and transmitted via encrypted e-mail.

AU-43 also provides the HSO a list of all clearance holders currently sponsored by their element. The list is accompanied by a memorandum from AU-43 requesting the HSO verify that the information on the list is correct. Verification ensures that unneeded security clearances are terminated and office symbols and sponsorship records of each cleared individual are correct.

NOTE: AU-43 can request reinvestigation paperwork for an individual and submit an investigation request to DCSA at any time if in possession of information that creates a security concern.

HQ Implementation Procedures

Reinvestigations:

Each fiscal year, AU-43 runs a report from the Central Personnel Clearance Index (CPCI) identifying all clearance holders in each HQ element who are due for reinvestigation. The report is sent to the HSO of the sponsoring element as an attachment to a memorandum requesting certain actions, which include:

- Ensuring that all personnel on the “due for reinvestigation” list still require a security clearance
- Ensuring that the clearance level for each person on the list is consistent with the person’s actual access to classified information
- Processing the required documents for reinvestigation.

The memorandum transmitting the list to the HSO contains specific instructions. The HSO should contact the supervisor of each person on the reinvestigation list to ensure the person is still employed and still requires his/her security clearance.

If the person is no longer employed, has left the element, or no longer needs a security clearance, his/her security clearance must be terminated. The actions required for each scenario are:

1. The Individual Is No Longer at DOE – When the employee is unavailable to sign the DOE F 5631.29, *Security Termination Statement*, the HSO must complete and sign the form. On the second page, the HSO should click the radio button indicating that the Subject is not available for debrief and submit it to AU-43.
2. The Individual Has Transferred to Another HQ Element – The HSO of the losing element must complete and sign the DOE F 5631.29, annotating that “This individual transferred to (name of gaining HQ element).” To fully comply with processing procedures, the transferring individual must also sign the form before the HSO of the losing element submits it to AU-43.
3. The Individual Is Still Supporting the Element but No Longer Requires a Security Clearance – The HSO must have the individual complete a DOE F 5631.29. In addition, the HSO must submit Template 5633.33 with “Downgrade to BAO” selected as the Clearance Action Requested. If a contractor no longer requires the clearance, the HSO must also complete and submit to AU-43 a new DOE F 473.2. AU-43 will contact the HSO if any additional paperwork is needed.

The documents mentioned in the three paragraphs above cannot be submitted via eCAR. They must be emailed to personnelsecurity@hq.doe.gov.

When the individual has a Q or TS security clearance and needs an L, S, or C clearance, or vice versa, the HSO must submit the documentation required to “Upgrade” or “Downgrade” the clearance in accordance with the instructions contained in Section 302, Other Security Clearance Actions, of the HQFMSP.

When the individual needs to retain his/her current security clearance, the employee must complete a DOE F 5631.18, *Security Acknowledgement*, and submit it to his/her HSO. For Federal employees, a copy of the employee’s Position Description (PD) and Position Designation Record (PDR) are required. For contractors, only a copy of the PDR is required. All of the required forms and documentation are submitted to AU-43 via eCAR for review and approval. If acceptable, an e-QIP request is initiated for the employee. See Section 304 for information on what actions the employee must take to complete e-QIP processing.

When the individual fails to submit the documentation required for his/her reinvestigation or does not complete the e-QIP process within the prescribed timeframe, the individual is advised that such failure will result in an administrative termination of his/her security clearance.

Clearance Verification:

In addition to the list of reinvestigations, each fiscal year, AU-43 runs a CPCI report identifying all the HQ Federal and contractor employees and consultants, by HQ element, with active or pending security clearances. The report is sent to the HSO of the sponsoring element as an attachment to a

memorandum requesting that certain actions be taken. The packages are scanned and transmitted via encrypted e-mail.

These actions include:

- Ensuring that all the personnel on the list still require their security clearance.
- Ensuring that the clearance level for each person on the list is consistent with the person's actual access to classified information.
- Ensuring the office symbol for each employee is correct.

The memorandum transmitting the list to the HSO contains specific instructions. The HSO is expected to contact the supervisor of each person on the list to verify the person still requires the security clearance and remains assigned to the office shown.

If the person is no longer employed, has left the element, or no longer requires a security clearance, his/her security clearance must be terminated. The actions required for each scenario are detailed under Reinvestigations, above.

If the individual has a Q or TS security clearance and needs an L, S or C clearance, or vice versa, the HSO should submit the documentation required to "Upgrade" or "Downgrade" the clearance in accordance with the instructions contained in Section 302, Other Security Clearance Actions.

When the individual has a different office symbol, the name of the employee must be highlighted on the verification list and his/her office symbol struck through with a line. The new office symbol must be handwritten beside the strikethrough. (Note that if the individual transferred to a different position (Federal employees only), AU-43 needs a copy of the PD and PDR).

Upon completion of the review, the entire list must be returned to AU-43 in accordance with the instructions contained on the original transmittal memorandum. This informs AU-43 that verification is complete and enables that office to update CPCI with the latest available information.

Points of Contact

For the names and contact information of those occupying the positions identified in this section, call (301) 903-5499 or (301) 903-4175.

Forms/Samples/Graphics

DOE Form 473.2, *Security Badge Request* (go to <https://www.energy.gov/sites/prod/files/2013/07/f2/DOE%20F%20473%20%28security%20badge%20request%29%20FORM%20FINAL%205-15-13.pdf> for a copy of this form)

DOE F 5631.18, *Security Acknowledgement* (go to <http://energy.gov/cio/downloads/security-acknowledgement-0> for a copy of this form)

DOE Form 5631.29, *Security Termination Statement* (go to <http://energy.gov/cio/downloads/security-termination-statement> for a copy of this form)

Sample of Template 5633.33, Personnel Security Clearance Action Request (see Attachment 301-3)

Section 306

Passing Clearances for Classified Meetings or Visits

This section applies only to Federal and contractor employees holding a clearance granted by the HQ Cognizant Personnel Security Office (CPSO). It does not apply to Federal or contractor employees physically located at a HQ facility whose clearance was granted by another DOE CPSO.

HQ clearance holders planning to attend a classified meeting at either a DOE field site, another government agency (OGA), or the U.S. Congress, may need to have their security clearances, SCI accesses, or Sigma accesses passed to the hosting facility prior to arriving at the meeting site.

Conversely, employees of DOE field sites, OGAs, and the U.S. Congress planning to attend a classified meeting at DOE HQ may need to have their security clearances, SCI accesses, or Sigma accesses passed to HQ before attending the meeting.

HQ Implementation Procedures

HQ Clearance Holders Attending Classified Meetings at DOE Field Sites:

A HQ clearance holder who will be attending a classified meeting at a DOE field site need not pass his/her security clearance information to that site unless he/she is visiting a DOE site supervised by the NNSA and requires the passing of Sigma accesses (see process for passing Sigma accesses below).

A HQ clearance holder visiting a SCIF at DOE field site need not pass his/her SCI access. The HQ employee must provide his/her full name and Social Security Number (SSN) to the meeting's host, so that his/her SCI access can be verified by the host's SSO.

HQ Clearance Holders Attending Classified Meetings at an OGA or the U.S. Congress:

HQ clearance holders attending a classified meeting at an OGA or the U.S. Congress must pass their security clearances and/or Sigma accesses to the facility hosting the meeting.

It may also be necessary to pass the employee's SCI access (see the HQ Process for Passing SCI Accesses subsection below for more information about when SCI accesses need to be passed).

HQ Process for Passing Security Clearances to DOE Field Sites, OGAs, and the U.S. Congress:

When a HQ clearance holder must pass their security clearance, a DOE F 5631.20, *Request for Visit or Access Approval*, is required. The employee, his/her administrative assistant, or the

servicing HSO is permitted to complete the DOE F 5631.20. The person completing the form must enter all information on Part A of the form, (the top half of the form). The following specific instructions are provided:

- The full name, date of birth, and SSN of all HQ clearance holders participating in the visit. For visits to Department of Defense facilities, the place of birth must also be listed.
- The name of the facility being visited (spell out acronyms).
- The purpose of the visit – must be more than just “meeting” or “briefing” without becoming classified. The inclusive dates may be for a one-day, one time visit, or may be used to permit access for a period not to exceed one year.
- Provide the name, title, telephone number, and email address of the person being visited or hosting the meeting.
- Provide the security office or visitor control point of contact along with a telephone and fax number.
- The level and category of information to be accessed (e.g., S/RD).
- If the visit will require access to a National Security Vault (NSV) this must be indicated on the form.
- Additional information can be provided in the section labeled “Prior arrangements have/have not been made as follows”

The portion of the DOE F 5631.20 entitled “Certification for Personnel Having DOE Clearance” must bear the printed name, title, and signature of the Federal official in the traveler’s organization who is certifying the need for the clearance to be passed. The certifying official must have the title of “Director” or be an equivalent level supervisor or manager.

The completed DOE F 5631.20 must be submitted to AU-43 for further processing. Forms that are not completed correctly, missing information, or not signed will be returned to the requester with no further action taken by AU-43. The DOE F 5631.20 should be submitted 15 working days prior to the visit. AU-43 cannot guarantee the visit request will be completely processed if not received at least 15 days prior to the visit. **This is especially critical for overseas travel and Department of State locations.**

HQ Process for Passing SCI Accesses to DOE Field Sites, OGAs, and the U.S. Congress:

HQ clearance holders passing their SCI clearances to a DOE field site, an OGA, or the U.S. Congress must do so through the HQ SSO in the Office of Counterintelligence (IN-20). Contact the HQ SSO for instructions on how to request the passage of an SCI clearance. The HQ SSO is available by e-mail at: SSO.Departmental@doe.gov.

HQ Process for Passing Sigma Accesses to DOE Field Sites, OGAs, and the U.S. Congress:

HQ clearance holders needing to pass Sigma 14, Sigma 15, and/or Sigma 18 access must complete and submit the Sigma Access Request Form via encrypted email to sigmaprocessing@nnsa.doe.gov. The DOE F 5631.20 is no longer required. Please direct all questions regarding Sigma accesses to sigmaprocessing@nnsa.doe.gov.

Visitors Attending Classified Meetings at HQ Facilities:

DOE Federal and contractor employees and OGA employees with a DOE-issued security clearance who will be attending a classified meeting at a HQ facility need not pass their clearances unless the HQ host advises otherwise. If the meeting involves access to SCI, see the Visitors Attending SCI Meetings at HQ Facilities subsection below.

OGA employees without a DOE-issued security clearance or employees of the U.S. Congress must pass their security clearances before attending a classified meeting at HQ.

AU-43 accepts the following forms for the passage of security clearances:

- DOE F 5631.20, *Request for Visit or Access Approval*
- NASA F 405 (National Aeronautics and Space Administration personnel only)
- NRC F 277 (Nuclear Regulatory Commission personnel only).

The visitor's employer must submit the above forms to AU-43 at least 15 working days prior to the visit.

NOTE: Cleared DOE personnel in the field need not submit a DOE F 5631.20 to AU-43; however, if Sigma 14, 15, or 18 access is requested, the Sigma Access Request Form must be completed and emailed (encrypted) to sigmaprocessing@nnsa.doe.gov.

Visitors Attending SCI Meetings at HQ Facilities:

DOE field employees who will be attending a meeting at HQ where SCI will be presented can have their SCI accesses verified by the HQ SSO via Scattered Castles. In order for the HQ SSO to search Scattered Castles, the HQ host of the meeting must provide, in writing, the full name and SSN of all employees attending the meeting.

Employees from an OGA or the U.S. Congress planning to attend a meeting at HQ where SCI will be presented must pass their SCI accesses through Intelligence channels. The SSO at the OGA or U.S. Congress accomplishes this by sending the required information to the responsible HQ SSO within IN-20. HQ personnel hosting a meeting where SCI will be presented can contact IN-20 to identify the responsible HQ SSO.

Points of Contact

For the names and contact information for those occupying the AU-43 positions identified in this chapter, call (301) 903-4175.

For the names and contact information for those occupying the IN positions identified in this chapter, call (202) 586-0335 or (202) 586-2231.

Forms/Samples/Graphics

DOE F 5631.20, *Request for Visit or Access Approval* (go to <http://energy.gov/cio/downloads/doe-f-563120> for a copy of this form)

This page intentionally left blank.

Section 307

HSPD-12 Credential for Personal Identity Verification (PIV)

Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, was issued on August 27, 2004. HSPD-12 states that it is the “policy of the United States to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal government to its employees and contractors (including contractor employees).” In essence, HSPD-12 requires that all Executive branch agencies, including DOE, issue their Federal and contractor employees a common, secure, and reliable identification badge that can be used to grant access to Federally-controlled facilities. The identification badge also permits employees to access Federally-controlled information systems.

Who Needs a HSPD-12 Credential?

Personnel supporting DOE for six (6) months or more, whether a Federal employee or a contractor employee, who do not require a security clearance (access authorization) but do require physical and logical access to DOE property, facilities, and information systems must go through the PIV process. This process is used to grant or deny a HSPD-12 credential.

IMPORTANT NOTE: If the employee requires a security clearance, DO NOT submit paperwork for a HSPD-12 credential and then submit a request for a security clearance. Please refer to section 301 for instructions on the security clearance process.

Requesting a HSPD-12 Credential:

Processing an applicant for a HSPD-12 credential involves several steps and multiple officials:

1. Sponsorship – The HQ element where the employee will work is responsible for sponsoring the employee for the HSPD-12 badge. The sponsor must be a Federal employee. Sponsorship includes, but not limited to, entering the employee’s date and place of birth, program office being supported, and citizenship status.
2. Enrollment – (fingerprints and a photograph of the employee) After the sponsor enters the required information into USAccess, the system will automatically contact the employee via e-mail with instructions for scheduling an appointment to enroll at a USAccess Credentialing Center. The employee must present two identity verification documents: one primary document and one secondary document.

NOTE: Employee must be enrolled in USAccess and fingerprinted before a PIV packet is submitted to AU-43 for processing.

- a. If the employee's fingerprints are deemed invalid in USAccess, AU-43 will notify the HSO who will cancel the Reprint and trigger a Reissuance which will prompt the employee to be fingerprinted again.
- b. If the employee's fingerprints are returned from DCSA as unclassifiable, AU-43 will notify the HSO and employee that a second set of prints is required. The HSO will trigger a reprint in USAccess.

NOTE: It is the responsibility of the HSO and the employee to notify AU-43 when the employee has been re-fingerprinted. USAccess will NOT notify AU-43.

3. Submission of HSPD-12 Badge Documentation – The following documents are to be submitted to AU-43 via the Personnel Security mailbox personnelsecurity@hq.doe.gov.
 - a. **Federal Employees – (Responsibility: Element's HC Specialist or HSO)**
 - DOE F 206.4, *Information Sheet for Sponsorship of HSPD-12 Credential*
 - OF-306, *Declaration for Federal Employment*
 - Resume and Offer Letter
 - Position Designation Record (PDR) and Position Description (PD):
Signature required
 - b. **Contractor Employees – (Responsibility: HSO or Sponsor)**
 - DOE F 206.4, *Information Sheet for Sponsorship of HSPD-12 Credential*
 - OF-306, *Declaration for Federal Employment*
 - DOE F 473.2, *Security Badge Request*
 - PDR: No signature required

Note: The employee must record his/her name on the DOE F 206.4 and the OF-306 exactly as it appears on the two identity verification documents presented to the Credentialing Center. For information on how to locate a USAccess Credentialing Center, how to schedule an appointment, and the required documents for enrollment, go to <https://www.fedidcard.gov/>

HSPD-12 Process:

1. Request received – When a request is received in the Personnel Security mailbox, AU-43 will review the submitted packet for completion and accuracy. The request will be returned if incomplete, missing documents, employee is not enrolled, and/or if paperwork is not completed correctly. This will delay the process so it is best to ensure the packet has all required documents.

2. e-QIP Processing – See Section 304 of the HQFMSP for information regarding e-QIP processing.
3. Background Investigation – Once the e-QIP process is completed, the applicant's information is automatically forwarded to DCSA.
4. Preliminary Approval – AU-43 will Preliminary Approve an employee if both the fingerprints and the SF-85 or SF-85P are clear of any derogatory information. USAccess will be updated to reflect the Preliminary Approval and the HSPD-12 credential will print at that time. If AU-43 is unable to Preliminary Approve, the employee will continue to use the Local Site Specific Only (LSSO) badge unless otherwise directed. An email will be sent to employee, HSO, and the Badge Office informing all parties of the Preliminary Approval and extension of either the LSSO badge or HSPD-12 credential. Please refer to Chapter 1, Physical Security, for additional information on badges.
5. Final Approval – AU-43 will adjudicate and make a final determination on the background investigation received from DCSA. No additional information should be required from the HSO and/or employee after the Preliminary Approval process. However, if additional information is required to render a final determination, an email will be sent to the employee and/or HSO.

Points of Contact

For the names and contact information for those occupying the AU-43 positions identified in this chapter, call (301) 903-5499 or (301) 903-4175.

Forms/Samples/Graphics

DOE F 206.4, *Information Sheet for Sponsorship of HSPD-12 Credential* (go to <http://energy.gov/cio/downloads/information-sheet-sponsorship-hspd-12-credential> for a copy of this form)

DOE F 473.2, *Security Badge Request* (go to <https://www.energy.gov/sites/prod/files/2013/07/f2/DOE%20F%20473%20%28security%20badge%20request%29%20FORM%20FINAL%205-15-13.pdf> for a copy of this form)

OF-306, *Declaration for Federal Employment* (go to http://www.opm.gov/forms/pdf_fill/of0306.pdf for a copy of this form)

Sample DOE F 206.4 (see Attachment 307-1)

Sample DOE F 473.2 (see Attachment 307-2)

Sample OF-306 (see Attachment 307-3)

Helpful Website

To access the Position Designation Tool, copy and paste this website into your Google Chrome browser: <https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool/#url=Automated-Tool>

Reminder: Section 307 refers to employees who will ONLY require a Non-cleared HSPD-12 credential. If the employee requires a security clearance, DO NOT submit paperwork for a HSPD-12 credential and then submit a request for a security clearance. Please refer to section 301 for instructions on the clearance process.

ATTACHMENT 307-1

DOE F 206.4
(4/2010)
Cancels DOE F 206.3

Treat as **Official Use Only** when PII entered.

PIV FILE #:
(for use by Registrar's Office Only)

Information Sheet for Sponsorship of HSPD-12 Credential

Privacy Notice: 42 U.S.C. 7101, 50 U.S.C. 2401 and Public Law 93-579 permit collection of the data requested on this form. The information is used to determine suitability for the issuance of a DOE security badge. The information will be used to identify proof and register Applicants as part of the Personal Identity Verification process. Providing this information is voluntary; however, failure to submit this information may result in denial of a DOE security badge.

Biographical Information (To Be Completed by Applicant)			
(1) Full Name: (must match the name on Driver's License or Passport)			
First	MI	Last	Suffix
Raylan	Harlan	Givens	
(2) Aliases: (Other names ever used, for example, maiden name, nickname, etc.)			
First	MI	Last	Suffix
Ray	Harlan	Givens	
(Make sure ALL aliases are listed)			
(3) Home Address			
123 Main Street Anywhere, MD 01234 (FULL COMPLETE ADDRESS)			
(4) SSN	(5) Date of Birth		(6) Country of Citizenship
123-45-6789	01/01/1990		USA
(7) Place of Birth:	City	State	Country
	Germantown	MD	USA
(8) Home E-mail:	RaylanG@gmail.com		
(9) Other E-mail:	N/A OR RaylanG@gmail OR RaylanHG@yahoo.com		
Employment Information (To Be Completed by Sponsoring Office)			
(10) DOE Affiliation:	(check one) ☐ Federal Employee ☒ Contractor ☐ Executive Staff ☐ Associate/Dignitary ☐ Service Provider ☐ Uniformed Services		
(11) Work E-mail:	Raylan.Givens@Hq.Doe.Gov OR TBD		
	(11a) Check here if applicant will not have business e-mail. ☐		
(12) Work Phone:	301-903-0000	(13) Federal Emergency Response Official:	☐ Y ☒ N
(14) PIV-I (new hire) or PIV-II (incumbent):	PIV-I	(15) Hired Under Recovery Act?:	☐ Y ☒ N
(16) Card Delivery Site (ex. FORS, SNL, SRS, NETL-PGH, ID, NNSA, SC, GTN):	GTN	(17) Clearance:	☐ Q ☐ L ☒ BAO
Contact Information (To Be Completed by Sponsor or Security Official)			
(18) Contact Name:	Jessica Jones (List an additional person for notifications if applicable)		
(17) Routing Symbol:	AU-43 (Program Office supported)	(20) Date:	01/01/20
(21) Phone:	301-903-1000		
(22) E-mail:	Jessica.Jones@Hq.Doe.Gov		

Contains information which may be exempt from public release under the Freedom of Information Act (5 U.S.C.552), exemption number(s) 6 Personal Privacy. Approval by the Department of Energy prior to public release is required.

Reviewed by _____ Date: 01/01/20

Treat as **Official Use Only** when PII entered.

ATTACHMENT 307-2

DOE F 473.2
(Administrative Update: 03/2013)
All Other Editions Are Obsolete

U.S. DEPARTMENT OF ENERGY
SECURITY BADGE REQUEST

OMB Control No.
1910-1800
OMB Burden Disclosure
Statement on Reverse

TO: Headquarters Physical Protection Team	(J) Date:
(A) FROM: NAME (printed) AND SIGNATURE OF DOE SPONSOR HAVING LIAISON WITH APPLICANT John Wick	(K) U.S. CITIZEN? ☒ YES ☐ NO IF NO, COUNTRY
(B) TITLE Director DIVISION/OFFICE AU-43	(L) REQUEST APPLICANT BE ISSUED: DOE HEADQUARTERS SITE-SPECIFIC SECURITY BADGE (USED AT HQ ONLY) (CHECK ONE): ☒ "BAO" TO HQ Facilities ☐ "FOREIGN NATIONAL" DOE STANDARD SECURITY BADGE (Used at HQ AND Other DOE Sites): (CHECK ONE): ☐ "Q" ☐ "L" ☒ "BAO" (Also Check): ☐ OGA ☐ IPA
I certify that the applicant requires access to a DOE HQS facility to Conduct Official DOE business	(M) BADGE AT: ☐ FORSTL ☒ GTN CONTRACT NUMBER: DOE 12345678 CONTRACT EXPIRATION DATE: 01/01/21
(C) DOE Sponsor Telephone Number: 301-555-5555	
(D) NAME OF APPLICANT (Last) (First) (Middle Name) Givens Raylan Harlan	(N) EMPLOYER CERTIFICATION I certify that a DOE Security badge is required for the applicant to perform official duties in a DOE facility. Pre-employment checks were conducted in accordance with company policy, all checks were favorable, and the applicant was found to be suitable for employment
(E) SOCIAL SECURITY NUMBER 123-45-6789	Jessica Jones Printed Name and Signature Date
(F) APPLICANT'S EMPLOYER NAME (Company Name) Any Company	I concur that the applicant requires access to a DOE facility to perform official duties.
(G) EMPLOYER ADDRESS: 123 Main Street, Anywhere MD, 01234	COR Printed Name and Signature of COR, Routing Symbol Date
(H) EMPLOYER Telephone Number 123-555-5555	I concur that the applicant requires access to a DOE facility to perform official duties
(I) PRIME CONTRACTOR NAME: Another Company	HSO (or Federal Designate) Printed Name and Signature HSO (or Federal Designate), Routing Symbol Date

PRIVACY ACT STATEMENT ON REVERSE

DOE F 473.2 INSTRUCTIONS

- (A), (B), & C **FROM: NAME (printed) AND SIGNATURE, TITLE, DIVISION/OFFICE AND TELEPHONE NUMBER OF DOE SPONSOR HAVING LIAISON WITH APPLICANT**
Provide printed name and signature, title, office and telephone number of DOE Federal employee sponsoring and certifying applicants' need for a security badge.
- (D) & (E) **APPLICANT'S NAME AND SOCIAL SECURITY NUMBER (SSN)**
Applicant's FULL NAME (Last, First and Middle) AND SSN.
- (F), (G), & (H) **APPLICANT'S EMPLOYER NAME, ADDRESS & TELEPHONE NUMBER**
Name, address, and telephone number of the company employing the applicant requiring a security badge.
- (I) **PRIME CONTRACTOR NAME**
Name of company listed as the Prime Contractor for the DOE Contract.
- (J) **DATE**
Date request is being submitted.
- (K) **IS THE APPLICANT A U.S. CITIZEN**
Check YES or NO. If NO, then indicate the country of citizenship.
- (L) **INDICATE BADGE TYPE TO BE ISSUED**
DOE HEADQUARTERS SITE-SPECIFIC SECURITY BADGES are issued to:
- Uncleared (Building Access Only – BAO) contractor employees or other personnel who perform work or require access ONLY at DOE HQ Facilities.
- Foreign Nationals
DOE STANDARD BADGES are issued to:
- Contractor, Other Government Agency (OGA), or Intergovernmental Personnel Act (IPA) employees with DOE HQS clearances.
- Uncleared BAO contractor, OGA, or IPA employees who require access to DOE HQS and other DOE Sites.
NOTE: if the applicant is an OGA or IPA employee, ALSO check the appropriate OGA or IPA box provided.
- (M) **BADGE AT**
Check where the applicant is to be badged; Forrester or Germantown. The DOE F 473.2 must be forwarded to the appropriate badge office location.
CONTRACT NUMBER & EXPIRATION DATE
Provide the Contract Number and Expiration Date of the DOE Contract.
- (N) **EMPLOYER CERTIFICATION**
Designated person employed with the applicant's company authorized to sign the certification.
CONTRACTING OFFICER REPRESENTATIVE (COR) & HEADQUARTERS SECURITY OFFICER (HSO) CONCURRENCES
Printed name/signature and date of the DOE Federal COR overseeing the contract. The printed name/signature and date of the HSO (or Federal employee delegated in writing to sign for the HSO) supporting the DOE Federal Sponsor.

ATTACHMENT 307-3

Declaration for Federal Employment*

(*This form may also be used to assess fitness for federal contract employment)

Form Approved:
OMB No. 3206-0182**GENERAL INFORMATION**

1. **FULL NAME** (Provide your full name. If you have only initials in your name, provide them and indicate "Initial only". If you do not have a middle name, indicate "No Middle Name". If you are a "Jr.," "Sr.," etc. enter this under Suffix. First, Middle, Last, Suffix)

◆ Raylan Harlan Givens

2. **SOCIAL SECURITY NUMBER**

◆ 123-45-6789

3a. **PLACE OF BIRTH** (Include city and state or country)

◆ Germantown, MD

3b. **ARE YOU A U.S. CITIZEN?**☒ YES ☐ NO (If "NO", provide country of citizenship) ◆4. **DATE OF BIRTH** (MM / DD / YYYY)

◆ 01/01/1990

5. **OTHER NAMES EVER USED** (For example, maiden name, nickname, etc)

◆ Ray Givens

6. **PHONE NUMBERS** (Include area codes)

Day ◆ 301-555-5555

Night ◆ 301-555-5555

Selective Service Registration

If you are a male born after December 31, 1959, and are at least 18 years of age, civil service employment law (5 U.S.C. 3328) requires that you must register with the Selective Service System, unless you meet certain exemptions.

- 7a. Are you a male born after December 31, 1959?

☐ YES☒ NO (If "NO", proceed to 8.)

- 7b. Have you registered with the Selective Service System?

☐ YES (If "YES", proceed to 8.)☒ NO (If "NO", proceed to 7c.)

- 7c. If "NO," describe your reason(s) in item 16.

Military Service

8. Have you ever served in the United States military?

☐ YES (If "YES", provide information below)☒ NO

If you answered "YES," list the branch, dates, and type of discharge for all active duty.

If your only active duty was training in the Reserves or National Guard, answer "NO."

Branch	From (MM/DD/YYYY)	To (MM/DD/YYYY)	Type of Discharge

Background Information

For all questions, provide all additional requested information under item 16 or on attached sheets. The circumstances of each event you list will be considered. However, in most cases you can still be considered for Federal jobs.

For questions 9, 10, and 11, your answers should include convictions resulting from a plea of *nolo contendere* (no contest), but omit (1) traffic fines of \$300 or less, (2) any violation of law committed before your 16th birthday, (3) any violation of law committed before your 18th birthday if finally decided in juvenile court or under a Youth Offender law, (4) any conviction set aside under the Federal Youth Corrections Act or similar state law, and (5) any conviction for which the record was expunged under Federal or state law.

9. During the last 7 years, have you been convicted, been imprisoned, been on probation, or been on parole?
- ☐
- YES
- ☒
- NO

(Includes felonies, firearms or explosives violations, misdemeanors, and all other offenses.) If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved.

10. Have you been convicted by a military court-martial in the past 7 years? (If no military service, answer "NO.") If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the military authority or court involved.
- ☐
- YES
- ☒
- NO

11. Are you currently under charges for any violation of law? If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved.
- ☐
- YES
- ☒
- NO

12. During the last 5 years, have you been fired from any job for any reason, did you quit after being told that you would be fired, did you leave any job by mutual agreement because of specific problems, or were you debarred from Federal employment by the Office of Personnel Management or any other Federal agency? If "YES," use item 16 to provide the date, an explanation of the problem, reason for leaving, and the employer's name and address.
- ☐
- YES
- ☒
- NO

13. Are you delinquent on any Federal debt? (Includes delinquencies arising from Federal taxes, loans, overpayment of benefits, and other debts to the U.S. Government, plus defaults of Federally guaranteed or insured loans such as student and home mortgage loans.) If "YES," use item 16 to provide the type, length, and amount of the delinquency or default, and steps that you are taking to correct the error or repay the debt.
- ☒
- YES
- ☐
- NO

U.S. Office of Personnel Management

5 U.S.C. 1302, 3301, 3304, 3326 & 8716

Optional Form 306
Revised October 2011
Previous editions obsolete and unusable

Declaration for Federal Employment*

(*This form may also be used to assess fitness for federal contract employment)

Form Approved:
OMB No. 3208-0182

Additional Questions

14. Do any of your relatives work for the agency or government organization to which you are submitting this form? (Include: father, mother, husband, wife, son, daughter, brother, sister, uncle, aunt, first cousin, nephew, niece, father-in-law, mother-in-law, son-in-law, daughter-in-law, brother-in-law, sister-in-law, stepfather, stepmother, stepson, stepdaughter, stepbrother, stepsister, half brother, and half sister.) If "YES," use item 16 to provide the relative's name, relationship, and the department, agency, or branch of the Armed Forces for which your relative works. ☐ YES ☒ NO
15. Do you receive, or have you ever applied for, retirement pay, pension, or other retired pay based on military, Federal civilian, or District of Columbia Government service? ☐ YES ☒ NO

Continuation Space / Agency Optional Questions

16. Provide details requested in items 7 through 15 and 18c in the space below or on attached sheets. Be sure to identify attached sheets with your name, Social Security Number, and item number, and to include ZIP Codes in all addresses. If any questions are printed below, please answer as instructed (these questions are specific to your position and your agency is authorized to ask them).

Question #13:

Type - Federal Income Taxes

Length - Didn't file 2014, 2015, 2016 taxes/Delinquent since 2014

Amount - \$20,000

Steps taking to resolve - Contacted IRS and have set up payment plan of \$250.00 a month.

Certifications / Additional Questions

APPLICANT: If you are applying for a position and have not yet been selected, carefully review your answers on this form and any attached sheets. When this form and all attached materials are accurate, read item 17, and complete 17a.

APPOINTEE: If you are being appointed, carefully review your answers on this form and any attached sheets, including any other application materials that your agency has attached to this form. If any information requires correction to be accurate as of the date you are signing, make changes on this form or the attachments and/or provide updated information on additional sheets, initialing and dating all changes and additions. When this form and all attached materials are accurate, read item 17, complete 17b, read 18, and answer 18a, 18b, and 18c as appropriate.

17. I certify that, to the best of my knowledge and belief, all of the information on and attached to this Declaration for Federal Employment, including any attached application materials, is true, correct, complete, and made in good faith. I understand that a false or fraudulent answer to any question or item on any part of this declaration or its attachments may be grounds for not hiring me, or for firing me after I begin work, and may be punishable by fine or imprisonment. I understand that any information I give may be investigated for purposes of determining eligibility for Federal employment as allowed by law or Presidential order. I consent to the release of information about my ability and fitness for Federal employment by employers, schools, law enforcement agencies, and other individuals and organizations to investigators, personnel specialists, and other authorized employees or representatives of the Federal Government. I understand that for financial or lending institutions, medical institutions, hospitals, health care professionals, and some other sources of information, a separate specific release may be needed, and I may be contacted for such a release at a later date.

- 17a. Applicant's Signature: Digital or Wet Signature ONLY Date
(Sign in ink)
- 17b. Appointee's Signature: Date
(Sign in ink)

Appointing Officer:

Enter Date of Appointment or Conversion
MM / DD / YYYY

18. **Appointee (Only respond if you have been employed by the Federal Government before):** Your elections of life insurance during previous Federal employment may affect your eligibility for life insurance during your new appointment. These questions are asked to help your personnel office make a correct determination.

- 18a. When did you leave your last Federal job? MM / DD / YYYY
DATE:
- 18b. When you worked for the Federal Government the last time, did you waive Basic Life Insurance or any type of optional life insurance? ☐ YES ☐ NO ☐ DO NOT KNOW
- 18c. If you answered "YES" to item 18b, did you later cancel the waiver(s)? If your answer to item 18c is "NO," use item 16 to identify the type(s) of insurance for which waivers were not canceled. ☐ YES ☐ NO ☐ DO NOT KNOW

U.S. Office of Personnel Management
5 U.S.C. 1302, 3301, 3304, 3328 & 8716

Optional Form 308
Revised October 2011
Previous editions obsolete and unusable

Chapter 4 Revision History: Revisions by date (Newest to oldest)

September 27, 2024

- Reformatted entire document to add sections and provide uniformity with other HQFMSP Chapters.
 - Added SIGMA and SCI access authorization approval requirements.
 - Updated DOE O 470.4b Chg. 2 to reflect latest change DOE O 470.4b Chg.3
 - Updated NISPOM language throughout the document to reflect 32 CFR Part 117, National Industry Security Program Operating Manual (NISPOM) Rule.
 - Reorganized paragraphs for better outline of procedures.
 - Updated Roles and Responsibilities for Facility Security Officer and Headquarters Security Officers (HSOs).
 - Separated Importance Ratings for Possessing and Non-Possessing Facilities.
 - Updated classified contract approval process to better outline timelines and scenarios.
 - Added overarching Federal directives for guidance on the NISP.
 - Added DCSA reciprocity FCL process to Section 402

Chapter 4

Foreign Ownership, Control, or Influence; Facility Clearance; and Classified Contract Registration

This chapter describes the security procedures adopted by the U.S. Department of Energy (DOE) Headquarters (HQ) to implement the requirements of the following directives:

- Executive Order 12829, *National Industrial Security Program*
- 32 CFR Part 117, *National Industrial Security Program Operating Manual (NISPOM) Rule*
- DOE Order 452.8, *Control of Nuclear Weapons Data*
- DOE Order 470.4B Chg. 3, *Safeguards and Security Program*

The objectives of these directives are to outline the process that contractors undergo to be authorized to perform classified work for the United States Government and the DOE.

- Section 401 identifies the roles and responsibilities of HQ and contractor personnel involved in the Foreign Ownership, Control, or Influence (FOCI) / Facility Clearance (FCL) Program
- Section 402 discusses the requirements and procedures for registering contractor and Federal facility clearances.
- Section 403 describes the requirements and procedures used to register, extend, request reciprocity, terminate classified contracts, and the process for transferring and terminating facility clearances.
- Section 404 discusses the recurring requirements for Facility Security Officers to ensure their facilities remain in compliance with DOE Directives.

Section 401

FOCI/FCL Program Roles and Responsibilities

HQ elements seeking to award classified contracts must ensure that prospective contractors are eligible to access DOE classified information. This eligibility process involves three-steps: obtaining a FOCI determination, obtaining a FCL; and registering classified contracts within DOE's Safeguards and Security Information Management System (SSIMS).

At HQ, all these actions are performed within the Office of Headquarters Industrial Security Operations (EHSS-42), within the Office of Headquarters Security Operations (EHSS-40).

HQ Implementation Procedures

HQ FOCI/Facility Clearance and Operations Program Manager:

The Director, EHSS-40, appoints an individual within EHSS-42 to serve as both the HQ FOCI Operations Program Manager and the HQ Facility Clearance and Approval Program Manager. The HQ FOCI/Facility Clearance and Operations Program Manager is responsible for receiving, reviewing, and approving FOCI submissions, FCL requests, and classified contract registration documentation.

Procurement Request Originators:

Procurement Request Originators (PROs) are officials within each HQ element authorized to initiate a request for goods or services provided through a contractor. PROs must thoroughly understand the nature of the goods or services they are requesting.

When a PRO initiates a request for services that requires access to classified information, he/she must know the level and category of the classified information to be accessed, whether special accesses are required, what security clearances are needed, and whether the contractor will maintain classified information at its own facility or perform the classified work within DOE facilities.

Contracting Officers:

All HQ Contracting Officers (COs) are part of the Office of Acquisition Management (MA-60). COs are responsible for analyzing procurement requests, developing solicitations, analyzing bids, ensuring the eligibility of bidding companies, letting contracts, and ensuring that the required security clauses are included in the contracts, when appropriate. COs are the official point of contact with the contractors and are ultimately responsible for ensuring that HQ contractors performing classified work comply with DOE security requirements.

Contracting Officer's Representatives:

Contracting Officer Representatives (CORs) are the Federal employees within each HQ element who monitor a contractor's performance on behalf of the CO. CORs work closely with the HQ FOCI/Facility Clearance team concerning DOE requirements for updating FOCI, FCL, and contract information. CORs verify the need for contractor employees to obtain a security clearance, provide the information needed to register classified contracts in SSIMS, and notify the HQ FOCI/Facility Clearance and Operations Program Manager when a new classified contract must be registered. The COR must also contact the HQ FOCI/Facility Clearance team when an existing contract needs to be renewed, modified, or terminated, at least 30 days prior to expiration date. CORs should also maintain a list of all cleared individuals under their purview.

Facility Security Officer:

A Facility Security Officer (FSO) is a contractor employee specifically identified to perform security functions on behalf of their contract employer and considered a Key Management Personnel (KMP) per NISPOM requirements. The FSO is responsible for understanding DOE security requirements and ensuring the contractor complies with national policy and governing directives. The FSO must notify DOE of any significant changes to include but not limited to company ownership, changes of address, changes in KMP, change of physical location of approved FCL, etc. The FSO must complete the Facility Security Officer Overview Course, available on the DOE Learning Nucleus site. FSO training is required by DOE O 470.4B, Chg. 3 and must be completed within one year after a DOE FCL has been granted or formal FSO designation has been made by contracting company leadership.

Headquarters Security Officers (HSOs):

HSOs are responsible for reviewing and submitting security clearance packages for contractor employees to DOE HQ Personnel Security, to include all KMP (see Section 301, Acquiring New Security Clearances). Before a request for a security clearance is submitted, HSOs ensure that all the classified contract-related information is registered in SSIMS. If the information is not registered in SSIMS, the HSO will work with the responsible COR to submit the required documentation to the FOCI/FCL Team for entry into SSIMS. When the FOCI/Facility Clearance and Approval Program Manager identifies the KMP and FSO for the company, the HSO will be notified. The HSO will coordinate with the FSO to complete clearance paperwork for KMPs and submit the documentation to the Office of Headquarters Personnel Security Operations within two weeks of the identification of the KMP. The clearance process for the KMPs may take at a minimum of 5 days if the individuals can be granted a DOE clearance via reciprocity. If a KMP cannot be reciprocally granted a clearance, they must be submitted as an applicant, which will increase the timeframe for granting the clearance as a background investigation will be required (more information on Security Clearance Actions can be found in the HQFMSP, Chapter 3, Section 303). HSOs are provided a copy of the completed DOE F 470.1, *Contract Security Classification Specification* (CSCS), which is used to register classified contracts in SSIMS. HSOs can request copies of completed CSCS and FDAR by contacting the HQ FOCI FAC TEAM to verify that the contract has been entered into SSIMS.

HSOs must be aware of all classified contracts that are in place to support their respective program office; therefore, HSOs must maintain copies of all registered CSCS and DOE F 470.2, *Facility Data and Approval Record* (FDAR). HSOs can request a copy of the contractor's FDAR by emailing HQ FOCIFACTEAM. HSOs must use these forms to enter the data into their element's Appendix to the HQFMSP. HSOs must remain in contact with the FSOs for each contract under their purview to help facilitate any changes necessary to keep company FCLs in compliance.

Points of Contact

For the names and contact information for those occupying the positions identified in this section, call (202) 309-8817 or 301-903-9990.

Section 402

Facility Clearance Registration

When a contract or business need requires employees to have access to classified information, the company or Federal facility requires a DOE FCL be granted. DOE FCLs are documented on the FDAR. Contractor and Federal facilities will fall under two categories: possessing and non-possessing.

HQ Implementation Procedures

Possessing Facilities:

The HQ Survey Team must conduct an initial survey. After the HQ Survey Team verifies that the contractor meets all applicable DOE security requirements, they issue DOE F 470.8, *Survey/Inspection Report Form*, which serves as the basis for issuing a FCL based on the Importance Rating of the work assigned to the contractor.

Importance Rating A – Issued to a facility approved to store TS matter

Importance Rating B – Issued to a facility approved to store S/RD matter

Importance Rating C – Issued to a facility approved to store all other levels and categories of classified matter

Importance Rating D – Issued to such facilities as common carriers, commercial carriers, or mail service contractors that are not authorized to store classified matter during nonworking hours

Importance Rating PP – Issued to a facility that stores government property of significant monetary value (more than \$5 million, exclusive of facilities and land values)

Non-Possessing (NP) Facilities:

The HQ Survey Team does not survey NP facilities, but the HQ FOCI/Facility Clearance and Operations Program Manager requires NP facilities to submit a *Plan for Non-Possessing Facilities*.

Importance Rating NP – Issued to a Non-Possessing (NP) facility that is not authorized to possess or store classified matter but whose contractor personnel perform classified work at an HQ facility. The NP rating permits contractor employees to be processed for a security clearance.

Importance Rating E – Issued to Excluded Parents, which is related to the FOCI Program.

FCL Clearance Requirements and Processing:

After the level of FCL has been determined for a contractor facility, and prior to the FCL being granted, the following action must be completed:

1. The HQ FOCI/Facility Clearance and Operations Program Manager will work with the company FSO and HQ element HSO to identify the company's KMP. Per NIPSOM requirements, KMP must be cleared to the level of the requested FCL prior to the FCL being granted.
2. DOE requires, at a minimum, the Senior Management Official (SMO), Facility Security Officer (FSO), and the Insider Threat Senior Program Official (ITPSO) be cleared to the level of the requested FCL. (**Note. Other identified KMP can be temporarily excluded from possessing the appropriate clearance for the purposes of granting a DOE FCL. Contact the HQ FOCI/FCL Team for exclusion procedures. **)
3. To facilitate KMP clearances being processed, the HQ FOCI/FCL Team will complete the FDAR and place the contractor facility in an "Awaiting Activation" status in SSIMS. A copy of the "Awaiting Activation" FDAR will be provided to the HQ element HSO, COR, CO, and EHSS-43 for KMP processing.
4. Once the required KMP are cleared, the contractor facility will be placed in an active status in SSIMS.
5. The HQ FOCI/FCL Team will provide the completed FDAR to the company FSO and responsible HSO to continue classified contract registration.

Reciprocal FCLs

If a contractor has an active FCL with an OGA under the National Industrial Security Program (NISP), the HQ FOCI/FCL Team will request FCL reciprocity from the OGA. Estimated time for this process may vary depending on the status or pending significant changes. The HQ FOCI/FCL Team will ensure the following:

1. That a Memorandum of Agreement to the cognizant security agency requesting reciprocal use of the FCL to register the contractor for access to classified DOE requirements
2. That the FCL granted by the OGA is at the appropriate classification level and category or that cognizance is requested if the DOE facility security level needed exceeds what the OGA has granted
3. That KMPs are processed and granted the appropriate access authorization level
4. That State, local, tribal, and other similar governmental authorities will not be registered as OGAs and will be handled in accordance with Executive Order 13549, *Classified*

National Security Information Program for State, Local, Tribal, and Private Sector Entities

5. If the contract is cleared under a Voting Trust Agreement, Proxy Agreement, Special Security Agreement, or Security Control Agreement, a copy of the FOCI mitigation plan is obtained from the cognizant OGA
6. Assurance is obtained from OGA that the FCL will not be canceled prior to the DOE cognizant security office being notified.

Registering OGA FCLs and Their Contractors in SSIMS

OGAs and their contractors must be registered in SSIMS to perform classified work for DOE or receive classified information from DOE. The requesting HQ element will consult with the HQ FOCI/Facility Clearance and Operations Program Manager to initiate and complete the registration process. The SSIMS registration must be completed by the HQ FOCI/Facility Clearance and Operations Program Manager.

If an OGA possessing facility is not registered in SSIMS, the requesting HQ element must send a *Statement of Security Assurance* (SSA) to the OGA security officer to complete and sign. The SSA must be returned to the HQ element and forwarded to the HQ FOCI/Facility Clearance and Operations Program Manager. Upon review by the HQ FOCI/Facility Clearance and Operations Program Manager, the SSA is used to develop the FDAR required to register the OGA in SSIMS. The SSA requires the OGA's security officer to notify the sponsoring DOE HQ Program Office and the HQ FOCI/Facility Clearance and Operations Program Manager if any changes are made to the information recorded in SSIMS. The SSA is valid for three (3) years from the date of entry into USSIMS and must be revalidated for continued access. The sponsoring DOE HQ Program Office must maintain accountability of SSAs under their purview and coordinate the revalidation and continued need for access of OGAs. The sponsoring DOE HQ Program Office must notify the HQ FOCI/Facility Clearance and Operations Program Manager within 30 days of expiration of the SSA to coordinate revalidation requirements.

When a DOE HQ element establishes a need-to-know for an OGA contractor (OGAC) without a contractual arrangement to receive classified matter. The Classified Mailing Address (CMA) for the OGAC may be verified in the National Industrial Security System (NISS) which is the Defense Counterintelligence and Security Agency (DCSA) system of record.

If an OGAC is not registered in SSIMS or NISS, the HQ FOCI/Facility Clearance and Operations Program Manager should be consulted for requirements.

Points of Contact

For the names and contact information for those occupying the positions identified in this section, call (202) 309-8817 or 301-903-9990.

Forms/References

[DOE F 470.2, Facility Data and Approval Record](#)

[DOE F 470.8, SURVEY/INSPECTION REPORT FORM](#)

[Statement of Security Assurance.](#)

Section 403

Classified Contract Lifecycle

DOE requires all classified contracts to be registered in SSIMS. To achieve this registration, the process in this section must be followed to ensure that prospective contractors are eligible to access DOE classified material. This section also provides guidance on security procedures associated with classified contract modification and termination as well as processes involved with the transfer and termination of FCLs.

HQ Implementation Procedures

Approving Classified Contracts:

When a PRO determines a need for contractor good or services, the PRO must complete DOE F 4200.33, *U.S. Department of Energy Procurement Request - Authorization*. Question 41 of this form identifies contract requires security clearances. If the contract does require security clearances, the PRO is instructed to attach a CSCS to the DOE F 4200.33. The CSCS provides the security classification requirements and justifies the contractor's need for a FOCI determination and FCL. The PRO submits these two forms to his/her servicing CO.

After the PRO submits the CSCS and DOE F 4200.33 to the CO, the CO will prepare the solicitation, receive bids, consider the bids, and makes a tentative selection.

- ❖ As part of the solicitation process, the CO will include the cursory FOCI review questionnaire to the potential contractors to aide in the selection process. This cursory review will identify if a prospective awardee will be required to undergo a FOCI review and determination, or if the company has an existing FOCI determination and FCL with DOE or OGA. This review should be returned to the HQ FOCI/FCL Team 30 days prior to a tentative selection being made.

Once a tentative selection is made, the CO will contact the HQ FOCI/Facility Clearance and Operations Program Manager, and requests confirmation that the contractor has a favorable FOCI determination on file with DOE or OGA. The following outcomes will occur:

1. If the contractor already has a favorable FOCI determination on file:
 - a. The HQ FOCI/Facility Clearance and Operations Program Manager informs the CO within 5 days of the tentative selection notification.
 - b. The CO or COR must forward the completed CSCS and a copy of the fully executed awarded contract listing all option years for the period of performance, to the HQ FOCI/Facility Clearance and Approval Program Manager.
 - c. The HQ FOCI/Facility Clearance and Operations Program Manager reviews the CSCS to identify the appropriate FCL. The FCL must be granted before the

contractor and its employees can access classified matter. Prior to a DOE FCL being granted, all required KMP must possess a security clearance commensurate with the level of the FCL.

- d. Upon registration in SSIMS, a copy of the completed CSCS and company FDAR is sent to the HSO to submit for security clearances for the contractor employees supporting the approved contact. A contractor cannot be granted a security clearance unless the CSCS for that contract has been entered into SSIMS.
 - e. A copy of the completed CSCS will also be provided to EHSS-43 and the Badging Office by the HQ FOCI/FCL Team.
2. If the company tentatively selected to perform the contract does not have a FOCI determination:
- a. The company is required to submit a FOCI package for review by the HQ FOCI/Facility Clearance and Operations Program Manager.
 - b. The FOCI package must be submitted electronically via the e-FOCI website. The website provides complete information about the e-FOCI submission system and the required documentation. The length of this process will depend on the company's ownership, structure, and business ventures. Estimated time may vary depending on the content submitted and if there is any FOCI which requires mitigation. The HQ FOCI/Facility Clearance and Operations Program Manager renders a FOCI determination after considering all the information submitted by the contractor.
 - c. Once a FOCI determination is made, the CO and COR will be notified.
 - d. The CO and COR will then follow the same processing guidelines outlined above.
 - e. Sensitive Compartment Information access: If the contract requires access to Special Compartmentalized Information (SCI), a signature is required by the DOE HQ Special Security Officer or Director of Intelligence. This coordination for approval must be completed by the respective CO or COR prior to submission to the HQ FOCI/Facility Clearance and Operations Program Manager for registration in SSIMS.
 - f. SIGMA access: Upon determination of SIGMA access authorization. The CO or COR is responsible for coordinating with the respective SIGMA Control Office(s) to obtain approval for SIGMA program authorization.
 - i. SIGMA 14/15 access:
 1. NA 122.4: Weapon Security and Control Division
 - ii. SIGMA 20:
 1. NA 82: Office of Nuclear Threat Science

Depending on whether a contract entity maintains an active FCL and if there are any pending change conditions or significant changes, the timing of completing and registering a CSCS in SSIMS may vary. The FCL will not be granted and the CSCS will not be processed, until all required KMP are cleared at the level required for the classified contract.

Extension of Classified Contracts:

When the period of performance for a classified contract is nearing the end date identified in SSIMS. The CO and/or COR must notify the HQ FOCI/Facility Clearance and Operations Program Manager period of performance (PoP) date on the CSCS must be updated to reflect the contract modification and entered SSIMS. This may be accomplished by completing a 'change' CSCS and providing a signed copy of the contract modification pages (which includes the new period of performance) to the HQ FOCI/Facility Clearance and Operations Program Manager. The CO and COR responsible for the contract are authorized to sign the 'change' CSCS and are the only DOE officials authorized to revise the contract period of performance. Before being sent to the HQ FOCI/Facility Clearance and Operations Program Manager, the 'change' CSCS and contract modification must be reviewed and approved by the supporting Classification Officer. For bridge contracts that have been issued a new contract number, a 'new' CSCS must be completed and signed by the CO, COR, and supporting Classification Officer.

The extension CSCS must be submitted by the CO or COR 30 days prior to the expiration date. This is necessary for the Office of Headquarters Personnel Security Operations and the DOE HQ Badging Office, to process all badges and avoid the stop of work for the company's employees.

Termination or Transfer of Facility Clearances and Classified Contracts:

Upon completion or termination of a classified contract the following actions must occur:

1. Within 30 days of contract completion or termination, the CO or COR must complete a 'termination' CSCS and submit it to the HQ FOCI/Facility Clearance and Operations Program Manager for entry into SSIMS.
2. In conjunction with the 'termination' CSCS, the HSO must complete the [Security Activity Closeout Certificate \(SACC\)](#) for the prime contract and each of its subcontractors registered in SSIMS. The HSO must obtain the contractor FSO signature for completion of the SACC.
3. The HQ Survey Team performs a Termination Survey on possessing facilities to ensure that the contractor has properly disposed of DOE classified information and other security assets. Termination Survey results are documented on DOE F 470.8.

If the employees of the terminated contract will not transfer to another classified contract or be employed by a new contractor, all security clearances must be terminated (see [Chapter 3](#), Other Actions). All security badges issued to contractor employees must be returned to DOE control. (DOE O 470.4B Chg.3, App. B, Sec.1, Ch.9, 1.b)

Points of Contact

For the names and contact information for those occupying the positions identified in this section, call (202) 309-8817 or 301-903-9990.

To verify that a specific classified contract has been entered into SSIMS, send an e-mail to [HQ FOCI FAC TEAM](#)

Forms/References

[DOE F 470.1, Contract Security Classification Specification](#)

[DOE F 4200.33, Procurement Request Authorization](#)

[Security Activity Closeout Certification](#)

Section 404

Recurring Requirements for FSOs

FSOs are required to manage the protection of all DOE classified material under their company's purview. To ensure company FCLs remain in compliance with DOE and Federal directives FSOs must satisfy the following requirements:

1. Annual reviews are required for companies with a FOCI mitigation, companies with parent organizations excluded by formal resolution, or organizations that have filed board resolutions to reduce non-controlling foreign ownership.
2. Companies that are not required to report annually are subject to random reviews throughout the duration of their FCL lifecycle with DOE HQ. Companies will need to respond within 5 business days of notification of review. A delayed response could result in the suspension of the company's FCL.
3. DOE must be informed when certain information about a contractor changes. The contractor's FSO must notify DOE within one week of the changes via the e-FOCI website. The following changes are reportable:
 - a. Changes in ownership, including stock transfers that affect control of the company.
 - b. Changes in the operating name or address of the company or any of its cleared branch locations.
 - c. Any change in KMP by submission of a 'significant change'. If a KMP does not have an active clearance, this can result in the suspension of the company's FCL. A Temporary Exclusion may be an option until the KMP is cleared with DOE.
 - d. Actions to terminate business or operations for any reason, including involvement in adjudication of or reorganization in bankruptcy
 - e. Written notification of any changes affecting FOCI or the answers to the questions presented in the latest Certificate Pertaining to Foreign Interests, or any changes in ownership or control that must be reported to the Securities and Exchange Commission, the Federal Trade Commission, or the Department of Justice.

Points of Contact

For the names and contact information for those occupying the positions identified in this section, call (202) 309-8817 or email the [HQFOCI/FCL Team](#).

Forms/References

Standard Operating Procedure for:

- Facility Clearance and Registration of Safeguards and Security Activities,
- Recording of Security Incidents,
- Equivalences and Exemptions, and
- Foreign Ownership, Control or Influence are Official Use Only, please contact the [HQ FOCI/Facility Clearance Team](#) for a copy.

Chapter 5

Classified Matter Protection and Control

This chapter describes the security procedures adopted by DOE HQ to implement the requirements of the following DOE directives:

- 32 CFR 2001 and 2003, *Implementing Directive*
- Atomic Energy Act of 1954, as amended
- Executive Order 13526, Classified National Security Information
- National Security Act of 1947, as amended
- Executive Order 12333, United States Intelligence Activities, as amended by Executive Order 13355
- DOE Order 471.6, *Information Security*
- DOE Order 475.2A, *Identifying Classified Information*
- DOE Order 452.8, *Control of Nuclear Weapon Data*
- *DOE CMPC Marking Resource*
- Classification Bulletin TNP-32, *Classification Guidance for Classified Meeting Locations at DOE/NNSA or DOE/NNSA Contractor Sites or Facilities*, dated May 27, 2010

The common objective of these directives is to protect classified information from unauthorized disclosure to potential adversaries who may wish to attack U.S. security interests, harm the American people, or develop weapons of mass destruction.

- Section 501 describes the roles and responsibilities of HQ employees who have access to, possess, or generate classified information. It also outlines the roles and responsibilities of those involved in administering the Classified Matter Protection and Control (CMPC) Program at HQ. Finally, it lists the various training requirements for personnel with Q and L security clearances and those performing specialized CMPC functions.
- Section 502 briefly describes the HQ classification program and the appointment of Classification Representatives.

- Section 503 describes the three categories and three levels of classified information in use throughout the U.S. government, special designators unique to DOE, and other special handling controls.
- Section 504 describes the specialized topic of identifying and handling classified or sensitive information generated by foreign governments.
- Section 505 describes the procedures for preparing and marking classified matter. The *DOE CMPC Marking Resource* is an invaluable tool for properly marking all types of classified matter.
- Section 506 describes how to protect classified matter while it is out of its normal storage container and in use.
- Section 507 describes the procedures and equipment required to properly store classified matter.
- Section 508 describes the procedures for reproducing classified matter and identifying the equipment that can be used.
- Section 509 defines what classified matter must be accounted for and the accountability mechanisms to be used by HQ elements.
- Section 510 discusses the requirement for each HQ element that receives or dispatches classified matter to establish a Classified Document Control Station (CDCS) to centrally manage such transmittals. It provides general operating instructions and training requirements for CDCS operators.
- Section 511 describes the procedures to be followed in receiving and transmitting classified matter, including the mailing, hand carrying, and electronic transmission of classified matter.
- Section 512 describes the procedures for identifying the mailing addresses to be used in sending classified matter to facilities operated by DOE and other government agencies.
- Section 513 deals with the use of Express Mail Services to send and receive classified matter.
- Section 514 describes the procedures and equipment required to properly destroy classified matter.

Section 501

Classified Matter Protection and Control Roles and Responsibilities

Individuals granted security clearances by the U.S. government are responsible for protecting the classified matter with which they are entrusted. This responsibility means the person has a duty to control access to the information and ensure that it is not disclosed to unauthorized persons. There is a two-part test to determine whether classified information can be shared with another person: 1) Does the other person have a security clearance that permits access to the classified matter? and 2) Does the other person have “need-to-know” for that classified information? If the answer to either question is “no,” the classified information cannot be disclosed to the other person.

Numerous rules and procedures apply to the protection and control of classified matter. This section describes the basic responsibilities of persons entrusted with classified information; subsequent sections describe specific protective measures in much greater detail.

The DOE HQ Classified Matter Protection and Control (CMPC) Program is managed by the Office of Information Security (HS-92).

HQ Implementation Procedures

HQ CMPC Program Manager:

The Director, HS-90, has appointed a single individual within HS-92 to serve as the HQ CMPC Program Manager. The CMPC Program Manager is responsible for developing HQ-wide CMPC procedures to implement the requirements of applicable laws, Executive Orders, and DOE directives.

Performance Plan Element:

All HQ Federal employees with a Q or L security clearance must have an element in their Performance Plans describing their responsibilities for protecting classified information. A commonly accepted Performance Plan Element is:

Goal Linkage: Ensure that classified information is protected under conditions that prevent compromise or access by unauthorized persons. (DOE Goal 3: Enhance nuclear security through defense, nonproliferation, and environmental efforts.)

Results-Focused Critical Element with Credible Measure(s): Properly handles, classifies, processes, stores, reproduces, transmits, and destroys classified information to prevent its loss, compromise, or unauthorized disclosure.

Weight: As determined by the employee's supervisor.

Comprehensive Security Briefing:

Title 32 CFR 2001 and DOE policy require that all individuals who are authorized to access classified information must receive instruction with respect to their specific security duties as necessary to ensure that they are knowledgeable of their responsibilities and applicable requirements. The instruction is provided in a Comprehensive Security Briefing, which is administered by the servicing badge office when the employee first receives an HQ security clearance and security badge reflecting his/her clearance level and before he/she is authorized access to classified information, an LA, or a VTR. Via video presentation and written materials, the briefing describes the requirements for proper handling and storage of classified matter, access control procedures for LAs and VTRs, escort requirements, penalties for mishandling classified information, controlled articles, and other topics associated with the protection of classified matter.

Upon completion of the Comprehensive Security Briefing, the employee is required to read and sign SF-312, *Classified Information Nondisclosure Agreement*, with the briefing official signing as the witness. The signed SF-312 documents the employee's completion of the Comprehensive Security Briefing. Any employee who fails to complete the SF-312 will have his/her access authorization terminated and will be denied access to classified matter. The badge offices maintain records of who completed the briefing and their signed SF-312s, which are retained for a period of 70 years.

Annual Security Refresher Briefing:

All HQ employees, both Federal and contractor, with a Q or L security clearance must complete an Annual Security Refresher Briefing. This computer-based briefing summarizes DOE security requirements, the threat to national security interests, and other matters concerning the proper handling and storage of classified matter. Personnel who are required to take the briefing receive an automated message advising them how to access the briefing, establishing a required completion date, and advising how to print a completion certificate. The automated system has an integrated audit capability to track who has completed the briefing. HSOs are required to monitor who within their element has not completed the briefing and take action to ensure that their element achieves a 100% completion rate.

Specialized CMPC Training:

Title 32 CFR 2001, Section 2001.71 requires specialized CMPC security training for security managers, security specialists, and all other personnel whose duties significantly involve the handling of classified information. In addition, for HQ positions, specialized training is required for HSOs, Alternate HSOs, and HSO Representatives representing

elements that handle classified information; CDCS operators; classified document couriers; and mailroom personnel. This training should be completed before or concurrent with the date the employee assumes any of the positions listed above, but in any case no later than six months from that date.

It is the responsibility of the Head of Element to determine which of the element's employees require specialized CMPC training and ensure that the identified employee(s) complete the training. Note that specialized training requirements may change (e.g., when an employee is assigned new security responsibilities or when an employee is involved a security incident regarding the mishandling of classified matter).

The HQ CMPC Program is responsible for developing specialized CMPC training courses and making the training available to the HQ Federal and contractor population.

The HQ CMPC Program Manager has developed and conducts specialized training courses for HQ personnel with specific security responsibilities. For example, there are training courses in:

- Classified document control station operations
- Congressional courier operations
- Classified document courier operations
- Hand carrying classified matter.

On request, the HQ CMPC Program Manager also develops and presents individualized CMPC courses for HQ organizations with specified requirements.

Specialized training courses are available throughout the year. HSOs are advised when many of these training opportunities are available and may nominate their organizational personnel to attend. Additionally, organizational management, or the HSO, may submit requests for specialized CMPC training at any time during the year.

Other CMPC Training:

The DOE National Training Center (NTC) in Albuquerque, New Mexico offers a variety of specialized CMPC courses. The HQ element is responsible for sponsoring and funding the attendance, travel, and other actions associated with their personnel attending NTC courses. NTC delivers their training both in Albuquerque and in a variety of other ways, including computer-based training, correspondence courses, and Mobile Training Teams. A link to the NTC website and course catalog is included in the Helpful Websites subsection below. The NTC website fully describes NTC's course offerings, schedule, and points of contact.

Points of Contact

For the names and contact information for those who occupy the positions identified in this section, call (301) 903-9990 or (301) 903-1163.

Helpful Websites

<http://www.ntc.doe.gov>

<http://www.hss.energy.gov/HQSecOp/cmhc.html>

Section 502 Classification

DOE Order 475.2A, *Identifying Classified Information*, establishes DOE's program for classifying and declassifying information and specifies requirements and responsibilities for implementing this program. This order also describes the procedures for classifying and declassifying information, documents, and material, as well as the associated processes, such as training, classifier appointments, and authority descriptions. These standard procedures are in use throughout DOE HQ.

HQ Implementation Procedures

- HQ elements that have employees who generate classified information, documents, or material must appoint a Classification Representative to assist individuals within the element implement the requirements in DOE Order 475.2A. To identify an element's Classification Representative, contact the Office of Classification's outreach program at 301-903-7567 or outreach@hq.doe.gov.
- Any document that is in a classified subject area and that might contain classified information must be reviewed by a Derivative Classifier (DC) with appropriate authority.
- Before a classified document can be declassified or have classified information removed (redacted), it must be reviewed by a Derivative Declassifier with the appropriate authority.
- When a document needs to be classified or declassified, contact the element's Classification Representative or the Office of Classification's outreach program to determine who the DCs or Derivative Declassifiers are within the element.
- When a document was issued as Unclassified or at too low a level or category, its classification must be upgraded. In such a case, the DC should notify the Office of Classification (HS-60) immediately after making the upgrade.
- All documents in a classified subject area that are intended for public release, or for submittal to Congress as Unclassified, must be reviewed by HS-60 or the NNSA Office of the Associate Administrator for Defense Nuclear Security (NA-70).

Points of Contact

For information about the Classification Program, call (301) 903-7567 or (301) 903-1163.

Helpful Websites

The Office of Classification's website is at: <http://hss.energy.gov/classification/>

To view the *DOE CMPC Marking Resource*, go to:

http://www.hss.energy.gov/SecPolicy/DOE_CMPC_Marking_Resource.pdf

Section 503

Types of Classified Matter

This section describes the levels and categories of classified matter in use throughout the U.S. government and the types of classified information that are unique to or controlled by DOE and/or DOE HQ.

Access to Classified Matter

Only personnel who have an appropriate security clearance and need-to-know are permitted to access classified matter. Additional access limitations may be indicated for classified matter through the use of control caveats or special control markings.

HQ Implementation Procedures

Classified information is defined as any information or material that has been determined by the U.S. government, pursuant to an Executive Order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security. There are four categories and three levels of classified matter. Categories and levels of classified information may exist in various forms, such as documents, matter, media, parts, or weapons systems.

Levels of Classified Information:

- Top Secret (TS) – The **Top Secret** classification level is applied to information, the unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security.
- Secret (S) – The **Secret** classification level is applied to information for which the unauthorized disclosure reasonably could be expected to cause serious damage to the national security.
- Confidential (C) – The **Confidential** classification level is applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

Categories of Classified Information:

- Restricted Data (RD) – All data concerning design, manufacture, or utilization of atomic weapons; production of [special nuclear material](#); or use of in the production of energy, excluding data declassified, and data removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954 (https://powerpedia.energy.gov/wiki/Atomic_Energy_Act_of_1954).

- Formerly Restricted Data (FRD) – [Classified information](#) jointly determined by the [Department of Energy](#) or its predecessor agencies and the [Department of Defense](#) to be related primarily to the military utilization of atomic weapons, and can be protected in a manner similar to [National Security Information](#).
- National Security Information (NSI) – Any information that has been determined, pursuant to Executive Order 13526, *Classified National Security Information* (http://en.wikipedia.org/wiki/Executive_Order_13526), or any predecessor order, to require protection against unauthorized disclosure and that is so designated.
- Transclassified Foreign Nuclear Information (TFNI) – Restricted Data information concerning the Atomic Energy programs of certain other nations that was removed from the RD category by joint DOE and CIA agreement for use by the Intelligence Community and safeguarded under Executive Order 13526.

Caveats and Special Controls (for classified matter):

Caveats and special control markings identify special handling or dissemination requirements and help describe the type of information involved, or who distributed or originated the information.

1. Caveats:

- Foreign Government Information (FGI) – See Section 504, Classified Foreign Government Information, for more detailed information
- Director of National Intelligence (formerly Director of Central Intelligence) – These markings are restricted, except as noted, to intelligence matter:
 - o No Foreign Dissemination (NOFORN); may also be used on Naval Nuclear Propulsion Information (NNPI)
 - o Originator Controlled Information (ORCON)
 - o Proprietary Information (PROPIN)
 - o Authorized for Release To (REL TO); usually used in conjunction with NOFORN
 - o Releasable by Information Disclosure Official (RELIDO).

NOTE: No Dissemination to Contractors (NOCONTRACT) and Warning Notice: Sensitive Intelligence Methods or Sources Involved (WNINTEL) designations are obsolete, but remain applicable on the documents that bear these markings until such time as the document is re-reviewed and re-marked.

2. Special Control Requirements:

- North Atlantic Treaty Organization (NATO)
 - o COSMIC TOP SECRET
 - o ATOMAL
 - o CRYPTO.
- Weapon Data

- o Sigma Category (SIGMA) (14; 15; 18; 20)
 - o Critical Nuclear Weapons Design Information (CNWDI) – Department of Defense designation TS or S/RD revealing the theory of operation or design of the components of a thermonuclear implosion-type fission bomb, warhead, demolition munition, or test device.
- Naval Nuclear Propulsion Information – NNPI may be classified or unclassified and must also be annotated NOFORN.
- Special Category (SPECAT)
- Dissemination and Reproduction Notices
 - o FURTHER DISSEMINATION ONLY AS AUTHORIZED BY GOVERNMENT AGENCY
 - o REPRODUCTION REQUIRES APPROVAL OF ORIGINATOR

Points of Contact

For information about the HQ CMPC Program, call (301) 903-9990 or (301) 903-1163.

Helpful Websites

The HQ CMPC Program website is at: <http://www.hss.energy.gov/HQSecOp/cmhc.html>

To view DOE Order 471.6, *Information Security*, go to:
<https://www.directives.doe.gov/directives/471.6-BOrder/view>

To view the *DOE CMPC Marking Resource*, go to:
http://www.hss.energy.gov/SecPolicy/DOE_CMPC_Marking_Resource.pdf

This page intentionally left blank.

Section 504

Classified Foreign Government Information

This section describes DOE HQ procedures for identifying and handling FGI. FGI requires protection pursuant to an existing treaty, agreement, bilateral exchange, or other obligation. FGI is defined as information that is:

- Provided to the U.S. government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;
- Produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any elements thereof, requiring that the information, the arrangement, or both are to be held in confidence; or
- Received and treated as “Foreign Government Information” under the terms of a predecessor order.

NOTE: North Atlantic Treaty Organization (NATO) information is FGI but must be safeguarded in compliance with NATO procedures (United States Security Authority for NATO Affairs [USSAN] 1-07).

HQ Implementation Procedures

General Requirements:

All FGI is classified national security information as defined by Executive Order 13526. The release or disclosure of classified FGI to any third country must have the prior consent of the originating government if required by treaty, agreement, bilateral exchange, or other obligation.

FGI must retain its original classification markings or be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Consult the *DOE CMPC Marking Resource* Foreign Government Markings Table.

TS/FGI, S/FGI, and C/FGI should be stored separately from other classified information, either in a separate approved classified repository or in separate drawers in a GSA-approved security container.

If the original markings in the foreign government documents are readily recognizable as relatable to a U.S. classification requiring special protection and control, the documents do not require re-marking.

If the foreign government marking is not readily recognizable as related to a U.S. classification, the foreign government document must be reviewed by a DC, and an equivalent U.S. classification must be applied.

Review by a DC is not required to apply a U.S. classification level that provides at least an equivalent level of protection to a document or material classified by the foreign government. Documents generated by DOE personnel that contain FGI must be reviewed by a DC with appropriate authority.

An incoming FGI classified document is considered to be classified in its entirety. Portion markings are not required to be added to the document; however, portion marking is required when a newly created FGI document contains U.S. information.

Accountability of FGI:

- **TS/FGI** – All TS/FGI is accountable. Reproduction requires the consent of the originating government. Destruction must be accomplished by two individuals and a Destruction Certificate must be completed by both individuals to record the actual destruction.
- **S/FGI** – S/FGI requires modified accountability. Records must be kept for receipt, external transfer, destruction, and reproduction. Unless prohibited by the originator, S/FGI may be reproduced, and reproduction must be recorded unless the requirement is waived by the originator. Destruction must be accomplished by two individuals, and a Destruction Certificate must be completed by both individuals to record the actual destruction.
- **C/FGI** – Accountability records need not be retained for C/FGI unless the originator establishes a requirement for such records.

Confidential/Foreign Government Information – Modified Handling Authorized:

For some FGI, the foreign government protection requirement may be lower than the protection required for U.S. Confidential information; however, the foreign government still expects that the information will be held in confidence. In such cases, the document is handled as Confidential – Modified Handling Authorized (C/FGI-MOD), and so marked on the first page. A DOE F 470.9, *C/FGI-MOD Cover Sheet*, must be used; this form is to be used only on C/FGI-MOD documents. The country of origin must be indicated at the bottom of the cover sheet. The marking on the first page of the document must be as follows:

This document contains *(insert name of country) (insert NSI classification level)* information to be treated as **CONFIDENTIAL – MODIFIED HANDLING AUTHORIZED**

Access to C/FGI-MOD does not require an access authorization, but does require need-to-know in performance of official duties.

C/FGI-MOD is national security information classified under Executive Order 13526. Uncleared individuals given access to C/FGI-MOD must be provided appropriate handling instructions, either via a briefing from the HSO or the manager responsible for the program involving the C/FGI-MOD, or via written instructions on an approved C/FGI-MOD coversheet, DOE F 471.2 (<http://energy.gov/sites/prod/files/DOE%20F%20471.2.pdf>).

Information systems that store and/or process C/FGI-MOD cannot be accessed or serviced by foreign nationals.

When not in use, C/FGI-MOD must be stored in a locked receptacle (e.g., file cabinet, desk, bookcase) that is accessible only to persons who need-to-know the information to perform their official duties. Such persons must prevent unauthorized disclosure or access by unauthorized persons.

C/FGI-MOD may be reproduced without permission of the originator to the minimum extent necessary to carry out official duties.

C/FGI-MOD must be transmitted in the same manner as classified matter unless this requirement is waived by the originating foreign government.

C/FGI-MOD information must be destroyed in the same manner as classified information (see Section 514).

Point of Contact

For information about the HQ CMPC Program, call (301) 903-9986 or (301) 903-1163.

Forms/Samples/Graphics

DOE Form 471.2, *C/FGI-MOD Cover Sheet* (for a copy of this form go to <http://energy.gov/sites/prod/files/DOE%20F%20471.2.pdf>)

Helpful Website

The HQ CMPC Program website is at: <http://www.hss.energy.gov/HQSecOp/cmpec.html>

This page intentionally left blank.

Section 505

Marking Classified Matter

This section describes DOE HQ procedures for marking classified matter. Regardless of date or agency of origin, classified matter must be marked to indicate at least the classification level and category (if RD, FRD, or TFNI). All classified documents dated **after** April 1, 1996, must be marked in accordance with directives in place at the time of origin.

HQ Implementation Procedures

General Procedures:

The markings that are common to all classified documents include:

- Classification level
- Classification category (if RD, FRD, or TFNI)
- Caveats (special markings)
- Authorized classifier information
- Originator identification
- Title/Subject marking
- Unique identification numbers (for accountable matter only)
- Portion marking (for documents containing NSI or TFNI).

Any deviation from these requirements will be specifically stated. Consult the *DOE CMPC Marking Resource* for details on how to properly mark classified matter in its various forms.

NOTE 1: DOE conforms to and does not exceed the requirements of the Federal government, implemented by the U.S. government Information Security Oversight Office (ISOO), for marking classified documents. If a classified document is originated by DOE, it must be correctly marked in all respects. If incompletely marked, the originating office should be consulted to resolve all discrepancies. Classified documents received by DOE from OGAs are often not marked in accordance with national standards. To ensure proper protection of such documents, these documents must be marked with the overall classification level and protected with the appropriate cover sheet for classified information. Resolution of OGA deficiencies and/or continuing patterns of deficiencies should be handled through the CMPC Program Manager, HS-92.

NOTE 2: All classified documents (other than Working Papers or draft documents – see below) must contain a classification authority block that identifies the DC who reviewed the document, the guide or source the decision was based upon, and the declassification date or event for NSI documents. This classifier's identification is recorded on the face of each classified document. A DC must make the classification determination for the

original copy of each document. Any change to any classified document requires a DC review. The placement of a DC's name on a classified document without the DC's direction or authorization is illegal and will result in an official inquiry and/or investigation. Consult DOE Order 475.2A for additional information on identifying classified information.

NOTE 3: All NSI documents and all page changes to NSI documents created after April 1, 1997, must be portion marked.

Classified Cover Sheets:

At a minimum, all classified documents must have an appropriate cover sheet (Top Secret, Secret, or Confidential) attached depicting the classification level of the protected classified matter. A cover sheet must be attached to the face of a document whenever that document is outside a GSA-approved security repository. Additionally, the back of all classified documents must also have an appropriate cover sheet attached or, if the back of the last page is blank, the overall highest classification level of the document may be marked at top and bottom of the page.

Marking Standard Form 700, Security Container Information:

Special considerations are in place for marking SF-700, *Security Container Information*, the three-part form used to record safe and door combinations. See Section 507, Storage of Classified Matter, for instructions on how to mark SF-700s.

Marking Electronic Files:

Individuals are responsible for ensuring that classified electronic files (e.g., e-mail, documents) that are transmitted or shared outside the individual's exclusive domain (i.e., the individual's computer) are reviewed and properly marked. More specifically, individuals are responsible for including all of the classified markings that are required to appear on paper copies of documents when classified documents (files) are in electronic form, including text within a database, data within a spreadsheet, and web-based documents (HTML, ASCII text file, etc.). Additional guidance is provided in 32 CFR 2001.23 (see Attachment 505-1).

The required markings include:

- Portion marking in the body of all NSI documents
- Classification level and category markings (if RD, FRD, or TFNI) at the top and bottom of each page, or at the beginning and end of the actual text if header and footer markings are impractical (e.g., e-mail) or not available with the software used
- Caveats, if any

- Title/Subject markings (regardless of category)
- Classification authority, with the name and title of the classifier, classification authority, and declassification instructions for NSI only.

NOTE: Portion marking is not required for documents/files containing RD or FRD.

Examples of electronic files that must be marked include, but are not limited to:

- Word processing, database, spreadsheet, and HTML documents
- E-mail and/or attachments to e-mail
- Files that are shared in a peer-to peer network (two or more personal computers directly connected to each other)
- Files that are posted to a classified network server for access by other than the originator
- Electronic files that are hand transmitted (physically handing media containing the file to another person).

Marking E-Mail Messages:

Consult 32 CFR Section 2001.23 (Attachment 505-1).

Classified Working Papers and Drafts:

Classified Working Papers and drafts are considered to be interim production stages toward the generation of a permanent document and are usually created during research or note taking at classified meetings, seminars, classes, symposiums, or conferences. Working papers must be:

- Marked with the date created
- Protected and marked in accordance with the highest potential classification level, category (if RD, FRD, or TFNI), and caveats if applicable
- Annotated with “Working Paper” or “Draft” on the first page of the text
- Protected by the approved classified cover sheet
- Destroyed when no longer needed
- Accounted for (if required) and controlled and marked in the manner prescribed for a finished document of the same classification when the working papers are:

- o Released by the originator outside the specific HQ element activity or office;
- o Retained for more than 180 days from the date of origin; or
- o Filed permanently.

Working Papers/drafts that are frequently updated as part of a project or study may be considered to be (re)originated upon each change. The date of each revision, addition, or change must be clearly indicated on the document. One suggestion is to line out (but not obliterate) the date of the last change and insert the new date of the current revision, addition, or change on the document itself. Another option is to attach a change sheet to the front of the document, listing the date of each change. Once re-dated, the 180-day limit for retention starts over again.

When the final classification of a draft or working paper must be sent outside the office of origin for a classification review and determination, it must be marked:

DRAFT - NOT REVIEWED FOR CLASSIFICATION

NOTE: This marking does not preclude the need to mark and protect the draft or working paper at the highest estimated classification level and category pending review.

If the classification determination cannot be made locally, a Document Undergoing Classification Review cover sheet (see Attachment 505-2) may be appropriately completed and attached to the draft document, with an appropriate classified cover sheet on top. This option should be used only when the DC within the organization cannot make the final classification determination for the document. This cover sheet does not preclude the need to mark the working paper/draft with the highest possible classification level and category.

Notes taken during a meeting, conference, etc., that involves classified information or a classified subject area are to be considered classified working papers and must be protected and marked with the highest potential classification level and category, and with appropriate caveats, as applicable. A review by a derivative classifier is required if the notes become a final document, are filed permanently, or are retained longer than 180 days. Transmission of notes of uncertain classification must be in accordance with Section 511, Receipt and Transmission of Classified Matter.

For detailed information on marking working papers and drafts, consult the *DOE CMPC Marking Resource*, accessible through the Helpful Websites subsection below.

Points of Contact

For questions about the HQ CMPC Program, call (301) 903-9986 or (301) 903-1163.

Forms/Samples/Graphics

32 CFR 2001.23 (Attachment 505-1)

Document Undergoing Classification Review Cover Sheet (Attachment 505-2) (a clean, .pdf version of this cover sheet may be requested by sending an e-mail to “HS-92 Operations”).

Helpful Websites

The HQ CMPC Program website is at: <http://www.hss.energy.gov/HQSecOp/cmpec.html>

To view the *DOE CMPC Marking Resource*, go to:

http://www.hss.energy.gov/SecPolicy/DOE_CMPC_Marking_Resource.pdf

ATTACHMENT 505-1

32 CFR 2001.23

Title 32: National Defense

PART 2001—CLASSIFIED NATIONAL SECURITY INFORMATION

Subpart C—Identification and Markings

§ 2001.23 Classification marking in the electronic environment.

(a) *General.* Classified national security information in the electronic environment shall be:

- (1) Subject to all requirements of the Order.
- (2) Marked with proper classification markings to the extent that such marking is practical, including portion marking, overall classification, “Classified By,” “Derived From,” “Reason” for classification (originally classified information only), and “Declassify On.”
- (3) Marked with proper classification markings when appearing in an electronic output (*e.g.*, database query) in which users of the information will need to be alerted to the classification status of the information.
- (4) Marked in accordance with derivative classification procedures, maintaining traceability of classification decisions to the original classification authority. In cases where classified information in an electronic environment cannot be marked in this manner, a warning shall be applied to alert users that the information may not be used as a source for derivative classification and providing a point of contact and instructions for users to receive further guidance on the use and classification of the information.
- (5) Prohibited from use as source of derivative classification if it is dynamic in nature (*e.g.*, wikis and blogs) and where information is not marked in accordance with the Order.

(b) *Markings on classified e-mail messages.*

- (1) E-mail transmitted on or prepared for transmission on classified systems or networks shall be configured to display the overall classification at the top and bottom of the body of each message. The overall classification marking string for the e-mail shall reflect the classification of the header and body of the message. This includes the subject line, the text of the e-mail, a classified signature block, attachments, included messages, and any other information conveyed in the body of the e-mail. A single linear text string showing the overall classification and markings shall be included in the first line of text and at the end of the body of the message after the signature block.
- (2) Classified e-mail shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion. A text portion containing a uniform

resource locator (URL) or reference (*i.e.*, link) to another document shall be portion marked based on the classification of the content of the URL or link text, even if the content to which it points reflects a higher classification marking.

(3) A classified signature block shall be portion marked to reflect the highest classification level markings of the information contained in the signature block itself.

(4) Subject lines shall be portion marked to reflect the sensitivity of the information in the subject line itself and shall not reflect any classification markings for the e-mail content or attachments. Subject lines and titles shall be portion marked before the subject or title.

(5) For a classified e-mail, the classification authority block shall be placed after the signature block, but before the overall classification marking string at the end of the e-mail. These blocks may appear as single linear text strings instead of the traditional appearance of three lines of text.

(6) When forwarding or replying to an e-mail, individuals shall ensure that, in addition to the markings required for the content of the reply or forward e-mail itself, the markings shall reflect the overall classification and declassification instructions for the entire string of e-mails and attachments. This will include any newly drafted material, material received from previous senders, and any attachments.

(c) Marking Web pages with classified content.

(1) Web pages shall be classified and marked on their own content regardless of the classification of the pages to which they link. Any presentation of information to which the web materials link shall also be marked based on its own content.

(2) The overall classification marking string for every web page shall reflect the overall classification markings (and any dissemination control or handling markings) for the information on that page. Linear text appearing on both the top and bottom of the page is acceptable.

(3) If any graphical representation is utilized, a text equivalent of the overall classification marking string shall be included in the hypertext statement and page metadata. This will enable users without graphic display to be aware of the classification level of the page and allows for the use of text translators.

(4) Classified Web pages shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion. A portion containing a URL or reference to another document shall be portion marked based on the classification of the content of the URL itself, even if the content to which it points reflects a higher classification marking.

(5) Classified Web pages shall include the classification authority block on either the top or bottom of the page. These blocks may appear as single linear text strings instead of the traditional appearance of three lines of text.

(6) Electronic media files such as video, audio, images, or slides shall carry the overall classification and classification authority block, unless the addition of such information would render them inoperable. In such cases, another procedure shall be used to ensure recipients are aware of the classification status of the information and the declassification instructions.

(d) *Marking classified URLs.* URLs provide unique addresses in the electronic environment for web content and shall be portion marked based on the classification of the content of the URL itself. The URL shall not be portion marked to reflect the classification of the content to which it points. URLs shall be developed at an unclassified level whenever possible. When a URL is classified, a classification portion mark shall be used in the text of the URL string in a way that does not make the URL inoperable to identify the URL as a classified portion in any textual references to that URL. An example may appear as:

http://www.center.xyz/SECRET/filename_(S).html

http://www.center.xyz/filename2_(TS).html

http://www.center.xyz/filename_(TS//NF).html

(e) *Marking classified dynamic documents and relational databases.*

(1) A dynamic page contains electronic information derived from a changeable source or ad hoc query, such as a relational database. The classification levels of information returned may vary depending upon the specific request.

(2) If there is a mechanism for determining the actual classification markings for dynamic documents, the appropriate classification markings shall be applied to and displayed on the document. If such a mechanism does not exist, the default should be the highest level of information in the database and a warning shall be applied at the top of each page of the document. Such content shall not be used as a basis for derivative classification. An example of such an applied warning may appear as:

This content is classified at the [insert system-high classification level] level and may contain elements of information that are unclassified or classified at a lower level than the overall classification displayed. This content may not be used as a source of derivative classification; refer instead to the pertinent classification guide(s).

This content is classified at the [insert system-high classification level] level and may contain elements of information that are unclassified or classified at a lower level than the overall classification displayed. This content may not be used as a source of derivative classification; refer instead to the pertinent classification guide(s).

(3) This will alert the users of the information that there may be elements of information that may be either unclassified or classified at a lower level than the highest possible classification of the information returned. Users shall be encouraged to make further inquiries concerning the status of individual elements in order to avoid unnecessary classification and/or impediments to information sharing. Resources such as classification guides and points of contact shall be established to assist with these inquiries.

(4) Users developing a document based on query results from a database must properly mark the document in accordance with §2001.22. If there is doubt about the correct markings, users should contact the database originating agency for guidance.

(f) Marking classified bulletin board postings and blogs.

(1) A blog, an abbreviation of the term “web log,” is a Web site consisting of a series of entries, often commentary, description of events, or other material such as graphics or video, created by the same individual as in a journal or by many individuals. While the content of the overall blog is dynamic, entries are generally static in nature.

(2) The overall classification marking string for every bulletin board or blog shall reflect the overall classification markings for the highest level of information allowed in that space. Linear text appearing on both the top and bottom of the page is acceptable.

(3) Subject lines of bulletin board postings, blog entries, or comments shall be portion marked to reflect the sensitivity of the information in the subject line itself, not the content of the post.

(4) The overall classification marking string for the bulletin board posting, blog entry, or comment shall reflect the classification markings for the subject line, the text of the posting, and any other information in the posting. These strings shall be entered manually or utilizing an electronic classification tool in the first line of text and at the end of the body of the posting. These strings may appear as single linear text.

(5) Bulletin board postings, blog entries, or comments shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion.

(g) Marking classified wikis.

(1) Initial wiki submissions shall include the overall classification marking string, portion marking, and the classification authority block string in the same manner as mentioned above for bulletin boards and blogs. All of these strings may appear as single line text.

(2) When users modify existing entries which alter the classification level of the content or add new content, they shall change the required markings to reflect the classification markings for the resulting information. Systems shall provide a means to log the identity of each user, the changes made, and the time and date of each change.

(3) Wiki articles and entries shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion.

(h) *Instant messaging, chat, and chat rooms.*

(1) Instant messages and chat conversations generally consist of brief textual messages but may also include URLs, images, or graphics. Chat discussions captured for retention or printing shall be marked at the top and bottom of each page with the overall classification reflecting all of the information within the discussion and, for classified discussions, portion markings and the classification authority block string shall also appear.

(2) Chat rooms shall display system-high overall classification markings and shall contain instructions informing users that the information may not be used as a source for derivative classification unless it is portion marked, contains an overall classification marking, and a classification authority block.

(i) *Attached files.* When files are attached to another electronic message or document, the overall classification of the message or document shall account for the classification level of the attachment and the message or document shall be marked in accordance with §2001.24(b).

(ii) *Reserved.*

ATTACHMENT 505-2

Document Undergoing Classification Review Cover Sheet

TOP SECRET / SECRET/ CONFIDENTIAL

(Only When This Page is Filled-in and Appropriate Classification Indicated - - Circle One)

Document Undergoing Classification Review

**Protect This Document At the Classification
Level and Category Marked on This Page**

TO: _____

FROM: _____

DATE: _____

RESTRICTED DATA

This Document Contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized Disclosure Subject to Administrative and Criminal Sanctions.

▲ Circle One (If Applicable) ▼

FORMERLY RESTRICTED DATA

Unauthorized disclosure subject to Administrative and Criminal Sanctions. Handle as Restricted Data in Foreign Dissemination Section 144.b., Atomic Energy Act 1954.

Instructions for Use of this Form

(You do not need to be an Authorized Classifier to use this Form)

1. Circle the highest estimated classification level at the top and bottom of this page (circle only one level).
2. Circle the *Restricted Data* or *Formerly Restricted Data* Warning Notice (only if applicable).
3. Fill in "To," "From," and "Date" lines.
4. Place this Form on top of the document pending classification review, and place an appropriate coversheet (SF-703 for Top Secret, SF-704 for Secret, or SF-705 for Confidential) on top of this page.

Note 1: Document attached hereto may contain classified information and may or may not contain any classification markings. It must be protected as marked on this page. This cover page must remain with this document until a final classification determination has been made and the document has been appropriately marked by an Authorized Classifier.

Note 2: Top Secret Documents must be hand carried or routed through an authorized courier. Use of any type mail or express mail service for Top Secret matter is prohibited. Transmittal of classified matter must be in accordance with DOE Orders.

TOP SECRET / SECRET/ CONFIDENTIAL

(Only When This Page is Filled-in and Appropriate Classification Indicated - - Circle One)

U.S. Department of Energy, Washington, DC
REF #: HS-1.312-2009-12

This page intentionally left blank.

Section 506

Protection of Classified Matter in Use

This section describes DOE HQ policies and procedures pertaining to the protection of classified matter while it is in use. When it is not actually being used, it must be stored within a security container or a VTR that is approved for open storage of classified matter. (See Section 507, Storage of Classified Matter).

HQ Implementation Procedures

All persons who access classified matter must possess a security clearance commensurate with the classification level and category of information being accessed and need-to-know for that information in the performance of their official duties. Classified matter will be protected at all times and, as a general rule, will be accessed for use only in approved LAs or VTRs. However, there are exceptions to the rule. See Section 201, Establishing, Maintaining, and Deactivating LAs, VTRs, and TLAs, for information on establishing a Temporary Limited Area for the review of classified information.

NOTE: Refer to Section 204, Classified Meetings Outside of LAs and VTRs Approved for Classified Discussions, if classified discussions are anticipated outside a LA or VTR.

Emergency Situations:

If the emergency is life threatening (e.g., explosion, fire), the health and safety of the individual takes precedence over the need to secure classified matter in accordance with normal storage requirements.

Depending on the intensity and urgency of the emergency situation, classified matter should be secured in the most expeditious way possible: in an accessible security container (preferred method), file cabinet, desk, alternate areas within the facility, etc.

No policy can specify employee actions for every conceivable scenario. **Use your best judgment while protecting both your health and safety and the classified matter.**

These actions must be taken after the emergency:

- All unsecured classified matter must be located, accounted for, and returned to proper storage.
- Security containers and VTRs must be inspected to ensure that they have not been compromised.

Fire and Evacuation Drills:

Fire and evacuation drills must be carried out as realistically as possible so that individuals know how to respond during a real emergency. Therefore, individuals should handle all classified information as described above, regardless of whether the emergency is real or a practice drill.

Emergency Response Personnel:

In an emergency involving an imminent threat to life or national defense, emergency personnel who are not otherwise routinely eligible for access to classified information may be granted emergency access to security areas and/or classified information. Examples include providing law enforcement personnel classified information about an improvised nuclear device found in a public place, sharing a classified DOE evaluation of the viability of a nuclear threat message with local emergency response personnel, or providing an attending physician with classified details about nuclear materials at a site to assist in the emergency treatment of a patient. The following actions must be taken if such an intentional release of classified information is required:

- The amount of classified information disclosed and the number of individuals to whom such information is disclosed must be limited to the absolute minimum required to achieve the intended purpose.
- The information must be transmitted over approved channels using the most secure and expeditious method.
- The recipient must be informed of what specific information is classified and the protection requirements for the information.
- The recipient must be briefed on his/her responsibilities for not disclosing the information and must sign a nondisclosure agreement.
- The information must remain in the physical custody of an authorized Federal government entity in all but the most extraordinary circumstances.

Within 72 hours of the disclosure of classified information or at the earliest opportunity that the emergency permits, but no later than 30 days after the release of classified information to an emergency responder, the official making the disclosure decision must report the disclosure. The report must include:

- A description of the disclosed information
- A list of individuals to whom the information was disclosed
- A description of how the information was disclosed and transmitted
- The reason for the emergency release
- How the information is being protected.

The disclosure must be made to:

- The Director, HS-90 and the NNSA Associate Administrator for Defense Nuclear Security (NA-72) when RD or FRD has been released
- The Director, HS-90, when NSI or TFNI has been released.

Points of Contact

For the names and contact information for those who occupy the positions identified in this section, call (301) 903-9986, (301) 903-9990, or (301) 903-1163.

Helpful Website

The HQ CMPC Program website is at: <http://www.hss.energy.gov/HQSecOp/cmpec.html>.

This page intentionally left blank.

Section 507

Storage of Classified Matter

This section describes DOE HQ policies and procedures pertaining to the storage of classified matter. In summary, all classified matter must be stored within a security container in an LA or VTR, or in a VTR approved for open storage of classified matter.

HQ Implementation Procedures

Classified matter must be stored at all times in a designated LA or VTR that has been approved and certified by HS-90 (see Section 201, Establishing, Maintaining, and Deactivating LAs, VTRs, and TLAs). Unless HS-90 has certified a VTR for the open storage of classified matter, all classified matter must be stored in GSA-approved containers located within approved and certified LAs or VTRs. GSA containers and VTRs in use for the storage of classified matter must be equipped with an X-07, X-08, or X-09 series electromechanical combination lock.

NOTE: Money, firearms, medicines, controlled substances, and other items of monetary value susceptible to theft shall not be stored in the same security containers used to store classified matter.

In general, TS matter shall be stored in a locked GSA-approved security container (i.e., closed storage) within a designated LA or VTR. The following types of classified storage facilities must additionally be protected by an intrusion detection system certified by HS-90:

- A VTR approved and certified for the open storage of classified matter
- An approved and certified VTR that opens into a Property Protection Area
- An LA or VTR with closed storage of TS matter.

Open storage of TS matter within rooms that meet VTR requirements **may be authorized** (see Section 201, Establishing, Maintaining, and Deactivating LAs, VTRs, and TLAs) **on a case-by-case basis** based on storage requirements that cannot be reasonably met by an alternative approved method (e.g., GSA-approved storage container). Requests for approval of open storage of TS matter must be predicated on a programmatic requirement for open storage, not as “a matter of convenience.”

NOTE: At HQ, TS matter can be stored only in the Forrestal and Germantown buildings.

Responsibilities for Security Containers and Vault-Type Rooms:

Personnel who access security containers and VTRs are responsible for protecting classified matter at all times and for locking classified matter in appropriate security containers whenever it is not in use or under the direct supervision of authorized persons. These

individuals must ensure that unauthorized persons do not gain access to classified matter. In areas approved for open storage, classified matter need not be stored in a security container (the open storage level/category authorized is indicated in the specific room or facility certification).

Repository Opening Procedures:

To open the door to a VTR:

- Deactivate the premise alarm system (if applicable).
- Dial the combination and open the lock.
- Record the opening on the SF-702, *Security Container Check Sheet*.
- After opening a VTR equipped with an XO series combination door lock, check the life-safety switch (see diagram below); it should be pushed **in** to prevent accidental locking.

CD-X-07 Door Lock Operation



To open a security container (safe):

- Dial the combination and open the lock.
- Record the opening on the SF-702.

NOTE: The sole custodian of a security container is not required to record each opening and closing of the container throughout the day. In such cases, the appropriate information should be recorded on the SF-702 the first time the container is opened that day. The container may be opened and closed as necessary without further record keeping. At the end of the day, information

should be recorded indicating the final closing of the container for that day. If two or more persons have authorized access to the container, each opening and closing must be duly recorded.

Repository Closing Procedures:

To close and secure a security container (safe):

- Visually check the immediate area and top of the container for any classified matter that may have been left unattended, and put it in the appropriate storage location.
- Close all safe drawers and lock the XO series combination lock by turning the dial at least three full rotations in the counterclockwise direction and then turning the dial at least one full rotation in the opposite, clockwise direction.
- Verify that all the container drawers are locked by attempting to turn the handle and simultaneously attempting to pull the drawer open. Then check each auxiliary drawer by activating its thumb release and attempting to pull the drawer open.
- Record the closing/checking action on the SF-702.
- At the end of the work day, complete the SF-701, *Activity Security Checklist*, that is explicitly tailored to the specific room, area, or activity. The SF-701 is to be posted inside the area being protected.

NOTE 1: If the dial cannot be turned in either direction, the container bolt locking mechanism has not engaged into the locking mode (e.g., a drawer may not be fully closed, or matter may be jammed in the drawer path).

NOTE 2: If the dial stops turning when turned in the clockwise direction, the container and/or lock is not locked.

NOTE 3: HQ facilities are required to utilize the XO series combination locks on security containers.

To close and secure the door to a VTR:

- Ensure that the life safety switch is pulled **out** (the off position) to permit activation of the door lock.
- With the door open, rotate the combination lock dial at least one turn to the left (counterclockwise); there will be a slight resistance to turning until the locking mechanism has engaged. *NOTE: If the dial will not turn counterclockwise, the life safety switch is engaged (on).*

- Exit the room and close the door securely; the locking mechanism will snap into and engage the strike on the door jamb.
- Rotate the combination lock dial one full turn to the right (clockwise). If the dial stops turning when turned in the clockwise direction, the XO series lock is not locked.
- Check that the door is fully secured:
 - If the VTR door **is not** equipped with an access control mechanism (cipher lock, card reader, etc.), attempt to open the door without activating the XO series combination lock. If the door **is** equipped with an access control mechanism (cipher lock, card reader, TESA® lock, keyed door knob, etc.), the access control must be activated with an attempt to enter the VTR without activating the XO series combination lock.
 - On a GSA-approved vault door, attempt to turn the handle release mechanism and open the vault door.
 - On a VTR door containing a mechanical or electromechanical cipher lock in addition to the XO series lock, activate the cipher code and/or card or key and attempt to open the door after securing the XO series door lock.
- Activate the premise alarm. *NOTE: Within HQ facilities, premise alarms for VTRs, when so equipped, must be activated whenever the facility is unoccupied.*
- Record each closing/checking action on the SF-702, which must be posted on the outside of the door to the VTR.

In case of a security system malfunction (e.g., door will not close or lock, or alarm system, if applicable, will not set up), do not leave classified matter unattended. Contact the element HSO, protective force personnel, or appropriate management official to determine a course of action, including an alternative way to secure the classified matter.

Possible Forced Entry into Security Containers and Vault-Type Rooms:

If there is any indication of forced entry into a security container or VTR, the individual making the discovery must notify the HQ protective force who must, in turn, follow the plan of action detailed in HQ protective force post orders. The discovery must also be reported to the HSO responsible for the LA or VTR so the HSO can report the discovery as a security incident (see Chapter 11, Incidents of Security Concern). The area must remain protected, and every effort must be made to leave the area untouched or undisturbed until a decision to proceed has been granted by HS-90. Appropriately cleared management or HSO personnel must stand by the area until the potentially compromised classified matter is secured and/or until released by HS-90. The individual discovering

the forced entry must stand by until he/she has given a statement to the DOE HQ protective force. A complete inventory of the contents of the protected matter must be made as soon as the scene has been released by HS-90.

Open and Unattended Security Containers and Vault-Type Rooms:

If a security container or VTR is found open and unattended at any time, the individual making the discovery must notify the DOE HQ protective force, who must, in turn, follow the plan of action detailed in HQ protective force post orders. The protective force contacts an individual authorized access to the security container (i.e., an individual listed on the SF-700), and that individual is then responsible for notifying the cognizant HSO.

The person notified of the discovery can either:

- Respond to the scene to inventory the contents of the container and personally relock the container, or
- Authorize the protective force to relock the container. The person notified or some other individual responsible for the container must inventory the contents of the container no later than the next working day.

The HSO will initiate action to change the combination, which must be considered potentially compromised, as soon as possible during duty hours or after the start of the next work day, as applicable. However, for an XO-series combination lock, the combination need not be changed if all of the following criteria are met:

- There is no reasonable or probable suspicion that the contents of the container have been disturbed.
- The numbers in the combination have not otherwise been compromised or subjected to compromise via a written or verbal record or communication.
- The existing combination has been tested to ensure its operability. If the existing combination to an XO-series lock fails to open the lock, a compromise must be assumed and HS-90 must be immediately informed via secure communication.

NOTE: The combination to other than an XO-series combination lock must be considered compromised and therefore must be changed.

Security container combinations (SF-700s) stored within a container that has been found open and unattended may have to be changed. All stored SF-700 combination envelopes must be examined for tampering. An expanded inquiry must be conducted for any SF-700 envelope that is open or shows signs of tampering, or for any security container

combination that is exposed by any means. The inquiry process must assume that any security container whose combination has been exposed is compromised.

During the security inquiry, if there is reasonable suspicion that the contents of the container have been disturbed (e.g., missing documents, rearranged material, combination was changed, an XO series combination lock no longer opens on the assigned combination, missing SF-700s, or other suspicious indicators), the Inquiry Officer must notify HS-90 before taking any further action.

Originals of the security documents associated with the container that was found open and unattended become supporting documentation for the inquiry; therefore, replacement documentation must be generated and the combination may need to be changed, as described above.

Controlling Access to Security Repositories:

Individuals requiring access to a security container or VTR must have a security clearance and special accesses for the highest classification level and most restrictive category, as well as caveat requirements, of the information stored in that repository. For example, only individuals with a Q security clearance may have the combination for a container holding S/RD. Also, the container in this example would have to be secured if an individual with an L security clearance were to work in the same room with the container. Access to the combinations of security containers should be limited to a minimal number of cleared individuals.

Containers containing classified matter must be secured when an individual with the appropriate security clearance does not have visual line-of-sight to the front of the container.

Containers may not be left open and unattended when inside a locked room unless the room is authorized for open storage of the highest level and category stored in the open container.

A security container with a combination lock on each drawer (multilock security container) must have a separate classified combination for each drawer, each one with a separate SF-700. A multilock cabinet is not considered secured unless all locks are locked with a classified combination (the 50-25-50 standard combination may not be used on unused drawers). Multi-lock containers are generally used for compartmentation purposes. If an SF-702 is used for each drawer, the combination lock on each drawer must be checked at the close of each business day.

A security container containing dual locks (two locks on each drawer), or an XO series lock used in the dual or supervisory combination mode (XO-series combination selection modes #2 and #3), normally referred to as “two-man control,” must use an SF-700 for each combination lock, or single XO series lock with dual combination control

enabled. The SF-700s for all such combinations must be stored in separate containers unless programmatic requirements dictate otherwise.

NATO documents must be segregated from other documents when stored in security containers. At a minimum, NATO documents may be segregated by being placed in separate files. Access to NATO documents requires an access briefing administered by the NNSA Security Operations Division (NA-71), which performs NATO Subregistry functions for HQ. If NATO documents are stored in a container with other classified documents, access to the container itself must be limited only to those individuals who have been granted access to NATO information. The record copy of the combination to a security container storing NATO information must be appropriately stored in another container authorized for the storage of NATO information.

U.S. State Department documents with the protective marking NODIS (No Distribution) are controlled by the Office of the Executive Secretariat, which also controls access to these documents. Document storage is limited to Office of the Executive Secretariat's LAs or VTRs and other organizations so designated by the Office of the Executive Secretariat.

Classified documents may be commingled within the same file folder; however, security clearance and need-to-know must be taken into consideration when filing classified documents. Classified documents removed from security containers must have the appropriate cover sheet attached. File folders containing classified matter, when removed from security containers, must be marked top and bottom, front and back, with the highest classification level of the contents or, alternatively, must have an appropriate cover sheet(s) attached.

End-Of-Day Security Check:

An SF-701, *Activity Security Checklist* (or equivalent form) must be used for end-of-day security checks of LAs and VTRs that contain security interests (e.g., security repository, classified computer, classified shredder). These forms should be maintained **inside** each LA or VTR. The form must be retained for 90 days following the date of the last entry unless involved in a security incident, in which case the form relevant to the inquiry is retained as an attachment to the Security Incident Report.

Open Storage Requirements:

Open storage of classified matter up to and including TS/RD may be authorized within rooms that meet VTR requirements, including alarm protection and XO-series combination locks on the door. Open storage approvals and certificates must be granted by HS-90 before open storage is implemented (see Section 201, Establishing, Maintaining, and Deactivating LAs, VTRs, and TLAs).

Individuals who access these areas must possess a security clearance for the highest classification level and most restrictive category of information that is in open storage.

Individuals without the appropriate security clearance or need-to-know must be escorted by a person with the appropriate security clearance and need-to-know while they are in the area. The escort must ensure that the escorted individual is not given access to information that the individual is not authorized to access.

All classified matter exceeding the clearance level of the person to be escorted, including such items as classified equipment and/or classified maps, photographs, and charts on walls, must be covered or removed from the view of any individual requiring escort before that person (with escort) enters.

All individuals who are not assigned to, who do not work in, or who are not listed on the area access list posted within the open storage VTR must sign in on a visitor log, which contains a printed name, signature, date, time in, time out, and name of escort. Visitor logs for these approved areas must be retained for 5 years. Visitor logs may be locally produced.

Access control, whether by mechanical means, electromechanical means, or personnel, must be strictly maintained. An open storage LA or VTR may never be left unoccupied unless fully locked with the XO-series combination lock and alarmed.

Security Container Information:

An SF-702 must be placed on each security container; on each combination-locked access door to a security area authorized for open storage of classified matter; and on each VTR entrance on the outside of the locking door so as to ensure high visibility upon inspection.

The SF-702 must be completed by the individual who opens, closes, or checks the security container, combination-locked security area access door, or VTR. In all cases, the individual who opens a security container is responsible for closing the container or transferring the responsibility for the security of that container to another authorized individual.

An SF-702 must contain at least one daily duty-day entry that the container was “checked by” with time and initials, regardless of whether the container was opened that day. Protective force checks, when required, are in addition to this check. Each container opening and closing must be recorded throughout the day except when the container is used by a sole custodian, in which case only one opening and closing entry is required. Another individual should annotate the “checked by” box, but if no one else is available, the person closing the container may fill in the “checked by.” HSOs should develop local procedures to ensure that all classified matter is properly stored and that security containers are checked at the end of each work day.

SF-702s must be retained for 90 days after the last date of entry on the form.

NOTE: Security containers located within approved open storage areas may or may not require the use of a separate SF-702, depending on the nature of the classified matter stored therein. Contact the CMPC Program Manager, HS-92, for guidance.

The diagram shows two identical 'SECURITY CONTAINER CHECK SHEET' forms side-by-side. The form on the right is labeled 'SF-702' with an arrow pointing to it. The forms contain various fields for recording container status, including 'TO #', 'FROM #', 'DATE', 'TIME', 'LOCATION', 'STATUS', 'REMARKS', and 'CHECKED BY'. Arrows indicate the flow of the document: a blue arrow points from the 'CHECKED BY' field of the left form to the 'CHECKED BY' field of the right form, and a red arrow points from the 'CHECKED BY' field of the right form to the 'CHECKED BY' field of the left form. To the right of the forms, there are instructions: 'Opened by', 'Closed by', 'Checked by', 'Record each opening and closing', 'Check daily even if not opened', and '90-day Retention'.

Security Repository (Safes and Doors) Combination Information:

Combinations to security containers, authorized open storage area combination-locked security access doors, and VTRs must be changed by an appropriately cleared individual who has authorized access to the combination. A change of combination and creation of a new SF-700, *Security Container Information*, is required when:

- An employee with access to the repository leaves, no longer requires access, or is no longer permitted access (includes administrative termination, suspension, or downgrading of security clearance lower than the level of classified matter being stored).
- There has been a known compromise, possible compromise, or discovery of a security repository that was left unlocked/open and unattended.
- The repository is put into service.
- The repository is taken out of service or prepared for turn-in; see Moving Security Containers (Safes), below.
- Maintenance has been performed on the repository by anyone other than individuals with required access, regardless of whether or not the lock was accessed or serviced.

XO-series locks, combinations for which were NOT provided to a maintenance technician, are exempt from combination changing IF the locking device portion of the container was not removed from the LA or VTR for servicing, AND the XO combination was tested to ensure the validity of the combination in place prior to servicing. If the known or existing combination does not function, this finding must be handled as a security incident and reported via secure channels.

NOTE 1: Combinations to containers storing NATO classified information must be changed at least annually. Combinations to containers storing communications security material must be changed every 2 years.

NOTE 2: The name and signature of the cleared individual changing a combination must be indicated in the "changed by" signature block of the SF-700.

*NOTE 3: The requested XO-series lock serial number information in block 8 of the April 2001 version of the SF-700 is **NOT** required at HQ. The risk of lockout and damage to the XO-series lock outweighs any gained advantage of extracting the serial number.*

NOTE 4: Top Secret combinations must be brought into accountability.

NOTE 5: Combinations to containers storing accountable NATO classified information must be brought into accountability by the appointed document control officer of the approved NATO registry element.

The SF-700 is used to record the following important information about each security container:

- The location of the container
- The date and other pertinent information concerning the last combination change
- The names of the individuals who know the combination to the container
- The name, address, and phone number of custodians who can respond should the container be found open and unattended
- The combination to the container.

The image shows the cover sheet of the SF-700 form. It is a complex document with multiple sections. At the top, it is marked 'SECRET/RO'. The main body contains several tables and text areas. A large red arrow points to a section labeled 'Names of persons with the combination here (excluding custodians on reverse side)'. To the right, there is a large 'SF 700' logo and a box labeled 'Classification for Training Purposes Only'. The bottom of the form contains a 'Privacy Act Statement' and a section for 'Part 1 - No Classification Required' and 'Part 2 and 2a - Classification on Top, Bottom, Front & Back'. The form is also marked with 'SECRET/RO' at the bottom.

The cover sheet (Part 1) of the SF-700 is to be completed, detached from the envelope portion of the form (Parts 2 and 2A), and affixed inside each lockable drawer of a security container or on the inside of the door to a VTR. The cover sheet (Part 1) is not to be affixed to the outside/exposed portion of a container or door and should not have any classification markings on it. The cover sheet should include:

- The room number and building where the container is located
- The date of the last combination change and the name and office symbol of the person who changed the combination
- The name, home address, and phone number of custodians who can respond if the container is found open and unattended
- Other repository custodians, without emergency responsibilities, must also be listed, but addresses and phone numbers are not required. Additional cleared personnel are added to this record when they receive the combination.

NOTE: There must be no external indication on any container or door as to the level of classified matter contained therein.

SUGGESTION: The record of non-emergency custodians may be maintained on the back side of the SF-700 envelope, or on a separate paper or card attached to the SF-700. Any other readily recallable record is also acceptable.

Part 2A of the SF-700 should be detached from the envelope portion of the form (Part 2) and the combination to the container entered onto it. Part 2A must then be marked on both the top and bottom of the front and back with the highest classification level and category of information stored in the container and sealed inside the envelope (Part 2). The envelope must be marked top and bottom, front and back, with the highest classification **level and category** of the information authorized to be stored in the security container. Classification authority or declassification instructions are not required on any portion of the SF-700.

*NOTE 1: Combinations are classified and should be committed to memory. Due to the vulnerability of the sealed flap on Part 2 of SF-700, it is suggested that brown paper sealing tape be placed over the flap and that a signature be affixed to the tape intersection with the envelope. Container combinations recorded on Part 2A, enclosed in Part 2 of SF-700, are to be stored in a centralized repository authorized for an equal or higher classification level and category. HSOs should determine the storage locations for such SF-700s by element or sub-element. Combinations protecting SCI must be stored within a SCIF. An SF-700 containing a TS combination must be appropriately stored and brought into accountability. The creation of a “master combination list” of multiple combinations for any program, office, or element is **prohibited**.*

NOTE 2: A record copy of combinations to VTRs and LAs, contained in properly marked, individually sealed envelopes, should be provided to the local CAS for storage. For purposes of life safety and emergency response, the CAS ensures that the HQ protective force has access to those combinations and/or keys to locking devices that deny ready access to occupied areas.

Superseded SF-700s should be destroyed as classified matter as soon as they are replaced.

Badge Office personnel are available to help make combination changes, but they are only authorized to prepare the lock for entry of the new combination; badge office personnel are not permitted to select or enter the numbers for the combination. To request assistance for a combination change at Forrestal, call 202-586-5764; or at Germantown, call 301-903-3330. E-mail requests to the badge offices are also permitted.

Moving Security Containers (Safes):

HSOs must become involved in the relocation or turn-in of a security container so they can ensure that appropriate security precautions are taken and can then properly annotate their security container records. There are three possible reasons for moving a safe:

1. The safe is no longer needed and will be turned in as excess – In this case, the HSO coordinates with the element’s Accountable Property Representative (APR), the Forrestal or Germantown badge offices, and the Office of Management (MA) to ensure that the safe is empty, the combination is reset, and the movement is completed. The HSO is responsible for removing the safe from his/her Appendix to the HQFMSP. Detailed instructions for HSOs in turning in a safe are included in Attachment 507-1.
2. The safe is being relocated to another room with no change in custodians – In this case, the HSO coordinates with the element’s APR and MA to ensure that the safe is configured for movement and that the movement is completed. The HSO is responsible for updating his/her Appendix to the HQFMSP to show the new location of the safe. Detailed instructions for HSOs in relocating a safe with no change in custodians are included in Attachment 507-2.

3. The safe is being transferred to another custodian – In this case, the HSO coordinates with the element's APR and MA to ensure that the safe is configured for movement and that the movement is completed. The HSO is responsible for updating his/her Appendix to the HQFMSP to show the new location and/or custodian of the safe. Detailed instructions for HSOs in relocating a safe with a change in custodians are included in Attachment 507-3.

NOTE: Relocating a security container and/or rearranging furniture within an alarmed room may interfere with the electronic protective system. Therefore, physical security personnel from HS-91 must conduct a security system performance test immediately after the move.

Use of Optional Form 89, Maintenance Record for Security Containers/Vault Doors:

An Optional Form (OF) 89 must be placed inside the control drawer of each security container and posted on the back of a door with a combination lock installed on it. The servicing lock or container technician uses the OF 89 whenever the security container is serviced or repaired. This form must remain inside the drawer or on the back of the door for the life of the container. **Do not remove the form when accessing the container.**

If a container has been drilled or otherwise modified to gain entry, a statement of repair must be entered and signed on the OF 89 by the technician and/or inspector, stating that the repair was in accordance with GSA standards (Federal Standard 809A), before the container can return to use for storage of classified matter. Alternatively, the certification statement may be attached to OF 89. If a security container has not been restored to GSA standards, the GSA certification label on the front of the container must be removed and a permanent sign affixed to the front stating "Not Authorized for Classified Storage."

Optional Form (OF) 89						
MAINTENANCE RECORD FOR SECURITY CONTAINERS/VAULT DOORS						
NOTE: Store this form in the security container or on the vault door.						
FORM		SERIAL NUMBER (Containers: Located on the side of the control drawer. Vault Doors and Mail and Parcel Containers: Located on the back of the door.)				
☐ SECURITY CONTAINER	☐ VAULT DOOR					
MANUFACTURER		GSA CLASS				
		☐ ONE ☐ TWO ☐ THREE ☐ FOUR ☐ FIVE ☐ SIX ☐ SEVEN				
OPERATING PROBLEM	TYPE OF MAINTENANCE	DATE REPAIRED/INSPECTED	TECHNICIAN		ORGANIZATION NAME	
			NAME	ACTIVITY		
SIGNATURE OF RESPONSIBLE OFFICIAL			NAME OF RESPONSIBLE OFFICIAL		DATE SIGNED	
AUTHORIZED FOR LOCAL REPRODUCTION			OPTIONAL FORM 89 (9-98)			
http://contacts.gsa.gov/webforms.nsf/0/8DC498D630558385258A720062D0C1/\$file/of89.pdf						

24-Hour Classified Receipt and Storage:

Any person who has possession of classified matter up to TS/RD (not including SCI and SAP matter) and cannot store it in a classified repository (e.g., lock failure, don't have the combination to the safe, after-hours courier, etc.) can deliver the matter to the Forrestal or Germantown CAS for storage. The CASs are available 24 hours a day, every day, for classified receipt and storage:

- The Forrestal CAS is located in Room 1G-022.
- The Germantown CAS is located in Room A-060.

The person in possession of the classified matter must leave it in its classified wrapper and deliver it to the CAS. CAS operators will provide a receipt for the classified package(s) and provide temporary storage until the next normal business day. The person who retrieves the stored classified matter from the CAS must present the signed receipt and appropriate DOE identification.

NOTE 1: Temporary storage of SCI or SAP material should be arranged separately, in advance if possible, with the program office concerned.

*NOTE 2: **Temporary After-Hours SCI Storage (Forrestal Only)** – On normal business days from 7 a.m. until 8 p.m., SCI material may be taken to and stored in the Forrestal DOE/IN Communications Center (GA-293). The phone number is 202-586-8686. This phone number is also monitored by the IN Communications Center duty officer when the Communications Center is closed. When notified by telephone that a request has been made for SCI material to be stored after normal business hours, the duty officer arranges for appropriately cleared IN personnel to meet with the requester in the Forrestal building to accept the SCI material and store it in accordance with programmatic requirements.*

*NOTE 3: **Temporary After-Hours SAP Storage** – After-hours storage of SAP material must be initiated by the requester at the **Forrestal CAS** located in room 1G-022. Upon notification by the requester, the CAS Operator will notify designated SAP personnel. In response to the notification, SAP personnel will respond to the Forrestal CAS to take possession of the material and store it in accordance with programmatic requirements.*

Points of Contact

For the names and contact information for those who occupy the positions identified in this section, call (301) 903-9986, (301) 903-9990, or (301) 903-1163.

For safe and door combination changes at Forrestal, call 202-586-5764; or at Germantown, call 301-903-3330.

Forms/Samples/Graphics

How to Excess a Safe (see Attachment 507-1)

Moving a Safe with No Change in Custodians (see Attachment 507-2)

Moving a Safe with a Change in Custodians (see Attachment 507-3)

OF 89, *Maintenance Record for Security Containers/Vault Doors Federal Standard* (for a copy of this form go to <http://www.gsa.gov/portal/forms/download/115434>)

SF-700, *Security Container Information* (for a copy of this form go to <http://www.gsa.gov/portal/forms/download/115574>). Originals of this form can be obtained from the Forrestal and Germantown Supply Centers.

SF-701, *Activity Security Checklist* (for a copy of this form go to <http://www.gsa.gov/portal/forms/download/115578>)

SF-702, *Security Container Checksheet*, (for a copy of this form go to <http://www.gsa.gov/portal/forms/download/115582>)

HQ F 5632.12, *Container Equipment Inspection Certificate* (this form is available from the Forrestal and Germantown Copy Centers)

Helpful Websites

The HQ CMPC Program website is at: <http://www.hss.energy.gov/HQSecOp/cmhc.html>.

To view the *DOE CMPC Marking Resource*, go to:
http://www.hss.energy.gov/SecPolicy/DOE_CMPC_Marking_Resource.pdf

ATTACHMENT 507-1

How to Excess a Safe

- Before excessing a safe, contact your element HSO so that he/she can guide you through the steps of preparation. For instance, if your safe is broken (it will not unlock, the handle will not turn, or a drawer is stuck), your HSO may have to have it drilled before you can access it to check for classified material.
- The HSO should then contact the APR within his/her element and request that the safe be turned in as excess. The APR, in turn, contacts MA to arrange a date and time to move the safe. The HSO should then inform you of that date/time.
- The HSO should also contact either the Forrestal or Germantown Badge Office to make an appointment to have the combination on the safe reset to its factory setting (50-25-50).
- **BEFORE** the move date of your safe, you and your HSO should:
 1. Examine the security container, remove all contents, and either destroy the classified contents or store them in another security container (instructions on this process are listed below under “Forms to be Used”).
 2. Destroy both the current SF-700, *Security Container Information*, that is inside the safe and the extra copy that should be stored elsewhere (it contains the actual combination to your safe). The SF-700 should be destroyed as appropriate for its classification level.
 3. Attach a handwritten sign on the front of the safe stating “EMPTY.” This is optional, but it is recommended because it clearly indicates that the safe has been cleared out.
 4. You and your HSO should be present when the badge office completes the task of resetting the combination (i.e., ensuring that it has been set back to the factory setting).
 5. Finally, complete and affix HQ F 5632.12, *Container/Equipment Inspection Certificate* (see form listed below), ensuring that the safe is empty and ready to be moved. MA will not move the safe if the form is not attached.

After the safe is turned in to MA, the HSO must remove the safe information from his/her Appendix to the HQFMSP. It is also a good practice for the HSO to e-mail the APR apprising him/her of the fact that the safe has been turned in to MA so that the APR can update the property records.

Your HSO will provide the forms and instructions that you need for the excess process. **Listed below** are the forms you will need before excessing your safe container and instructions on where to find them.

Forms to be Used when Excessing a Safe

1. HQ Form 5632.12, Container/Equipment Inspection Certificate

This form is mandatory and should be completed and signed by the owner of the safe **and** the HSO. Before the form is completed, the owner of the safe should check each of its drawers to ensure that no classified matter and/or documents remain. Use a flashlight to check the very back of and underneath each drawer to verify that no documents are “stuck” in between or under the drawers. Any items in the safe at the time of inspection must be removed and, if classified, stored properly in another security container, or destroyed. The HSO should be present to witness the owner’s inspection of the safe and ensure that the inspection is complete (signing the inspection sheet). The form should then be taped to the front of the security container. ***This form can be obtained at the Forrestal and Germantown Copy Centers.***

2. Standard Form 700, Security Container Information

This form should be inside every safe drawer that has a lock. If the safe has multiple locking drawers, the form should be in every drawer containing a lock. The form contains information about the safe, its custodian(s), information on who to contact in case the safe is found open and unattended, and the names of all personnel with access to the safe. The cover sheet (Part 1) of the form and all copies of the combination portion (Parts 2 and 2A) of the form should be destroyed when the safe is turned in as excess. The form should be destroyed consistent with the classification level and category shown on it.

3. Optional Form 89, Maintenance Record for Security Containers/VTR Doors

This form should be in every safe drawer that has a lock. If the safe has multiple locking drawers, the form should be in every drawer containing a lock. The form is usually blank but will be completed when/if the security container requires maintenance of any kind. ***This form should ALWAYS remain inside the security container, whether it is moved or not. This form can be found here: <http://www.gsa.gov/portal/forms/download/115434>. You can print the form and put it in your security container.***

At the end of this process, nothing should remain in the security container except the OF 89.

ATTACHMENT 507-2

Moving a Safe with No Change in Custodians

- Before moving a safe from one location to another, i.e., a different office location, contact your HSO for specific instructions.
- Your HSO will contact your element's APR who, in turn, contacts MA to request a date for the safe to be moved. The APR will notify you when this date is established.
- If you are to remain the custodian for the safe, you do not have to check or empty the contents, complete any forms, or change the combination. You should, however, change the room number on your present SF-700, *Security Container Information* (all copies).
- If you are moving the safe because you are relocating to another office, ensure that any person/persons who currently share your safe (i.e., who have access to the combination) remain on your SF-700. If you do not want those persons to have access to your safe in your new location, complete a new SF-700 showing you as the custodian and any other person/persons that you choose to have access to your safe.
- The safe must remain locked at all times during the move.
- It is advisable that either you or your HSO be present during the move to ensure that there is no compromise of the safe or its contents and that the safe is delivered to its designated location.

No additional forms are needed for this particular move situation. However, ***the HSO should change his/her Appendix to the HQFMSP to reflect the new location of the safe. It is also a good practice for the HSO to e-mail the APR apprising him/her of the fact that the safe has been moved and providing the old room number and the new room number, so that the APR can update the property records.***

ATTACHMENT 507-3

Moving a Safe with a Change in Custodians

- Before moving a safe from one location to another, i.e., a different office location, contact your HSO for specific instructions.
- Your HSO will contact your element's APR to request a change in ownership of the safe and to schedule a date for moving it. The APR, in turn, contacts MA to request a date for the safe to be moved. The APR will notify you when this date is established.
- The HSO must contact either the Forrestal or Germantown Badge Office to make an appointment to have the combination on the safe reset to a number of the new custodian's choosing.
- **BEFORE** the transfer/move date of the safe, you and your HSO should:
 1. Examine the safe, remove all contents, and either destroy the classified contents or store them in another security container (instructions on this process are listed below under "Forms to be Used"). All OF 89s, *Maintenance Record for Security Containers/VTR Doors*, **must be retained within the safe**.
 2. Destroy both the SF-700, *Security Container Information*, that is inside the safe and the extra copy that should be stored elsewhere (it contains the actual combination to your security container). The old SF-700 should be destroyed as appropriate for the classification level of the SF-700.
 3. Attach a handwritten sign on the front of the safe stating "EMPTY." This is optional, but it is recommended because it clearly indicates that the safe has been cleared out.
 4. Complete and affix HQ F 5632.12, *Container/Equipment Inspection Certificate* (see form listed below), ensuring that the safe is empty and ready to be moved. MA will not move the safe if the form is not attached.
 5. The new custodian and his/her HSO should be present when the badge office completes the task of resetting the combination, ensuring that the new combination is known to the new owner and works properly.
 6. The new custodian completes a new SF-700 with the new combination, new owner information, and information about all those who will have access to the safe.
 7. After the safe is moved, the HSO annotates his/her Appendix to the HQFMSP to reflect the new owner/location. If the new owner or location is a different HQ element, the HSO transferring the safe should contact the HSO gaining the safe to advise him/her of the move. If the move is within the same HQ element, it is also a good practice for the HSO to e-mail the APR apprising him/her of the fact that the safe has been moved and

providing the name of the new custodian and the location, so that the APR can update the property records.

Forms to be Used when Moving a Safe to a New Custodian

1. HQ Form 5632.12, *Container/Equipment Inspection Certificate*

This form is mandatory and should be completed and signed by the owner of the safe **and** the HSO. Before the form is completed, the owner of the safe should check each of its drawers to ensure that no classified matter and/or documents remain. Use a flashlight to check the very back of and underneath each drawer to verify that no documents are “stuck” in between or under the drawers. Any items in the safe at the time of inspection must be removed and, if classified, stored properly in another security container, or destroyed. The HSO should be present to witness the owner’s inspection of the safe and ensure that the inspection is complete (signing the inspection sheet). The form should then be taped to the front of the security container. ***This form can be obtained at the Forrestal and Germantown Copy Centers.***

2. Standard Form 700, *Security Container Information*

This form should be inside every safe drawer that has a lock. If the safe has multiple locking drawers, the form should be in every drawer containing a lock. The form contains information about the safe, its custodian(s), information on who to contact in case the safe is found open and unattended, and the names of all personnel with access to the safe. The cover sheet (Part 1) of the form and all copies of the combination portion (Parts 2 and 2A) of the form should be destroyed when the safe is emptied. The form should be destroyed consistent with the classification level and category shown on it.

The safe’s new owner should create a new SF-700 and post it properly within each locking drawer. The combination portion of the SF-700 should be placed in a different security container and at the servicing CAS.

3. Optional Form 89, *Maintenance Record for Security Containers/VTR Doors*

This form should be in every safe drawer that has a lock. If the safe has multiple locking drawers, the form should be in every drawer containing a lock. The form is usually blank but will be completed when/if the security container requires maintenance of any kind. ***This form should ALWAYS remain inside the security container, whether it is moved or not. This form can be found here: <http://www.gsa.gov/portal/forms/download/115434>. You can print the form and put it in your security container.***

At the end of this process, nothing should be left in the security container except the OF 89.

Section 508

Reproducing Classified Matter

This section describes how to properly reproduce classified documents at DOE HQ.

HQ Implementation Procedures

Reproduction of classified documents must be limited to the minimum number of copies consistent with operational requirements and any further reproduction limitations indicated on the document. Reproduction must be performed by authorized, appropriately cleared individuals knowledgeable of the procedures for classified reproduction and only in the performance of official or contractual duties. Reproduced copies are subject to the same protection and control requirements as the original.

Restrictions:

Classified documents may be reproduced without approval of the originator, except where documents contain markings that limit reproduction without the specific written approval of the originator. Markings that limit the reproduction of classified matter include:

- TS/FGI may not be reproduced without the express permission of the originating government, except as needed to facilitate review for declassification. However, after such reviews are completed, reproduced documents containing classified information must be destroyed in accordance with Section 514, Destruction of Classified Matter.
- For Intelligence Community documents only, the Originator Controlled (ORCON) caveat marking may be used to restrict reproduction to only that allowed by the originator.
- For non-Intelligence Community documents, the following statement, or one similar in content, may be used to restrict reproduction to that allowed by the originator:

REPRODUCTION REQUIRES APPROVAL OF THE ORIGINATOR

Reproduced accountable documents must be brought into accountability (see Section 509, Accountability of Classified Matter).

Reproduction Machines:

Reproduction of classified documents in HQ facilities must be accomplished only on machines located within LAs or VTRs that are specifically approved for classified reproduction. The LA or VTR must also be accredited for classified reproduction and be so annotated on the Security Area Approval certificate (see Section 201, Establishing, Maintaining, and Deactivating LAs,

VTRs, and TLAs, for a discussion of Security Area Approval certificates). Machines approved for classified reproduction are designated by conspicuously posted copier certification signs specifying the highest level and category of classified matter that may be reproduced. The copier certification sign must contain the make, model and DOE property number of the authorized copier and be signed and dated by the element HSO and/or Information Systems Security Officer (ISSO). Certification signs for classified reproduction machines are machine- and room-specific. Relocation or replacement of a classified copier requires a newly initiated sign. A sample of the Certification Sign is provided in Attachment 508-1. Additionally, notices regarding any restrictions or requirements pertaining to the reproduction of classified documents on a particular copier must also be posted conspicuously next to the copier. A sample of Classified Reproduction Procedural Instructions to be posted by the HSO is provided in Attachment 508-2.

All Headquarters reproduction machines that are within an LA or VTR but are NOT approved for classified reproduction must have a sign posted near the machine indicating it is not approved for classified reproduction. A sample sign is provided in Attachment 508-3.

NOTE: All facsimile machines are considered to be copiers and are subject to the same signage requirements as copiers.

Both classified and unclassified digital copiers must undergo an approval process prior to purchase or lease. The element ISSO can help determine which digital copiers may be acquired and what security measures must be met. Also, the element HSO should be informed when a new copier is acquired.

Any digital copier located in an LA accredited for closed storage and for classified reproduction must have its hard drive removed and appropriately stored and must be powered down whenever the area is unattended. Likewise, any digital copier located in a VTR that is not approved for open storage must be powered down and the hard drive removed and stored as described above. Digital copiers without hard drives may be located in LAs or VTRs accredited for closed storage and classified reproduction; such copiers must still be powered down when the area is unattended.

Digital copiers located in VTRs approved for open storage may be left unattended without removing the hard drive or powering down the machine in accordance with approved open storage procedures.

Reproduction Process:

Inside an LA or VTR, classified documents must be transported to and from the reproduction machine area in the appropriate manner (see Section 511, Receipt and Transmission of Classified Matter). Access to classified matter being reproduced must be controlled to preclude unauthorized disclosure.

When copying is complete, the reproduction path and all paper trays of the reproduction machine should be checked to ensure no classified matter has been retained. Collection trays of double-

sided copy machines demand particular attention. Any remaining classified matter should be handled and disposed of in a manner approved for classified destruction.

After reproduction has been completed, one blank copy should be made and carefully examined to ensure that all residual images are eliminated from the machine. If examination of this blank copy reveals no images, it may be disposed of normally (recycle or general trash, as appropriate). If any previously reproduced image or portion thereof appears on the blank copy, repeat the procedure as necessary, handling and disposing of all blank copies as classified non-accountable matter. Contact your HSO immediately regarding this problem.

If a paper jam or other malfunction cannot be readily resolved, the HSO must be summoned; however, at no time may classified matter be left unattended within the copier room or area. The phone number of the HSO is posted on the certificate for the classified copier. A passerby may be summoned to provide assistance in contacting the HSO.

Classified copies should be properly marked as soon as possible.

Reproducing classified matter on copiers located outside of LAs and VTRs is PROHIBITED.

Points of Contact

For information about the HQ CMPC Program, call (301) 903-9986 or (301) 903-1163.

Forms/Samples/Graphics

Sample Classified Reproduction Certification Sign (see Attachment 508-1)

Sample Classified Reproduction Procedural Instructions Sign (see Attachment 508-2)

Sample Copier Not Approved for Classified Sign (see Attachment 508-3)

Helpful Website

<http://www.hss.energy.gov/HQSecOp/cmpc.html>

ATTACHMENT 508-1

Sample Classified Reproduction Certification Sign

This Machine
AUTHORIZED for the REPRODUCTION
of up to and including

SECRET/RD

Subject to the restrictions contained in the
Headquarters Facilities Master Security Plan
**Valid Only With Current DAA Accreditation and Approved Security Plan for
this Digital Copier**

Date of Accreditation _____ Date of Expiration _____

ISSO _____ HSO _____
(printed name and phone number) (printed name and phone number)

Room _____ Organization _____

Copier Information _____
Make Model DOE Property Number

REF #: HS-1.31-2008-50

ATTACHMENT 508-2

Sample Classified Reproduction Procedural Instructions

CLASSIFIED REPRODUCTION PROCEDURAL INSTRUCTIONS FOR DIGITAL COPIERS

1. See accompanying *AUTHORIZATION SIGN* for classification limits and instructions.
2. Observation of classified operations must be limited to persons with appropriate clearance and need to know.
3. Reproduction authorizations are required for ORCON, NATO, SCI, or other control caveats which limit or prohibit reproduction without specific permission.
4. Limit number of copies to only that which is absolutely required. If matter is accountable, all copies must be brought under control.
5. Unacceptable or excess copies **MUST** be collected and destroyed as classified information (accountability and destruction receipts not required).
6. After copying operations are completed, see "Sanitization Procedures for Digital Copiers" sign for sanitization instructions.
7. **DOUBLE CHECK** the copying area before departing to ensure no classified matter remains (i.e., originals removed from copying plate, copies removed from machine collection tray(s) or collating bin(s), and copies to be destroyed are collected).
8. The ISSO must be notified of any anomalies experienced during the classified copying process (i.e., paper jams, images remaining on the blank copy, unauthorized exposure of uncleared individuals to classified information, classified documents found in the copier at the start of copying operation, etc.)

POST THIS NOTICE IN THE IMMEDIATE VICINITY OF COPIERS USED FOR CLASSIFIED REPRODUCTION

REF #: HS-1.31-2008-14a

ATTACHMENT 508-3

Sample Copier Not Approved for Classified Sign

Classified Activities **PROHIBITED** on This
Equipment
Absolutely NO Exceptions!



Section 509

Accountability of Classified Matter

Most classified matter does not require accountability; however, several types of classified matter do require accountability due to national, international, or programmatic requirements.

Accountability systems provide an audit trail or chain of custody for the Department's most sensitive classified documents and media. Types of classified matter encountered at DOE HQ that require accountability include, but may not be limited to:

- All TS matter, including TS/FGI.
- S/RD (or higher) matter stored outside an LA or higher.
- Any matter that requires accountability because of national, international, or programmatic requirements.
- National requirements, such as Cryptography (CRYPTO) and designated COMSEC.
- International requirements, such as NATO ATOMAL (Restricted Data), designated United Kingdom (UK) documents, or other FGI designated in international agreements.
- Special programmatic requirements (e.g., SAP and Sigma 14).
- Secret documents containing FGI if so designated in a treaty or international agreement.
- Prior to April 12, 2011, media containing S/RD or higher was designated as Accountable Classified Removable Electronic Media (ACREM) and was accountable. After April 12, 2011, media formerly designated as ACREM remains accountable only if it qualifies under the current definition of accountable matter contained in DOE Order 471.6, *Information Security*. The media formerly designated as ACREM must remain in accountability until verification that none of the information that requires the media to be accountable (including nuclear weapons data) can be retrieved or recovered from that piece of media, or until the media is destroyed. The term ACREM is no longer used.
- Completed Parts 2 and 2A of SF-700, *Security Container Information*, constitute an accountable document if any of the information stored in that container is accountable. It does not, however, need to be placed into the formal accountability system (as detailed below). A simple paper or computerized log will satisfy accountability requirements for these parts of the SF-700 if the log includes the container number as the unique identification number, date created, classification level and category, and date taken out of accountability and reason (e.g., change of combination, or turn-in of container). Classifier and declassification information are not required on an SF-700.

HQ Implementation Procedures

Accountability Systems:

Classified Document Control Station (CDCS) personnel within each HQ element, with the assistance of the HQ CMPC Program Manager, must establish a system to track the element's accountable classified matter. See Section 510, Classified Document Control Stations, for a discussion of CDCS operations. Accountability records are required when accountable matter is originated, reproduced, transmitted, received, destroyed, or changed in classification.

Accountable documents must be assigned a unique number to track the document throughout its life in that office. The accountability system must have the capability to reflect each transaction (generation, reproduction, transmission, declassification/downgrading, destruction, etc.) performed for documents entered into the accountability system. Overall accountability system requirements are detailed in DOE Order 471.6, *Information Security*.

Inventories:

CDCS personnel must inventory all accountable documents annually. The inventory must include a visual verification of each document, as well as a reconciliation of the documents on hand with the list of documents in the accountability records.

Any discrepancies found during the inventory must be reported to the element HSO, who must in turn report those findings to the HQ Security Incidents and Infractions Program Manager within HS-91 and the CMPC Program Manager within HS-92. Inventory discrepancies may be reportable as Incidents of Security Concern as described in Chapter 11, Incidents of Security Concern. The HQ Security Incidents and Infractions Program Manager may instruct the element HSO to complete and submit DOE F 5639.2, *Reporting Unaccounted for Documents*, in order to document the inventory discrepancy.

In conjunction with the inventory process, or on a continuous basis, HSOs are to ensure that organizational classified holdings are reviewed for the purpose of inventory reduction.

Accountability Records:

Accountability records must include the following information for each accountable item:

- Date of the matter
- Brief description of the matter (unclassified description preferred)
- Unique identification number (each document, including reproductions, must have a unique number assigned to it)
- Classification level, category (if RD/FRD/TFNI), and caveat (if any)

- Disposition of the accountable matter (e.g., destruction, reproduction, downgrading, declassification, dispatch outside the facility, or incorporation into another accountability record and the date)
- Originator identification
- Authority for contractor retention
- Date received (if applicable)
- Office/activity from which the matter was received (if applicable), including the office or activity name and address from which matter was transmitted to the recipient
- The individual who checked it in and/or out (i.e., the person who has personal responsibility for it).

Accountability records ensure a chain of custody so that all accountable matter can be located at any given time, whether it is stored or in use. Accountability procedures should be recorded in an organization's CDCS procedures (see Section 510, Classified Document Control Stations).

Accountable information temporarily transferred to another organization within the same facility must be entered into the receiving organization's accountability records if the material is kept more than 180 days without return to the sender.

Master files and databases created in central data-processing facilities to supplement or replace Top Secret records are not authorized for disposal under General Records Schedule 18. This type of file must be scheduled on DOE F 1324.5, *Request for Records Disposition Authority*.

All accountability records (e.g., logs, inventory records, receipts) for Secret and Confidential material shall be maintained for 2 years. Accountability records for Top Secret shall be maintained for 5 years.

Points of Contact

For information about the HQ CMPC Program, call (301) 903-9990.

Forms/Samples/Graphics

DOE Form 5639.2, *Reporting Unaccounted for Documents* (for a copy of this form go to <http://energy.gov/sites/prod/files/cioprod/documents/5639-2.pdf>)

DOE F 1324.5, *Request for Records Disposition Authority* (for a copy of this form go to <http://energy.gov/cio/downloads/doe-f-13245>)

Helpful Websites

The HQ CMPC Program website is at: <http://www.hss.energy.gov/HQSecOp/cmpc.html>.

To view DOE Order 471.6, *Information Security*, go to:
<https://www.directives.doe.gov/directives/0471.6-BOrder-admchg1/view>.

Section 510

Classified Document Control Stations

DOE Order 471.6, *Information Security*, requires that control stations be established to control the classified matter received by and/or dispatched from DOE facilities. Personnel must be designated and specially trained to operate these control stations and must have security clearances commensurate with the level of their classified matter control responsibilities. At DOE HQ, a control station is known as a Classified Document Control Station (CDCS).

HQ Implementation Procedures

Applicability and Scope:

Each HQ element that receives or transmits classified matter, or that has the potential to receive or transmit classified matter, must establish at least one CDCS. A CDCS is a gateway through which all incoming and outgoing classified matter must transit. HQ elements may establish more than one CDCS, such as one at the Forrestal Building and another at the Germantown Building, when additional CDCSs are needed for efficient operations. An HQ element that has minimal classified holdings or only an occasional need to receive or transmit classified matter may establish a partnership with another element to use their CDCS.

The purpose of the CDCS is to prevent unauthorized access to and unauthorized removal of the element's classified matter. A CDCS is the primary point where classified matter may be received or transmitted by the HQ element. CDCS personnel generate the records required for the receipt and transmittal of classified matter, maintain access lists (when required), and generally control the classified matter received by and/or dispatched from the element.

CDCS Standard Operating Procedures must be developed in detail and updated as necessary by the station operators in consultation with the element HSO and the HQ CMPC Program Manager.

Appointments and Designations:

1. CDC Station Operators and Alternates – The Head of each HQ element with a CDCS, **or his/her designee**, must appoint one Primary CDCS Operator and at least one Alternate CDCS Operator for each CDCS within the element. The responsible HSO must enter the names of the appointees into the element's Appendix to the HQFMSP and must notify the CMPC Program Manager in writing. The names of the appointees must be readily available for surveys and inspections. The number of CDCS operators should be kept to the minimum required to process the amount of classified mail, facsimiles, and other matter received or transmitted by the element.

CDCS personnel must possess a security clearance commensurate with the highest level and category of classified matter that passes through the CDCS.

2. Classified Mailing Address (CMA) Authorized Designees – Each HQ element with a CDCS must appoint specific cleared individuals to act as CMA Authorized Designees, who are authorized to receive classified United States Postal Service (USPS) mail from the Forrestal and Germantown Central Mailrooms. CMA Authorized Designees are normally the CDCS operators; however, in unique circumstances where minimal additional designees are required, other cleared personnel may be appointed. CMA Authorized Designees who are not CDCS operators must be trained by their HSO or the HQ CMPC Program Manager in the handling of classified matter in accordance with operational procedures in place within the organization.

Since the Central Mailrooms at the Forrestal and Germantown Buildings will only deliver classified mail to a CDCS, they need to be informed of the locations of all CDCSs and the names of the CMA Authorized Designees who can accept classified mail when it is delivered. The mailrooms obtain this information from the registry of CDCSs and CMA Authorized Designees that is maintained by the HQ CMPC Program Manager.

HSOs must send an e-mail identifying the locations of their element's CDCS(s) and the names of their CMA Authorized Designees. The HSO must also provide immediate e-mail updates as required. The e-mail address to be used for the updates is shown in Attachment 510-1. The HQ CMPC Program Manager uses the e-mails to maintain the registry of CDCSs and designees.

3. Express Mail Document Control (EMDC) Designees – All incoming overnight express mail has the potential to contain classified matter; therefore, all overnight express mail packages must be handled as classified matter. Each HQ element with a CDCS must appoint specific, cleared individuals to act as EMDC Designees.

HSOs must send an e-mail identifying the names of their EMDC Designees and must provide immediate e-mail updates whenever there are changes. The e-mail address to be used for the updates is shown in Attachment 510-2. The HQ CMPC Program Manager uses these e-mails to maintain a registry of EMDCs.

Training:

All CDCS personnel must complete CDCS training before assuming CDCS duties. This training is tailored to the responsibilities of CDCS personnel and includes the following subject areas: generation and marking, physical protection and storage, reproduction, accountability, transmission and receipting (including hand-carry), destruction, and emergency procedures. CDCS training is provided by the HQ CMPC Program Manager. On a case-by-case basis, the CMPC Program Manager is authorized to temporarily waive the training requirement based on an individual's previous experience and the ability of the

organization's HSO to guide the individual on CDCS duties until the formal training is available.

CDCS Operations:

1. Receipt of Classified Matter – All incoming classified matter must transit through an element's CDCS before being released for storage in any other organization's designated classified document repository. This requirement applies to all incoming classified mail, as well as other classified matter hand carried into HQ facilities.

Upon receipt of the matter, CDCS personnel examine the package for evidence of tampering, as applicable, open the package, and determine whether to retain the material (e.g., accountable matter) or release it to another classified document repository custodian. When transferring classified matter to another authorized classified document repository custodian or classified matter user within the organization, CDCS personnel are responsible for ensuring that they give the classified matter only to individuals with appropriate security clearances (i.e., a security clearance equal to or higher than the information) and that the transfer is accomplished without compromising the material (e.g., left unattended on the desk of a repository custodian).

CDCS personnel must inspect package contents to ensure all classified documents are marked with the highest classification level at the top and bottom of the front page and back page. CDCS personnel affix the appropriate classified cover sheet to the document (if it is not already affixed). For any other discrepancy in document marking, the document recipient is responsible for reconciling it with the sender.

CDCS personnel are also responsible for reconciling the package contents with the document receipt and returning the signed receipt to the sender as soon as possible. Discrepancies between the package contents and the package receipt are reported immediately to the sender. If the discrepancy cannot be resolved in one business day, the HQ CMPC Program Manager must be notified. Copies of signed receipts are maintained at the CDCS in accordance with the DOE Records Schedule and the National Archives and Records Administration (NARA) General Records Schedule (2 years for Secret and Confidential, and 5 years for Top Secret).

NOTE: Although receipts for Confidential matter are not required, any receipt received with Confidential matter must be signed and returned.

2. Transmission of Classified Matter – All classified matter being transmitted out of an HQ element (mailed or hand carried) must be processed through the element's CDCS. CDCS personnel ensure that appropriate document receipts (such as DOE F 470.10, *Classified Matter Receipt*) are used, the package is properly marked and wrapped, and the appropriate mail carrier and CMAs are used. The document sender is responsible for ensuring that the document is properly marked with appropriate

classification markings. Most organizations task the CDCS personnel with the responsibility for ensuring that the CMA has been verified by consulting the information contained in SSIMS. Additionally, it is the responsibility of the sender, not CDCS personnel, to provide the transmittal letter (when required) to be included in the package with the classified matter.

CDCS personnel prepare an outgoing *Classified Matter Receipt* in triplicate when mailing and quadruplicate when preparing a package for hand carry. They maintain a copy of the outgoing receipt in a suspense file until the signed receipt is returned from the recipient. Copies of returned signed receipts are maintained at the CDCS in accordance with the DOE Records Schedule and the NARA General Records Schedule (2 years for Secret and Confidential and 5 years for Top Secret).

NOTE 1: Classified Matter Receipts are not required for outgoing Confidential matter, unless the outgoing Confidential matter is being hand carried outside of an HQ facility and the receipt is used to document what matter is being hand carried.

NOTE 2: It is recommended that signed receipts be returned by the recipient within 15 days. Mandatory follow-up action is required if receipts are not returned within 30 days.

For all classified matter hand carried outside of an HQ facility, a copy of the receipt, or other manifest, must be left with the servicing CDCS, and one signed Unclassified copy must be carried on the person of the individual hand carrying the package. If the hand carried matter is returned to the same CDCS, the receipt copy is used to reconcile the original package contents with what is returned. If the hand carried matter is left at a destination and the courier had the recipient sign a receipt, the courier must return the receipt to the CDCS. If the hand carried matter is destroyed by the hand carrier at the destination, the individual should annotate the receipt with the date, time, and location of destruction; certify the destruction with his/her signature on the receipt; and return the receipt to the servicing CDCS, or certify the destruction using a DOE F 5635.9, *Record of Destruction*. The DOE F 5635.9 should be given to the appropriate CDCS personnel by the individual hand carrying the classified matter upon his/her return to the facility.

NOTE: Classified matter hand carried outside the facility but intended for return to the CDCS on the same day must be on record with the CDCS. All hand carried classified matter must be reconciled upon return to the facility.

Facsimile Classified Document Control Stations:

Since a facsimile machine is capable of receiving and transmitting information, a facsimile machine approved for receiving and transmitting classified documents is, by definition, a CDCS. A facsimile machine may function separately as a stand-alone CDCS, or it may be a piece of equipment within an established CDCS.

If the classified facsimile machine is a stand-alone CDCS, Primary and Alternate Control Station Operators must be appointed and listed in the element's Appendix to the HQFMSP in the same manner as a normal CDCS.

Although Primary and Alternate Control Station Operators are appointed for each classified facsimile machine, other users trained in the operation of the classified facsimile equipment and procedures may be authorized to use the equipment. Therefore, all classified facsimile machine users must comply with all the established procedures.

The person using the STE encryption interface to a classified facsimile machine is responsible for ensuring that the individual on the receiving end possesses the appropriate security clearance and need-to-know before transmitting any data. SSIMS validation is also required to ensure that the facility has the appropriate storage capability for the transmitted classified matter.

Receipt of classified facsimiles must be confirmed with the intended recipient. Facsimile logs, or separate receipts, must be retained for all (including Confidential) incoming and outgoing classified matter. NARA guidelines are applicable for maintaining records. Return facsimile receipts are preferable; however, verbal acknowledgement of receipt of classified transmission is permitted but must be annotated (either on the facsimile log or on the record copy of the outgoing facsimile cover page) with the name of the person receiving the classified facsimile, time and date received, and number of pages received. Discrepancies in the number of pages received and the number of pages transmitted must be resolved immediately.

Appropriate classification markings, as in any classified document, are required for all incoming and outgoing classified facsimiles. Specific attention must be given to the overall classification level marking of the outside of the back page of an incoming classified facsimile. If applicable, formal accountability for incoming and outgoing classified facsimiles is required.

Classified cover sheets must be applied to all incoming classified facsimiles immediately after receipt and before distribution.

Points of Contact

For information about the HQ CMPC Program, call (301) 903-9986.

Forms/Samples/Graphics

Sample E-Mail Notification for Classified Mailing Address Authorized Designees (see Attachment 510-1)

Sample E-Mail Notification for Express Mail Document Control Designees (see Attachment 510-2)

DOE Form 470.10, *Classified Matter Receipt* (for a copy of this form go to http://energy.gov/sites/prod/files/cioprod/documents/Form_470_10_fillable_X.pdf)

DOE F 5635.9, *Record of Destruction* (for a copy of this form go to <http://energy.gov/sites/prod/files/cioprod/documents/5635-9.pdf>)

Helpful Websites

The HQ CMPC Program website is at: <http://www.hss.energy.gov/HQSecOp/cmhc.html>

To view the *DOE CMPC Marking Resource*, go to: http://www.hss.energy.gov/SecPolicy/DOE_CMPC_Marking_Resource.pdf

ATTACHMENT 510-1

Sample E-Mail Notification for Classified Mailing Address Authorized Designees

Send the e-mail to: "HS 92 Operations"

The e-mail "Subject" block should be: "Notification of Classified Mailing Address (CMA) Authorized Designees"

The body of e-mail should include the following information:

"The Office of _____ has approved the following personnel to receive and open classified USPS mail addressed to this office:

Name of Designee: _____ Security Clearance Level: _____

Organization code and/or organizational name:

Building name:

Room number/location of Classified Document Control Station:

Telephone number:

Repeat the above information, as necessary, to identify all designees.

If the person is to be added to an existing list of designees, clearly include the word "ADD" behind the person's name.

If a person is to be deleted, an e-mail notification is also required. Indicate in the body of the e-mail that the person is no longer approved to receive and open classified USPS mail, and include the word "DELETE" behind the person's name.

E-mails will be accepted only from the element HSO.

ATTACHMENT 510-2

Sample E-Mail Notification for Express Mail Document Control Designees

Send the e-mail to: "HS 92 Operations"

The e-mail "Subject" block should be: "Notification of Express Mail Document Control Designees"

The body of e-mail should include the following information:

"The Office of _____ has approved the following personnel to receive and open express mail packages addressed to this office:

Name of Designee: _____ Security Clearance Level: _____

Organization code and/or organizational name:

Building name:

Room number/location of Classified Document Control Station:

Telephone number:

Repeat the above information, as necessary, to identify all designees.

If the person is to be added to an existing list of designees, clearly include the word "ADD" behind the person's name.

If a person is to be deleted, an e-mail notification is also required. Indicate in the body of the e-mail that the person is no longer approved to receive and open classified express mail, and include the word "DELETE" behind the person's name.

E-mails will be accepted only from the element HSO.

Section 511

Receipt and Transmission of Classified Matter

This section describes DOE HQ procedures for the receipt and transmission of classified matter. The Forrestal, Germantown, and 955 L'Enfant Plaza facilities are the only HQ facilities authorized to conduct classified activities; therefore, classified matter can only be received or transmitted at those HQ facilities. DOE-approved contractor sites are permitted to receive and transmit classified matter in accordance with their DOE contract(s), their FDARs (DOE F 470.2 – see Chapter 4), and their security plans.

HQ Implementation Procedures

All classified matter received or transmitted by HQ elements must be processed through a CDCS (see Section 510, Classified Document Control Stations). The CDCS is responsible for receiving all classified matter addressed to the element and transmitting all classified matter dispatched by the element. In short, the element's CDCS is the organization's gateway for all incoming and outgoing classified matter. The CDCS also maintains the associated classified document receipts and any required inventory records.

Receiving Classified Matter by Mail:

All mail, including express mail, is initially received by the two HQ Central Mail Rooms located at the Forrestal and Germantown Buildings. The mailrooms sort and deliver the mail in accordance with established procedures. All registered, certified, and express mail is handled as controlled mail and distributed only to CDCS personnel who have been specifically designated to receive classified and express mail (see Section 512, Classified Mailing Addresses, and Section 513, Express Mail Service).

Receiving Classified Matter by Facsimile:

A classified facsimile machine is, in itself, a CDCS or part of an existing CDCS. Rules for receiving classified facsimiles are contained in Section 510, Classified Document Control Stations.

Headquarters Classified Mailing Addresses:

All classified mail being sent to a HQ element via the USPS must use the proper CMA.

The CMA for HQ elements located in the Forrestal and 955 L'Enfant Plaza facilities is:

ATTN: (ORGANIZATION) (INTENDED RECIPIENT)
US DEPT OF ENERGY
PO BOX 23865
WASHINGTON DC 20026-3865

The CMA for HQ elements located in the Germantown facility is:

ATTN: (ORGANIZATION) (INTENDED RECIPIENT)
US DEPT OF ENERGY
PO BOX A
GERMANTOWN MD 20875-0963

Transmitting Classified Matter in General:

Classified matter may be transmitted only in the performance of official and contractual duties. Unless the transmission is required by the specific terms of the contract or required for performance of the contract, the contractor must obtain written authorization from the contracting HQ element before transmitting classified matter outside of the facility.

The CDCS servicing an HQ element is expected to perform most of the actions associated with transmission of classified matter. These actions include selecting the proper method of transmission, packaging and wrapping the matter appropriately, preparing classified document receipts when required, maintaining transmission logs when required, and maintaining accountability records when required. The HQ CMPC Program Manager provides training for CDCS personnel throughout the year.

The individual for whom the CDCS is transmitting the classified matter is responsible for knowing the name of the intended recipient, verifying that he/she has the appropriate security clearance, and ensuring that he/she has need-to-know. **CDCS personnel are responsible for determining the recipient's CMA and verifying that the receiving facility is approved by DOE to store classified material at a classification level and category equal to or higher than what is being transmitted, unless the organization's CDCS procedures delegate that responsibility to some other individual(s).**

Transmission of Top Secret Matter:

Top Secret matter may be transmitted out of HQ facilities only by the Defense Courier Service, Department of State Courier System, approved communications networks (including approved classified facsimile), Headquarters Courier Service (within the Washington, D.C. metropolitan area), and designated hand carry personnel (as designated by the organizational hand carry approval authority). Use of the USPS or other commercial organizations is prohibited.

Approved Methods for Transmitting Secret and Confidential Matter Outside of an HQ Facility:

1. HQ Courier Service – The HQ Courier Service may be used to transmit Top Secret, Secret, and Confidential matter between the Forrestal and Germantown facilities and to other Federal agencies in the Washington, D.C. metropolitan area. Classified matter must be **double wrapped**, properly marked, addressed to the proper CMA, and placed in an

HQ F 1410.5, *Classified Matter between Offices in DOE Headquarters*, red and white (“Candy Stripe”) envelope. HQ F 1410.6, *DOE Messenger Receipt*, must be attached to the “Candy Stripe” envelope, and the transaction must be logged into the courier’s register. All signatures on the HQ F 1410.6 must be accompanied by the signer’s DOE badge number or printed name. Both the HQ F 1410.5 and the HQ F 1410.6 must include the recipient’s name, organizational symbol, room number, and building or, if delivered to another government agency, the exact delivery point address. All classified matter to be couriered must also be accompanied by DOE F 470.10, *Classified Document Receipt*, or equivalent. These receipts must be retained for 5 years for Top Secret and 2 years for Secret and Confidential matter.

2. Transmission by the USPS – The USPS is the most common means of transmitting classified matter outside an HQ facility. All Confidential and Secret matter transmitted via USPS must be sent as Registered Mail, and the matter must be packaged and wrapped as described under “Packaging Classified Matter for Transmission Outside of an HQ Facility,” below. The matter must be sent to a CMA that has been verified through SSIMS.

USPS mail services cannot be used for Top Secret classified matter.

3. Transmission by Express Mail (Overnight Mail) Services – Express mail services shall not be used as a matter of routine or convenience for transmitting classified matter.

Express mail services cannot be used for Top Secret classified matter.

Use of any express service receptacles at or near a commercial building or at curbside locations is prohibited.

At a minimum, the following conditions must be met concerning express mail:

- Only designated CDCS personnel may prepare express mail packages for dispatch.
- Effective May 1, 2011, the HQ authorized commercial express mail service organization for outgoing classified express mail (overnight mail) is United Parcel Service (UPS). (Note: On rare occasions, a recipient organization may only accept incoming express mail service from a carrier other than UPS. The recipient’s requirement to use a carrier other than UPS must be recorded in SSIMS.) OGAs may send express mail to DOE via other carriers.
- Express mail addressees must be identified in SSIMS under “Overnight/Classified Common Carrier Address.” (Note that this is always a street address.).
- The return address on DOE transmitted express mail is:
 - o Forrestal: Sender’s Name (Routing Symbol)
US Dept of Energy

1000 Independence Ave SW
Washington DC 20585
o Germantown: Sender's Name (Routing Symbol)
US Dept of Energy
19901 Germantown Rd
Germantown MD 20874-1290

Express mail must not be used to transmit classified matter on Fridays or on days preceding a holiday. "Next business day" deliveries on Fridays or the day before a holiday are not authorized.

All classified matter must be properly receipted, all packages must be double wrapped, and envelopes must be appropriately addressed before being inserted into the packaging provided by the express mail service.

There must be no mark on the external express mail box or envelope to indicate or imply that it contains classified matter. This restriction includes positional titles such as classified document custodian, security officer, classified control station, or any other wording that denotes or implies the presence of classified matter.

The sender must notify the intended recipient(s) of the proposed shipment and arrival date. There must be no reference to the fact that classified matter is being transmitted unless notification is made through a secure telephone. In addition, the sender must inform the addressee of the commercial carrier package Air Bill Label Number.

To ensure direct delivery to the addressee only, the release signature block on the Air Bill Label will not be executed under any circumstance.

4. Transmission by Facsimile – Only CDCS personnel or their designees/authorized users may operate classified facsimile machines. Transmission of classified information via facsimile machines that are not accredited for classified operation by the OCIO is strictly prohibited.
5. Hand Carry – Personnel with a security clearance equal to or higher than the classification level and category of classified matter to be transmitted may be authorized to hand carry it between destinations. The various circumstances involving hand carry are described in detail in the subsections below.
6. Transmission by STE – A STE device must be used to transmit classified information telephonically. STEs must be used within HQ LAs or VTRs unless the HQ Communications Security Program Manager, within HS-1.2, has specifically approved their use in other locations, such as the residences of senior DOE officials. Generally, the speakerphone capability of a STE device will not be activated in the encrypted mode unless the LA or VTR has been approved for amplified discussion by the HQ TSCM Team.

Secure telephone calls are placed initially in the clear (non-secure) mode. When the caller desires to go secure, the keying device is activated by pressing the appropriate button on the instrument. This procedure places the instrument in the secure mode. The STE instrument then displays a message in the message window showing the highest classification level authorized to be discussed over the circuit. When not in use, the Fortezza card used to activate the STE's secure mode must be stored in a room separate from the STE instrument or in a GSA-approved repository in the same room as the STE instrument.

The STE user must clearly understand two important points:

- The person using the STE is responsible for ensuring that the individual on the distant end possesses the appropriate security clearance and need-to-know for the information being discussed.
- The person using the STE is responsible for ensuring that the classified portion of the discussion cannot be overheard by uncleared personnel who may be under escort inside or outside the local office area.

Also see Section 205, Secure Telecommunications Equipment (Phones).

Packaging Classified Matter for Transmission Outside of an HQ Facility:

Classified matter to be transmitted outside a facility must be double-wrapped (enclosed in opaque inner and outer containers) except as otherwise specified below.

1. Envelopes – When envelopes are used for packaging, the classified matter shall be protected from direct contact with the inner envelope. This can be done by affixing the appropriate cover sheet to both the front and back of the matter. The inner envelope shall be sealed and marked with the receiver's and the sender's classified mailing addresses, the overall classification level and category (if RD, FRD, or TFNI) of the contents, and any appropriate caveats. The outer envelope shall be sealed and marked with the receiver's and the sender's classified mailing addresses. No markings or notations shall be made on the outer envelope indicating that the contents are classified. All seams of both wrappings must be sealed with brown sealing paper tape to aid in preventing undetected, unauthorized access to the contents while in transit.
2. Bulky Items – If the item is of a size, bulk, weight, or nature precluding the use of envelopes for packaging, other containers of sufficient strength and durability shall be used to protect the item while in transit. Both the inner and outer containers will be marked as stated in the above paragraph.
3. Locked Briefcases – A locked briefcase is authorized for hand carrying of classified matter within the Washington, D.C. metropolitan area. If a locked briefcase is used to hand carry classified matter of any level, the briefcase may serve as the outer container (wrapper). The inner container shall be sealed, addressed with the sender's and recipient's

classified mailing addresses, and marked with the overall classification level (and category if RD, FRD or TFNI) of the contents and with any appropriate caveats (see above paragraphs concerning packaging). The briefcase (outer container) must indicate the classified mailing address of the carrier and shall contain no markings to indicate that the contents are classified. A commercial luggage tag containing this address, affixed to the briefcase, is suggested.

NOTE: A briefcase may not serve as the outer container for travel aboard commercial aircraft or when hand carrying or couriering classified matter to Congress or to an OGA when the intention is to leave the classified matter at the destination.

4. Tamper-Indicating Envelopes – Plastic tamper-evident security closures (bags, envelopes) are authorized for transmission of classified matter. For this use, tamper-resistant closures must meet all of the following criteria:

- High strength coex film, or high strength Mylar type material, or equivalent
- In-line closure
- Opaque
- Must not contain "zip open" feature.

Points to be considered when using tamper-indicating envelopes include:

- Standard classification and addressing markings must be applied.
- The use of rubber stamps (for classification, addresses, etc.) is not permitted because the rubber stamp ink will not completely dry and will rub off or smear on the envelope's surface.
- Permanent markers (e.g., Sharpie permanent marker, or equivalent) should be used for classification markings and addresses.
- These envelopes may be used as the inner and/or outer wrapper(s) when hand carrying.
- These envelopes may be used as the inner envelope/wrapper when transmitting classified matter through the USPS, but not as the outer envelope or wrapper.
- These envelopes may be used for the inner and/or outer envelope(s)/wrapper(s) when transmitting classified matter via express mail. The package would then be placed within the appropriately addressed packaging (envelope or box) provided by the express mail carrier.
- External sealing tape is not required.

- Use of mailing labels is not recommended because some brands of stick-on labels do not adhere well to the coex film or Mylar, and may detach in cooler temperatures.
5. Rifkin Safety Sac – The Rifkin Safety Sac® Document Handling Bag reusable key-locking fabric bag may also be used for hand carrying of classified material outside a facility.

Classified Mailing Addresses:

CMAs must be used for classified matter transmitted outside a HQ facility. These addresses are located in the SSIMS database and are valid for 30 days following the last database access.

NOTE: A mailing address for the inner envelope of a given facility may differ from the mailing address for the outer envelope for the same facility, and addresses for USPS registered and certified mail may differ from that of express or common carrier mail for the same facility.

Transmittal of Classified Matter between HQ Facilities (Other Than Hand Carrying):

The Forrestal, 955 L'Enfant Plaza, and Germantown facilities are considered to be separate facilities; therefore, *non-hand carried* classified matter transmitted between these facilities must be handled by the element's CDCS. The CDCS uses their internal established procedures to coordinate with the mail room and/or HQ Courier Service to effect the transmittal.

Classified Document Receipts:

An appropriately prepared DOE F 470.10, *Classified Matter Receipt*, must accompany all accountable and Secret documents transmitted outside a facility and must be enclosed within the inner envelope or container. If all items are going to one recipient, one receipt may be used for multiple items. Regardless of the number of items being transmitted, one receipt should be completed for each recipient. SSIMS must be consulted for appropriate and any special mailing instructions. All receipts should be Unclassified and should be prepared in triplicate, or quadruplicate if package is to be hand carried.

A record must be maintained for *all* classified matter, regardless of classification level, that is hand carried or couriered outside of an HQ facility. A DOE F 470.10 or equivalent manifest may be used to record the classified matter being hand carried or delivered to Congress.

Hand Carrying of Classified Matter within an HQ Facility:

Classified matter that will be hand carried to personnel located in a separate LA or VTR within the Forrestal, 955 L'Enfant Plaza, or Germantown facilities may be carried by personnel having an appropriate access authorization for the level and category of classified matter involved. The

matter must have the appropriate cover sheet attached to the front of a document and appropriate markings (or an appropriate cover sheet) on the outside back page or cover. The matter must be transported within an HQ F 1410.5, *Classified Matter between Offices in DOE Headquarters*, red and white striped envelope. The HQ F 1410.5 must be marked with the recipient's name, room number, routing symbol, and telephone number.

Hand Carrying of Classified Matter within a Limited or Exclusion Area:

Classified matter that will be hand carried to personnel located within the same LA or VTR within the Forrestal, 955 L'Enfant Plaza, or Germantown facilities may be carried by personnel having an appropriate access authorization for the level and category of classified matter involved. Transmittal is authorized with an appropriate cover sheet attached to the front of a document and appropriate markings (or an appropriate cover sheet) on the outside back page or cover.

Hand Carrying of Classified Matter Outside a Facility within the U.S.:

The Head of each HQ Element must designate in writing a responsible official (e.g., the HSO) within the element to approve employees to hand carry classified matter out of a facility. This authority should be limited to as few people as operationally feasible.

The individual(s) designated by the Head of Element to approve employees within the organization to hand carry classified matter must maintain a record of those granted the authority to hand carry.

Only classified matter that is absolutely essential for the purpose (e.g., visit or meeting) may be hand carried. Alternatives to hand carrying must be considered. Options include USPS Registered Mail, express mail services, use of DOE authorized courier service, and secure facsimile.

Individuals hand carrying classified matter shall have an access authorization equal to or higher than the classification level and category of the classified information involved and be aware of their responsibility to protect classified information.

Travelers must not take classified matter to private residences or other unapproved places (e.g., hotel or motel rooms). Therefore, travelers who expect to arrive at the destination outside normal duty hours must be instructed to make prior arrangements for storage of classified matter through the host security office. All classified matter, when not in the possession of authorized individuals, must be stored only in DOE-approved facilities, or as specified in approved contingency plans. Arrangements shall be made in advance of departure for overnight storage at an approved facility that has appropriate storage capability.

The individual(s) designated by the Head of Element to approve employees within the organization to hand carry classified matter are required to ensure that each individual they authorize to hand carry is briefed on hand carrying responsibilities. *A Sample Briefing for*

Persons Authorized to Hand Carry Classified Documents is provided in Attachment 511-1. A record of hand carry briefings must be maintained. Each briefing must include, at a minimum:

- Packaging and addressing
- Transportation
- Protection of classified matter
- Transfer and receipting of classified matter
- Storage requirements, if applicable, for securing classified matter outside the HQ facility
- Procedures to validate through SSIMS that the hand carry destination is approved for the appropriate classified matter to be used, stored, discussed, etc., at the intended destination
- Handling and associated prohibitions (e.g., hotels, restaurants, residences, etc.)
- Reporting loss/compromise
- Contingency plans (inability to get to destination, traffic or other emergencies, route diversions, alternate storage locations, etc.)
- Point(s) of contact for assistance.

The individual(s) designated by the Head of Element to approve employees within the organization to hand carry classified matter must provide approval each time classified matter is to be hand carried outside the Washington, D.C. metropolitan area. Repeated approval for hand carrying classified matter **within** the Washington, D.C. metropolitan area is not required and is valid until rescinded by the appropriate authority. Hand carrying classified matter **outside** the Washington, D.C. area is authorized provided that:

- The employee has received a hand carry briefing.
- An unusual situation warrants such action.
- The classified matter is not available or cannot be made available at the destination.
- Time does not permit transmission by other authorized means.
- The classified matter can be properly handled and protected while being hand carried.
- The transmission can be successfully completed on the same day.
- The classified matter can be appropriately stored upon arrival.
- Contingency plans for delayed arrival and unforeseen circumstances (e.g., unscheduled

overnight delay outside the destination area, or weather delays) have been developed and approved by the Element. A *Sample Hand Carry Contingency Plan* is provided in Attachment 511-2.

A record is required for *all* classified matter, regardless of classification level, that is hand carried outside a facility. An **Unclassified** copy of this record must be in the possession of the employee who hand carries the classified matter, and a copy of the record must be maintained by the element's HSO or CDCS. The record may be a DOE F 470.10 or a locally produced manifest/record that identifies the classified matter being hand carried. The DOE F 470.10, manifest, or record must include:

- Subject or title
- Classification level and category of the matter being hand carried
- Date of the matter being hand carried
- Date the matter was removed from the facility
- Signature of the person removing the matter
- Date the matter was returned, transferred, or destroyed.

When the hand carrying employee returns to the facility, CDCS personnel must make a full reconciliation of the hand carried classified matter by reviewing the returned classified matter, receipts, and/or destruction certificates.

Hand Carrying Aboard Commercial Aircraft within the U.S.:

Classified matter may be hand carried aboard commercial passenger aircraft within the U.S. with the approval of the Head of Element or his/her designee. The purpose of the airport procedures outlined herein is to preclude the opening of classified packages by the Transportation Security Administration (TSA) screening personnel. The Federal Aviation Administration (FAA) Advisory Circular dated 11/06/81 has been cancelled, and the TSA has replaced it with the guidelines below.

TSA Letter of Instruction to Carry Classified Material through a Screening Checkpoint at an Airport

The purpose of this guidance is to provide instruction to United States Government and contractor couriers on the procedures required to transport classified materials through TSA airport screening checkpoints.

Upon arrival at the screening checkpoint, ask a Transportation Security Officer (TSO) at the Travel Document Check or an available TSO stationed in front of the screening checkpoint to speak to the Supervisory Transportation Security Officer (STSO). The STSO will verify the courier's documentation, see list of required documentation below, and grant specialized screening of any classified materials carried by the courier. In order to transport U.S.

Government classified material through a TSA screening checkpoint at an airport, a courier must present to the STSO all of the following items:

- 1) Identification (ID) issued by his or her agency*
- 2) A second piece of Government-issued photo ID*
- 3) An authorization letter to carry the classified material from his or her agency with all of the following information:*
 - a. Full name of the agency*
 - b. Full name of the courier*
 - c. Date of issue and expiration date of the assignment*
 - d. Full name, signature, and telephone number of the official issuing the letter, card, or form*
 - e. Full name, signature, and telephone number of the official designated to confirm the letter, card, or form*

In the event that an authorization letter, card, or form is not presented, or if the letter is missing any information listed above, or if the courier is not able to produce two forms of ID, as explained above, the material will not be permitted into the sterile area unless it has been properly screened.

Please note that only the U.S. Government classified material is eligible for specialized screening, the courier and any non-classified property carried by the courier is subject to screening. The STSO will ensure that any classified material is always within the line of sight of the courier during the screening process and is not subject to any additional inspection.

The authorization letter to carry the classified material must be from the Head of Element or his/her designee and must be on letterhead stationery. In addition to the original letter, the traveler should also have sufficient authenticated copies to provide a copy to each airline involved. A *Sample Letter of Authorization to Transportation Security Administration to Hand Carry Classified Material* is provided in Attachment 511-3.

The classified package must be hand carried and not placed in checked baggage. The traveler is subject to normal screening procedures. Hand-held packages will normally be screened by x-ray examination. If security personnel are not satisfied with the results of the inspection, and the person hand carrying the material is requested to open a classified package for visual examination, the individual should inform the screener that the carry-on items contain U.S. government classified information and cannot be opened. Under no circumstances may the classified matter be opened by the traveler or security personnel.

Hand Carrying of Classified Matter outside the U.S.:

Hand carrying of classified matter outside the U.S. is generally prohibited. However, in rare circumstances, the HQ CMPC Program Manager or the HQ DOE Cognizant Security Authority may approve the transmission on a case-by-case basis.

NOTE: Approval from the U.S. Department of State Bureau of Diplomatic Security (DS), Office of Diplomatic Courier Services (DS/C/DC) must also be obtained before classified matter may be hand carried outside the U.S.

Under no circumstances may classified matter be transmitted physically across international boundaries except by U.S. Department of State (DOS) diplomatic professional couriers or specifically DOS authorized nonprofessional couriers. Nonprofessional diplomatic couriers (e.g., DOE courier) may be authorized by DOS for international transporting **only in emergencies, when the professional DOS courier service will not cover the area into which the diplomatic pouch must be carried or the post to which the pouch is addressed within the time that official business must be conducted.**

Nonprofessional couriers must be U.S. citizens and full-time direct hire U.S. government employees; have a Top Secret (or DOE “Q”) security clearance, a diplomatic passport, a diplomatic visa, and diplomatic credentials bearing the seal and signature of the current Secretary of State; and have an E-country clearance with the notation that the courier is authorized to perform nonprofessional courier functions. Additionally, the classified material must be enclosed in sealed diplomatic pouches obtained from DS/C/DC until delivered to its official destination.

Several other conditions must be met before DOS will authorize a nonprofessional courier to hand carry classified matter across international borders. Contact the HQ CMPC Program Manager for additional information.

Transmittal of Classified Matter to Congress:

Classified documents must be hand carried to the U.S. Congress, since Congress has no CMAs.

The Office of Congressional and Intergovernmental Affairs (CI), the NNSA Office of Congressional, Intergovernmental and Public Affairs (NA-3.5), and the Office of the Chief Financial Officer, Office of the Budget (CF-30), are solely responsible for the transmittal of classified matter to Congress. Consequently, any deviation from the requirements listed below must be approved by the CI Director (CI-1), NA-3.5, or CF-30. If a deviation from this policy is approved by CI-1, NA-3.5, or CF-30 and if staff members from some other organization are authorized to hand carry classified matter to Congress, then the HQ CMPC Program Manager must train the authorized individual(s) in their courier responsibilities before they can courier the material.

With one exception, only appropriately cleared and designated employees of CI, NA-3.5 and CF-30 are authorized to deliver classified matter to the Congress. When determining which HQ organization to contact to make arrangements for delivery of classified to Congress:

- CI-1 is the designated courier for DOE classified matter to Congress.
- CF-30 is the designated courier for ad hoc staff requests for classified matter addressed to the Senate Appropriations Committee or the House Appropriations Committee.
- NA-3.5 is the designated courier for NNSA classified matter to Congress.

The one exception to the listing above applies to specifically designated and cleared NNSA personnel who are authorized to courier only the *Annual Report to Congress on DOE/NNSA Special Access Programs*. National policy requires that this annual report must be delivered to Congress by the Government Program Manager and/or the Government Program Security Manager, or their authorized representative, in coordination with the Special Access Program Oversight Committee (SAPOC) Executive Secretary, as appropriate. The SAPOC Executive Secretary should notify CI of the impending delivery.

The HQ Courier Service is not to be used for couriating classified matter to Congress. However, the HQ Courier Service may be used to transmit the classified matter from an HQ organization to the CI, NNSA, or CF points of contact. As soon as an organization becomes aware that it has an upcoming requirement for classified to be couriered to Congress, it should make telephonic contact with one of the CI, NA-3.5, or CF-30 points of contact (see Points of Contact for Deliveries to Congress, below) to arrange for the delivery.

Packages for Congress must be properly wrapped and addressed through the appropriate DOE, NNSA, or CF point of contact to the name of the receiving member of Congress, Congressional Committee, or staff member. DOE F 470.10 (or equivalent) must be executed for *all* classified documents that are transmitted to Congress. Two copies of the receipt must be packaged within the transmitted envelope. A duplicate unclassified copy of the receipt should be made available for the courier to retain, and a fourth copy should be kept with the CDCS records.

NOTE: Documents intended for different members of Congress, different Congressional Committees, and/or different staff members must be individually packaged and wrapped and must contain separate receipts within each package. A separate DOE F 1410.6, DOE Messenger Receipt, must be used for each separate package.

Points of Contact for Deliveries to Congress:

- DOE:
Clarence K. Tong, Legislative Affairs Specialist, Office of Congressional and Intergovernmental Affairs, CI-01, (202-586-5470).

Kim Gibson, Office of Congressional and Intergovernmental Affairs, CI-1, (202-586-3600).

- NNSA:
Clarence Bishop, Director, Office of Congressional, Intergovernmental and Public Affairs, NA-3.5, (202-586-8343)

Jed D’Ercole, NNSA Director of Congressional Affairs, (202-586-3839)
- CF:
Julie G. Middleton, Office of the Chief Financial Officer, Office of the Budget, CF-30, (202-586-0673)

Transmittal of Classified Matter to Foreign Governments and the International Atomic Energy Agency (IAEA):

The disclosure, release, and transfer of classified information to a foreign government is complex and requires the coordination and approval of several HQ organizations. Contact the HQ CMPC Program Manager for guidance.

Points of Contact

For the names and contact information for those who occupy the positions identified in this section, call (301) 903-9986 or (301) 903-9990.

Forms/Samples/Graphics

Sample Briefing for Persons Authorized to Hand Carry Classified Documents (see Attachment 511-1)

Sample Hand Carry Contingency Plan (see Attachment 511-2)

Sample Letter of Authorization to Transportation Security Administration to Hand Carry Classified Material (see Attachment 511-3)

HQ Form 1410.5, *Classified Matter between Offices in DOE Headquarters* (“Candy Striped Envelope”), available from the Forrestal and Germantown central supply stores

HQ Form 1410.6, *DOE Messenger Receipt* (available from the Forrestal and Germantown Transportation Offices)

DOE Form 470.10, *Classified Matter Receipt* (for a copy of this form go to http://energy.gov/sites/prod/files/cioprod/documents/Form_470_10_fillable_X.pdf)

Other Reference

DOE Order 142.2A, *Voluntary Offer Safeguards Agreement and Additional Protocol with the International Atomic Energy Agency*

Helpful Websites

The HQ CMPC Program website is at: <http://www.hss.energy.gov/HQSecOp/cmhc.html>

To view the *DOE CMPC Marking Resource*, go to:
http://www.hss.energy.gov/SecPolicy/DOE_CMPC_Marking_Resource.pdf

ATTACHMENT 511-1

Sample Briefing for Persons Authorized to Hand Carry Classified Documents

HAND CARRY OF CLASSIFIED MATTER BRIEFING FOR OFFICE OF _____ PERSONNEL

The following discussion is intended to assist you in discharging your security responsibilities when hand carrying classified matter.

Hand carrying of classified matter places significant security responsibilities upon you. You can avoid this situation by considering alternative means for transmitting the classified matter. These alternatives include sending the matter via courier, express mail, certified mail, or secure facsimile. Your servicing Classified Document Control Station (CDCS) Operators can assist you in transmitting the matter by these means. Hand carrying classified matter is authorized only when operationally necessary, not for convenience.

Hand carrying classified matter usually involves one of two types of situations:

- The person hand carrying the classified matter is merely a courier delivering the documents to a new custodian, where a transfer of custody is contemplated.
- The classified matter is to remain chargeable to the hand carrier during the period of removal from the office, and thereafter is to be returned to the hand carrier's office files.

The removal of classified matter from your office must be coordinated through your Headquarters Security Officer (HSO) and/or servicing CDCS. Appropriate documents need to be generated on the classified matter you are hand carrying. It will take some time to generate these documents and instruct you in how to use them, so do not expect to have these requirements completed within a few minutes. You must also return to your CDCS when you have completed hand carrying the classified matter in order to reconcile your delivery records.

If you are hand carrying only between the Forrestal and Germantown Buildings, your standard DOE security badge will be accepted as proof that you are authorized to hand carry classified matter. You should inform your HSO of your intention to hand carry between the two buildings and you **must** process through your CDCS to prepare the documents, package, and required labels. As stated above, you must also return to your CDCS when you have completed hand carrying the classified matter in order to reconcile your delivery records.

If classified matter is to be hand carried outside the Washington, D.C., metropolitan area, specific authorization from your HSO is required. You will need to furnish information about your travel plans and airline flights in order to generate the documents you will need to protect the classified matter and still meet airport screening requirements. Again, these documents will take time to produce.

You can expect to be challenged by DOE field personnel and security officials at other government agencies about whether or not you are authorized to hand carry classified matter. The Office of _____ has developed a special authorization card to help verify that you are authorized to hand carry classified matter. To date, the hand carry authorization card, when used in conjunction with your standard DOE badge, has been accepted as proof of your hand carry authority, but there is no guarantee that it will always be accepted.

You will be given a Contingency Plan describing your responsibilities if there are travel difficulties, weather conditions, or other unforeseen circumstances that will significantly delay delivery of the classified matter. Review the Contingency Plan and keep it handy so you can find and comply with it when you really need it.

Your overall **responsibility** is to take all steps possible to ensure that the classified matter is not lost or otherwise compromised. You need to know that:

- Persons hand carrying classified matter must possess an access authorization commensurate with the level of information being hand carried and must be aware of their responsibility to continuously safeguard classified information.
- You must retain the classified matter in your personal possession AT ALL TIMES or store it – appropriately wrapped and sealed and subject to removal only by you or an appropriately cleared individual – in a DOE-approved repository.
- Taking classified documents to private residences is prohibited.
- Storing classified matter in hotel/motel rooms or safes, vehicles or their compartments, public lockers, or any other unapproved repository is prohibited.
- You may not make unnecessary convenience stops while transporting classified matter.
- All classified matter to be hand carried must be appropriately marked and wrapped.

If you lose or misplace any classified matter, or if it is compromised or possibly compromised, you must report the situation immediately to your HSO. If the incident occurs during non-working hours, you must notify, as soon as practical, the DOE Emergency Operations Center. The phone numbers for making these reports are on the HSS hand carry authorization card and in the Contingency Plan you will be given. If the incident occurs while you are attending classified meetings at other DOE or government facilities, you should also inform that facility's security officer or the security officer responsible for the meeting.

I acknowledge that I have read this briefing and understand my responsibilities for hand carrying classified matter:

_____	_____	_____
Printed Name	Signature	Date

ATTACHMENT 511-2

Sample Hand Carry Contingency Plan

Anyone hand carrying classified matter must be made aware of their organization's contingency plan for handling unexpected delays in the delivery of that matter. This is the contingency plan for personnel assigned to the Office of _____. This plan is not intended to cover all the circumstances that might occur; instead, it is a guide to help the individual cope with common delays such as traffic conditions, weather emergencies, and unexpected facility closings.

This contingency plan must be explained to and a copy provided to Office of _____ personnel each time they hand carry classified matter.

Contingency Plan for Hand Carrying in the Washington, D.C. Metropolitan Area:

1. The DOE standard badge is the only document required to verify that the person is authorized to hand carry classified matter between DOE facilities in the Washington, D.C. area.
2. If, however, classified matter is to be delivered to or removed from non-DOE Headquarters facilities in the Washington DC area, there may be a need for a special hand carry authorization. Hand carry authorization cards are available from the Office of _____ Headquarters Security Officer (HSO).
3. All classified matter must be double-wrapped in the manner prescribed by DOE directives. The double-wrapping can be performed by the individual's Classified Document Control Station.
4. Classified Document Receipts or a Hand Carry Manifest identifying *all classified matter regardless of its classification level and category* must be included in the package being hand carried. Classified Document Receipts or the Hand Carry Manifest can be prepared by the Office's Classified Document Control Station. Station Operators will provide the required number of receipts or the manifest and provide instructions in how to use and return them.
5. If there will be an unusual delay in delivering classified matter, the person hand carrying the matter must contact his/her HSO and inform him/her of the situation. The Office of _____ HSO may be reached at _____ during regular hours. After regular hours, or if the HSO is unavailable, the Emergency Operations Center can be contacted 24 hours per day at _____.
6. If the classified matter cannot be delivered promptly to the intended recipient, it must remain in the personal possession of the person hand carrying it. It *may not* be stored in the trunk of a car, a home, a hotel/motel room, a hotel/motel safe, a locker, or anything outside the personal control/possession of the person hand carrying it. *By deciding to*

hand carry the classified matter, the individual accepts full responsibility for ensuring the security of that matter. Responsibility cannot be transferred to any other person or organization without the approval of the HSO.

7. If the classified matter cannot be delivered until after normal business hours, it may be taken to a DOE Protective Force Central Alarm Station (CAS) for safe storage. The CASs at the Forrestal and Germantown Buildings are the 24-hour classified matter receiving points for DOE facilities in the Washington, D.C. metropolitan area. The Forrestal CAS is in Room 1G-024 and the Germantown CAS is in Room A-060. The CAS will provide a hand receipt for the matter received. Do not lose this receipt because the CAS will demand return of the receipt before releasing it back to the person who delivered it.

8. If the classified matter cannot be retained by the person hand carrying it and it cannot be secured in an approved manner, the person should discuss the situation with the HSO for alternate instructions.

9. If hand carried classified matter is lost, stolen, misplaced, or otherwise cannot be accounted for, the HSO or the DOE Emergency Operations Center must be notified *immediately*.

Contingency Plan for Hand Carrying Outside the Washington, D.C. Metropolitan Area:

1. Any employee who anticipates the need to hand carry classified matter outside the Washington, D.C. area should have a special hand carry authorization card. Hand carry authorization cards are available from the HSO.

2. The person hand carrying the matter must ensure that the intended destination is approved to handle and store classified matter at the level and category being delivered. This check can be performed by Office of _____ Classified Document Control Station Operators.

3. All classified matter must be double-wrapped in the manner prescribed by DOE directives. The double-wrapping can be performed by the Office of _____ Classified Document Control Station.

4. Classified Document Receipts or a Hand Carry Manifest identifying *all classified matter regardless of its classification level and category* must be included in the package being hand carried. Classified Document Receipts or the Hand Carry Manifest can be prepared by the Office of _____ Classified Document Control Station. Station Operators will provide the required number of receipts or the manifest and provide instructions in how to use and return them.

5. If there will be an unusual delay in delivering classified matter, such as adverse weather conditions, lengthy airport/airline delays, or other emergencies, the person hand carrying the matter must contact his/her HSO and inform him/her of the situation. The

HSO may be reached at _____ during regular hours. After regular hours, or if the HSO is unavailable, the Emergency Operations Center can also be contacted 24 hours per day at _____. These numbers are also printed on the hand carry authorization card.

6. If the classified matter cannot be delivered promptly to the intended recipient, it must remain in the personal possession of the person hand carrying it until it is placed into secure storage. Secure storage is not the trunk of a car, a hotel/motel room, a hotel/motel safe, a locker, or anything other than the personal control/possession of the person hand carrying it or a repository approved for storage of the matter being carried. *By deciding to hand carry the classified matter, the individual accepts full responsibility for ensuring the security of that matter. Responsibility cannot be transferred to any other person or organization without the approval of the HSO.*

7. If the situation is such that the individual cannot properly protect the classified matter, the HSO can assist. Please contact the HSO at the number listed above. The HSO can request a search of the Safeguards and Security Information Management System (SSIMS) to determine whether any of the following secure facilities may be available to the traveler:

- a. A local DOE site approved for storing classified matter at the level and category being hand carried.
- b. A local DOE contractor facility approved for storing classified matter at the level and category being hand carried.
- c. A local U.S. military installation with the capability to store classified matter at the level and category being hand carried.
- d. A local FBI office with the capability to store classified matter at the level and category being hand carried.
- e. If none of these options are available, the traveler may be instructed to take the classified matter to a United States Post Office during business hours and mail the matter either to him/herself at DOE, to his/her HSO, or to the recipient via Registered Mail, as appropriate, using the DOE classified mailing addresses listed below (or the recipient's classified mailing address):

Germantown Office

ATTN: (Organization) (Intended Recipient)
U.S. Department of Energy
P.O. Box A
Germantown, MD 20875-0963

Forrestal Office

ATTN: (Organization) (Intended recipient)
U.S. Department of Energy
P.O. Box 23865
Washington, D.C. 20026-3865

If the classified matter is turned over to one of the above entities, the package must be closely inspected for signs of tampering or unauthorized opening once it is back in the custody of the person responsible for it. If such signs are evident, the situation must be reported immediately to the HSO.

8. If hand carried classified matter is lost, stolen, misplaced, or otherwise cannot be accounted for, the HSO or the Emergency Operations Center must be notified *immediately*.

9. In emergency circumstances (such as natural disaster, terrorist attack, city evacuation, or any circumstances where appropriate storage or delivery as described above is absolutely not possible), common sense must apply in protecting the classified matter. In any situation or circumstance, you must personally protect the classified matter until it is appropriately secured at the earliest possible opportunity. In such emergencies, keep your HSO informed, and in all cases, you will be required to provide a report of the incident to your HSO as soon as you return to DOE HQ.

ATTACHMENT 511-3

**Sample Letter of Authorization to Transportation Security Administration to Hand Carry
Classified Material (Letterhead Stationery)**

Date:

ADDRESSEE: TRANSPORTATION SECURITY ADMINISTRATION

SUBJECT: Letter of Authorization to Hand Carry Classified Material

This is to certify that the individual indicated below, who is an employee of the Office of _____, United States Department of Energy, is hereby authorized to hand carry classified matter related to National Security aboard a commercial aircraft.

Courier: Full Name

Agency ID: US Department of Energy

Dates of Issue and Expiration of Assignment: (dates of start and expiration of
assignment)

Official Issuing

Authorization Letter: Full Name

Signature

Telephone Number

To Confirm

Authorization Contact: Full Name

Signature

Telephone Number

Sincerely,

Issuing Official Name

Issuing Officer Title

Section 512

Classified Mailing Addresses

Classified matter must be addressed only to approved CMAs (i.e., mailing, shipping, or overnight express delivery) contingent upon the appropriate method of transmission. The CDCS operator must consult SSIMS to verify the CMA and the authorized storage capability of the receiver before dispatching the matter.

This section describes DOE HQ procedures for obtaining various CMAs.

HQ Implementation Procedures

It is recommended that each element have at least one CDCS operator designated to access SSIMS to acquire CMAs and to verify the approved classified storage capability of the receiving facility. This information is contained on DOE F 470.2, *Facility Data and Approval Record* (FDAR), which is stored in SSIMS. The form lists the receiving facility's Facility Clearance (Block 16); the authorized classified storage capability; classification level and category (Block 18); and the authorized CMAs for the method(s) of transmission that are authorized for the specific facility (Blocks 13, 17, and 20). CMAs verified through SSIMS are valid for 30 days from the date of validation. If no one in the HQ element has access to SSIMS, contact the Office of Information Security (HS-92). See the Points of Contact subsection below for information on contacting HS-92.

NOTE 1: SSIMS is an automated classified database that must be accessed through an information system approved and accredited to process classified information. Individuals requiring access to SSIMS should initially contact their ISSO, who will assist in locating an accredited system or provide assistance in accrediting a system to process classified data.

NOTE 2: To acquire SSIMS browser access and training, contact the SSIMS Administrator, Office of Security Assistance (HS-52). See the Points of Contact subsection below for information on contacting HS-52.

CMAs for HQ Elements:

CMAs for HQ elements are available in SSIMS. Each HQ element is registered in SSIMS as either a non-possessing or possessing facility. The FDAR for each HQ element reflects whether the element is authorized to receive classified matter at the Forrestal building, the Germantown building, or both locations. The FDAR also indicates the classification and category level of the HQ element's storage capability.

CMAs for Other DOE Federal Facilities:

CMAAs for all non-HQ DOE facilities must also be verified in SSIMS. If the facility is able to receive classified matter, the FDAR reflects the classification and category level of storage capability and the CMA.

Contractor Facilities:

Companies that have contractual arrangements that require storage of classified matter in their contractor offices are registered in SSIMS as possessing facilities. The FDARs for possessing contractor facilities reflect the CMA and storage capabilities, as well as classified shipping and overnight addresses where appropriate.

Other Government Agencies:

CMAAs for OGAs must be verified in SSIMS. The FDARs for OGA facilities reflect the CMA information, classified shipping and overnight addresses (if appropriate), and the level of classification and category of matter the OGA is authorized to store.

OGA Contractors:

CMAAs for OGA contractors must be verified in SSIMS. The FDARs for OGA contractor facilities reflect the CMA information, classified shipping and overnight addresses (if appropriate), and the level of classification and category of matter the OGA is authorized to store.

Points of Contact

For information about the HQ CMPC Program, call (301) 903-9986.

To contact the Office of Security Assistance (HS-52) to obtain access to SSIMS, call (301) 903-5108 or (301) 903-1163.

To contact the Office of Information Security (HS-92), call (301) 903-9990.

Forms/Samples/Graphics

DOE F 470.2, *Facility Data and Approval Record* (for a copy of this form go to <http://energy.gov/sites/prod/files/cioprod/documents/470-2%281%29.pdf>)

Helpful Website

The HQ CMPC Program website is at: <http://www.hss.energy.gov/HQSecOp/cmpec.html>

Section 513

Express Mail Service

Classified matter is sometimes transmitted through express mail; however, express mail packages cannot be marked as containing classified matter. Thus, there is a possibility that the recipient of an express mail package will not be aware that it contains classified matter and may not open it promptly or store it properly. To ensure that all express mail packages are opened promptly, that the contents are inspected, and that action is taken to properly store classified matter, it is DOE HQ policy for Express Mail Center personnel to release all express mail packages directly to the person to whom it is addressed (addressee) or to an Express Mail Document Control (EMDC) designee. If the addressee is not available, the express mail package must be released to another person who has been specifically appointed by the HQ element to receive and open such packages. Such individuals who are authorized to receive and open express mail on behalf of others within their organizations are known as EMDC designees.

NOTE: TS matter may not be transmitted via express mail.

NOTE: Commercial express mail service shall not be used as a matter of routine or convenience for transmitting classified matter. However, when such express service is deemed operationally necessary, CDCS personnel must follow their organization's procedures for transmitting a classified express mail package.

HQ Implementation Procedures

Appointment of Express Mail Document Control Designees:

Each HQ element must designate EMDC personnel before they can pick up express mail packages from the HQ Express Mail Offices on behalf of personnel within their organizations. The element's HSO must submit a list of the organization's EMDC designees to HS-92 via e-mail. HSOs should use the *Sample E-Mail Notification for Express Mail Document Control Designees* (Attachment 513-1) to inform HS-92 of the element's EMDC designees. When there are changes in an element's list of EMDC designees, the HSO must immediately notify HS-92 of the changes by e-mail, using this same e-mail format.

NOTE: The Forrestal and Germantown Express Mail Offices are not authorized to release an express mail package to anyone other than the addressee, or an individual on the element's list of EMDC designees.

HQ elements are registered in SSIMS as either a possessor or non-possessor of classified matter:

1. Possessing Elements are HQ elements that can receive and store classified matter at the Forrestal, 955 L'Enfant, or Germantown facilities. EMDC designees from a Possessing Element must have a Q or L security clearance. CDCS personnel (see Section 510, Classified Document Control Stations) may also serve as EMDC designees.

2. Non-Possessing Elements are HQ elements that are not approved to receive or store classified matter at any of the HQ facilities. EMDC designees from a Non-Possessing Element are not required to possess either a Q or L security clearance.

Incoming Express Mail Packages to Possessing HQ Elements:

On the day the express mail package is received at HQ, the Express Mail Office at Forrestal or Germantown notifies the addressee via e-mail.

NOTE: This notification is an Express Mail Office practice that does not relate to security requirements.

Unless specifically prohibited by an organization (e.g., NA, HS, and SC), only the addressee or the cleared EMDC designees are authorized to retrieve packages from the Express Mail Office. Whoever retrieves the package is responsible for taking possession of the package, opening it, and inspecting it to determine whether it contains classified matter. If the package contains classified matter, it must be taken immediately to the element's CDCS for proper processing and/or storage. In any event, express packages must not be left unopened in an individual's inbox, on a desk, or in any other area awaiting attention by the intended recipient or some other person.

If the addressee or EMDC designee is unavailable or does not pick up the package by early afternoon of the following day, the Express Mail Office contacts the HSO for the recipient's organization and requests that arrangements be made for the package to be retrieved by a cleared EMDC designee or the addressee. On the morning of the third day, if the package has not been picked up by EMDC personnel or the addressee, the Express Mail Office notifies HS-92, which will decide what action to take on the undelivered package.

Outgoing Express Mail Packages from Possessing HQ Elements:

If an outgoing express package contains classified matter, it must be handled by the element's CDCS personnel. If the outgoing express package contains only unclassified matter, anyone can deliver the package to the servicing express mail office.

Incoming Express Mail to Non-Possessing HQ Elements:

On the day the express mail package is received at HQ, the servicing Express Mail Office at Forrestal or Germantown notifies the addressee. The addressee or EMDC designee is responsible for reporting to the Express Mail Office, taking possession of the package, and inspecting it to determine whether it contains classified matter. If it does, the HSO of the element must be notified, take possession of the classified matter, and seek guidance from HS-92.

If the package has not been picked up by early afternoon of the following day, the Express Mail Office contacts the designated HSO for the recipient's organization. On the morning of the third

day, if the package has not been picked up, the Express Mail Office notifies HS-92, which will decide what action to take regarding the package.

Outgoing Express Mail from Non-Possessing HQ Elements:

Anyone can deliver an unclassified outgoing express package to the local Express Mail Office in accordance with the local element's procedures.

In the uncommon event that a non-possessing element must transmit classified matter via express mail, an appropriately cleared person (e.g., the HSO) must coordinate with the CDCS of a possessing element to effect this transmission.

EMDC Designee or Addressee Responsibilities:

EMDC designees or addressees must immediately pick up express mail packages when contacted by the Forrestal or Germantown Express Mail Office. Upon return to their respective office or designated security area, the EMDCs must immediately open the package and ensure that it does not contain classified matter.

To determine whether the package contains classified matter, first open the outer express package wrapping. If the material inside is not further wrapped and contains no classification markings, the material may be handled as unclassified. If classification markings are present, handle the package as classified matter as described below.

If the material inside contains an additional wrapping that is not marked with classification markings, open the inner wrapping. If there are no classification markings on the inner wrap, handle as unclassified. If classification markings are present, handle the package as classified matter as described below.

Packages with classification markings may only be opened by cleared personnel within designated approved security areas. If the addressee or EMDC designee does not meet these requirements, he/she must not open the package any further and must immediately contact the organization's HSO or CDCS personnel for additional guidance.

NOTE: If the individual cannot locate CDCS personnel, a cleared HSO, Alternate HSO, or HSO Representative, he or she must immediately contact HS-92 for assistance.

Point of Contact

For information about the HQ CMPC Program, call (301) 903-9990.

Forms/Samples/Graphics

Sample E-Mail Notification for Express Mail Document Control Designees (see Attachment 513-1)

Helpful Website

The HQ CMPC Program website is at: <http://www.hss.energy.gov/HQSecOp/cmpc.html>

ATTACHMENT 513-1

Sample E-Mail Notification for Express Mail Document Control Designees

Send the e-mail to: "HS-92 Operations"

The e-mail "Subject" block should be: "Notification of Express Mail Document Control Designees"

The body of e-mail should include the following information:

"The Office of _____ has approved the following personnel to receive and open express mail packages addressed to this office:

Name of Designee:

Security Clearance Level:

Organization code and/or organizational name:

Building name:

Room number/location of Classified Document Control Station:

Telephone number:

Repeat the above information, as necessary, to identify all designees.

If the person is to be added to an existing list of designees, clearly include the word "ADD" behind the person's name.

If a person is to be deleted, an e-mail notification is also required. Indicate in the body of the e-mail that the person is no longer approved to receive and open classified mail and include the word "DELETE" behind the person's name.

E-mails will be accepted only from the element HSO, Alternate HSO, or HSO Representative.

This page intentionally left blank.

Section 514

Destruction of Classified Matter

This section describes how to properly destroy classified matter at DOE HQ.

HQ Implementation Procedures

HQ elements and support contractors should establish procedures for an ongoing review of their classified holdings to reduce their classified inventory to the minimum necessary. Multiple copies, obsolete matter, and other classified waste should be destroyed as soon as practical. Records disposition schedules, including the NARA General Records Schedule, and DOE records schedules must be taken into consideration before documents or other classified matter can be designated for destruction. If classified matter is under a court order prohibiting its destruction, guidance must be requested from the DOE Office of General Counsel.

Approved Methods of Destruction:

Classified matter must be destroyed beyond recognition to preclude reconstruction. The approved methods of destruction at HQ are:

1. Shredders – Crosscut shredders are approved for the destruction of all classified **paper documents**. The shredder must reduce the paper to a particulate size not greater than **1mm x 5mm** during the destruction process. The user should inspect the particulate output each time to ensure that the particulate size is no larger than 1mm x 5mm. Additionally, approximately every 6 months, HSOs are asked to check the particulate output of the shredders used by their elements to destroy classified matter. If the size requirement is not met, that particular shredder is taken out of operation until it can be repaired or replaced. Shredder residue meeting particulate requirements may be disposed of as normal unclassified (recyclable) waste.

Crosscut shredders purchased prior to December 31, 2003, that produce residue with a particle size not exceeding 1/32" x 1/2" may continue to be used for the destruction of classified paper matter. If these shredders cannot be repaired or restored to cut residue within 1/32" x 1/2", they must be taken out of service.

Crosscut shredders that produce a particulate size that meets the above requirement may be approved by the elemental HSO. Shredders approved by HSOs for classified destruction must be located in LAs or VTRs and must be designated by conspicuously posted signs. Shredders **approved** for classified destruction must have the sign posted either on the equipment or nearby. The sign must contain the make and model of the shredder and be signed and dated by the appropriate HSO. A sample of the sign is provided in Attachment 514-1. All shredders located in an LA or VTR that are **not approved** for destruction of classified matter must have a *Not*

Authorized for Classified Destruction sign posted on the shredder (provided in Attachment 514-2).

2. HQ Centralized Classified Destruction Facility (CCDF) – The CCDF is located at the Germantown, MD facility. It is used to destroy bulk amounts of classified or Controlled Unclassified Information paper documents and non-paper matter, such as audio and video tapes, viewgraphs, film, floppy disks, removable hard drives, and communication devices (e.g., Blackberry-type devices).
3. Other Methods – On rare occasions, the CCDF may be unavailable for destruction operations (while undergoing maintenance or for other reasons). When the CCDF is not operating, the Director, HS-90, in consultation with the OCIO, may identify and approve alternative means of bulk classified destruction.

Destruction of Non-Accountable Classified Matter:

The destruction of non-accountable classified matter may be accomplished by one individual. No witness is required, and no record of destruction is required. The person doing the destruction must have a security clearance equal to or higher than the classification level, and category, and any other caveats, as applicable, of the waste material.

Preparation of Non-Accountable Classified Matter for Destruction:

Classified matter that cannot be destroyed on approved crosscut shredders located within HQ offices must be properly packaged and transported to the CCDF. The following guidelines should be followed for the destruction of **non-accountable classified matter**:

- Paper, plastics (including floppy disks), and metal (including metallic computer disks and removable hard drives) must be sorted into separate, properly annotated classified burn bags not to exceed 10 pounds in weight in Forrestal and 15 pounds in Germantown. Personally-owned, non-official effects are not to be included in waste matter. Failure to comply with destruction preparation procedures may result in the issuance of a security infraction.

NOTE: Paper clips, heavy duty staples, and metal or plastic fasteners must be removed from all paper documents and waste. Bags containing fasteners of any kind will be returned to the originator.

- Classified burn bags are available in the DOE self-service supply rooms. They are recognizable by the red and white stripes on their outside surface. These bags are designated **only** for classified waste. The name, routing symbol, telephone number, and room number of the person responsible for the burn bag, and the type of matter contained within, must be clearly marked on the side of each bag for identification. The weight of the matter within each burn bag is limited to 10 pounds for those generated at the Forrestal Facility and 15 pounds for those generated at the

Germantown Facility. The bags should be folded at least once and stapled shut every 2 inches. Burn bags are to be protected as classified matter until they are destroyed.

- Burn bags may be delivered to the following collection points during the times listed:
 - o Forrestal Building – Room GI-007 between 3:00 p.m. and 4:00 p.m., Mondays, Wednesdays and Fridays. No appointment is necessary.
 - o Germantown Building – Room R-002 between 9:30 a.m. and 10:30 a.m., Mondays, Wednesdays and Fridays.

Destruction of Accountable Classified Matter:

The destruction of accountable classified matter must be witnessed by an appropriately cleared individual other than the person destroying the matter. Both the destruction official and the witness must have a security clearance equal to or higher than the classification level and category of the classified information to be destroyed. Facilities in which only one employee has the appropriate clearance must contact the HSO or HS- 92 for guidance on destruction.

A DOE F 5635.9, *Record of Destruction*, or equivalent, must be completed whenever accountable classified matter is destroyed. An operator within the element's CDCS must authorize the destruction and maintain all DOE F 5635.9s or other destruction records/receipts. Destruction certificates for accountable matter should be retained for 5 years for Top Secret and 2 years for Secret and Confidential.

Accountable matter may be destroyed with an HSO-approved crosscut shredder or at the CCDF. An appointment must be made by calling the CCDF operator at the phone number included in the Points of Contact subsection below. The CCDF operator will not sign the DOE F 5635.9 as the destruction official and cannot serve as the witness to the destruction. The HQ element destroying the accountable matter must provide both the destruction official and a witness to the destruction.

See Section 509 for examples of accountable classified matter.

Points of Contact

For information about the HQ CMPC Program, call (301) 903- 9990.

To contact the Forrestal Collection Facility, call (202) 586-8600.

To contact the Germantown Collection Facility, call (301) 903-3910.

To make an appointment at the Germantown Central Destruction Facility, call (301) 903-2035.

Forms/Samples/Graphics

Sample Authorized for Classified Destruction Sign (see Attachment 514-1)

Sample Not Authorized for Classified Destruction Sign (see Attachment 514-2)

DOE Form 5635.9, *Record of Destruction* (for a copy of this form go to <http://energy.gov/sites/prod/files/cioprod/documents/5635-9.pdf>)

Helpful Website

The HQ CMPC Program website is at: <http://www.hss.energy.gov/HQSecOp/cmhc.html>

ATTACHMENT 514-1

Sample Authorized for Classified Destruction Sign

This Shredder		
AUTHORIZED for the DESTRUCTION OF		
CLASSIFIED MATTER		
Subject to the restrictions contained in the Headquarters Facilities Master Security Plan		
Room _____	Date _____	
Element _____	HSO _____	
	Phone _____	
Shredder Information _____	Make _____	Model _____
		Property Number _____
REF #: HS-1.31-2006-11		

ATTACHMENT 514-2

Sample Not Authorized for Classified Destruction Sign



Chapter 6 Revision History:

Date	Description
1/28/15	Pg. 602-5, Line 24, updated paragraph
10/16/18	Pg. 6-1, removed reference to DOE Order 142.3A, <i>Unclassified Foreign Visits and Assignments Program</i> . This order has been archived and superseded by DOE O. 470.4B
10/16/18	Pg. 602-1, removed reference to DOE Order 142.3A, <i>Unclassified Foreign Visits and Assignments Program</i> . This order has been archived and superseded by DOE O. 470.4B – reference to DOE Order 142.3A replaced with DOE O. 470.4B
10/16/18	Pg. 601.3, updated point of contact phone number
10/29/19	Pg. 6-1, added reference DOE Order 142.3A, <i>Unclassified Foreign Visits and Assignments Program</i> .
10/29/19	Pg. 602-1, added reference DOE Order 142.3A, <i>Unclassified Foreign Visits and Assignments Program</i> .
10/29/19	Pg. 602-2, “Exemptions” Added: See DOE O. 142.3A Ch. 1
10/29/19	Pg. 602-9, “Procedures” Added: Indices Checks
10/29/19	Pg. 602-43 “Attachment 602-12” Changed to: Intelligence and Counterintelligence (IN-20) for final review and approval.
11/15/19	Pg. 601-2 Added “Foreign National visitors and assignees will not be processed for HSPD-12 credentials. Visits and assignments will be processed in line with the requirements of DOE O 142.3A Chg. 1. Upon approval of all required documentation all foreign national visitors and assignees will be issued a Local Site-Specific Only (LSSO) badge”.
11/15/19	Pg.602-2 Added, “Foreign National visitors and assignees will not be processed for HSPD-12 credentials. Visits and assignments will be processed in line with the requirements of DOE O 142.3A Chg. 1. Upon approval of all required documentation all foreign national visitors and assignees will be issued a Local Site-Specific Only (LSSO) badge”.

Chapter 6

Foreign Interaction

This chapter describes the security procedures adopted by DOE HQ to implement the requirements of the following Executive Order and DOE directives:

- Executive Order 12344 (as prescribed by 42 U.S.C. 7158)
- DOE Order 470.4B, *Safeguards and Security Program*, Appendix B, Section 4
- DOE Order 475.1, *Counterintelligence Program*
- DOE Order 551.1C, *Official Foreign Travel*
- DOE Manual 552.1-1A, *U.S. Department of Energy Travel Manual*
- DOE Order 552.1A, Change 1, *Travel Policy and Procedures*
- DOE Order 142.3A, *Unclassified Foreign Visits and Assignments Program*.

The directives have two objectives: the first objective is to protect DOE sensitive and classified information from being disclosed to foreign nationals, except when authorized by international treaties and agreements; the second is to ensure that DOE employees and contractors performing official travel have the appropriate travel documentation and approvals from the country they will visit.

- Section 601 covers the procedures for intentionally sharing classified information with foreign nationals in accordance with U.S. treaties and international agreements.
- Section 602 covers the procedures for hosting foreign national visitors and assignees at DOE HQ for unclassified purposes, including meetings, conferences, and events sponsored by HQ elements.
- Section 603 covers the procedures for performing foreign travel, both official and unofficial, and when the traveler must notify IN-20 of his/her plans. These procedures apply to current and some former DOE employees.

This page intentionally left blank.

Section 601

Foreign National Classified Visits

DOE provides technical and policy leadership to the U.S. government and international community to achieve nonproliferation objectives and to share scientific and technical information. To achieve these objectives, there will be times when foreign visitors who have security clearances will require access to US classified information. The procedures described in this section are intended to assist HQ elements in complying with DOE directives related to the sharing of classified information in accordance with U.S. treaties and international agreements.

HQ Implementation Procedures

This subsection describes the procedures and approvals needed to provide authorized foreign nationals access to U.S. classified information and serves as the implementation plan for all HQ elements.

- The Head of Element (or their officially appointed delegate) must approve classified foreign visits to HQ facilities. The delegate must be a Federal employee, a U.S. citizen, and have a security clearance appropriate for the classification level of the visit. The delegation must be made in writing and copies of the delegation must be provided to the Office of Security Assistance (AU-52) and the HQ Foreign Visits and Assignments (FV&A) Team within AU-41.

NOTE: The term "Approval Authority" is used throughout this section and means the Head of Element or his/her designee. The Head of Element remains responsible for all activities that occur during the visit/assignment, regardless of who signed the approval.

- The Approval Authority for each HQ element must understand what DOE classified information within his/her purview may be shared with foreign nationals in accordance with international agreements or treaties.
- When it becomes necessary to share classified information with a foreign national, the Approval Authority must appoint, in writing or verbally, a member of the element's staff to act as host for the foreign visitor.
- The host ensures the visitor's clearance is commensurate with the classification level of the information being accessed and that the visitor has a "need-to-know." The host may need to obtain a written Security Assurance from the foreign visitor's home government verifying that the visitor has the requisite security clearance (see Special Access Permissions subsection, below).
- The host arranges an appropriate meeting space in a LA (VTRs are unacceptable) within DOE HQ. The classified information may not be provided to the visitor outside an LA.

- No classified information outside the scope of the treaty or international agreement may be provided or discussed.
- Prior to the visit, the host prepares a Memorandum for Record (see Attachment 601-1). The memorandum includes information about the visitor, the name of the treaty or international agreement that the visit will be conducted under, the purpose and location of the visit, and other pertinent data. Once the visit is completed, the Memorandum for Record must be updated to include required confirmation or “closeout” information.
- After the Memorandum for Record is prepared, the host attaches it to a cover memorandum requesting the Approval Authority to approve the classified visit (see Attachment 601-1).
- Once the classified visit is approved, but before the arrival of the foreign visitor, a copy of the approval memorandum is provided to the HQ FV&A Team. The HQ FV&A Team, in turn, ensures a copy of the approval memorandum is provided to the HQ facility reception desk to permit entry of the foreign visitor. If a copy of the approval memorandum is not provided to the HQ FV&A Team prior to the visit, it is almost certain that the foreign visitor will not be admitted.
- The HQ element sponsoring the visit assigns a Q or L-cleared escort who is a U.S. citizen to meet the foreign national at the HQ facility reception desk. Foreign visitors are badged as uncleared visitors and must be escorted for the duration of the visit.
- Foreign National visitors and assignees will not be processed for HSPD-12 credentials. Visits and assignments will be processed in line with the requirements of DOE O 142.3A Chg 1. Upon approval of all required documentation all foreign national visitors and assignees will be issued a Local Site-Specific Only (LSSO) badge.
- Escorts must complete an escort briefing prior to being assigned escort responsibilities. The element HSO conducts the original briefing and verifies completion by entering it in the "CMPC Training Records" section of his/her Appendix to HQFMSP.
- **No information about visits is to be entered into the FACTS database and no additional coordination is required.**
- All documentation supporting the classified visit must be retained for 5 years in accordance with the DOE Records Inventory and Disposition Schedule (RIDS). AU-52 reserves the right to request copies of visit/assignment requests, approvals, and supporting documentation. AU-52 may request additional information regarding the classified visit; these inquiries must be answered according to AU-52’s specified timeframe.

Special Access Permissions:

- When the foreign visitor holds a security clearance from a U.S. government agency other than DOE, a DOE F 5631.20, "U.S. Department of Energy Request for Visit or Access Approval," must be submitted to DOE. These procedures are discussed in Section 306, Passing Clearances for Classified Meetings and Visits, of the HQFMSP.
- When the foreign visitor requires access to Sigma information, (i.e., subsets of nuclear weapons information classified under the Atomic Energy Act and grouped by subject matter) a DOE F 5631.20 for that visitor must be prepared and submitted (see Section 306, Passing Clearances for Classified Meetings and Visits, for procedures on submitting a DOE F 5631.20).
- When the visitor is without a U.S. government clearance, he/she must present a Security Assurance certificate from his/her government to the person hosting the visit. Security Assurance certificates are issued based upon the procedures described in the pertinent treaty or international agreement; therefore, DOE has no standard procedure for requesting or obtaining Security Assurance certificates. The host for the classified visit must work with the U.S. State Department and/or the foreign embassy to obtain the Security Assurance certificate. Security Assurance certificates must remain on file within the hosting HQ element for 5 years.

Points of Contact

For the names and contact information for those occupying the positions identified in this chapter, call (202) 202-586-8075.

HQ Foreign Visits and Assignments Team: e-mail to "HQ FV&A team@hq.doe.gov"

Forms/Samples/Graphics

Sample Memorandum to Request Approval of Classified Visit and Sample Memorandum for Record (see Attachment 601-1)

ATTACHMENT 601-1

Sample Memorandum to Request Approval of Classified Visit and Sample Memorandum for Record

MEMORANDUM FOR (NAME AND TITLE OF ELEMENT'S APPROVAL AUTHORITY)

FROM: (NAME AND TITLE OF HOST)

SUBJECT: Request for Approval of Classified Foreign Visit

DOE Order 142.1, CLASSIFIED VISITS INVOLVING FOREIGN NATIONALS, requires approval be obtained prior to the visit of a cleared foreign national who will be given access to classified matter. This memorandum is to request your approval of a DOE-sponsored visit to be attended by the foreign national(s) identified on the attached Memorandum for Record.

The following information is submitted:

1. Purpose of Visit: (As appropriate.)
2. Facility to be Visited: (Name of Building or Facility Only. ***Do not*** include room number.)
3. Estimated Start/Estimated End Date of Visit: (As required.)
4. Badging: The host will meet the visitor(s) at the reception desk and ensure the visitor receives the appropriate badge. The visitor(s) will be under escort at all times.
5. Memorandum for Record: A Memorandum for Record containing specific information about the visit and visitor(s) has been completed with currently available information and is attached. When the visit is complete, the Memorandum for Record will be updated with all remaining required information and retained by the hosting office.
6. Name and Telephone Number of Host: (As appropriate.)

It is recommended that this visit be approved.

Attachment

APPROVED: _____

DISAPPROVED: _____

DATE: _____

**When separated from
attachment, handle this
document as UNCLASSIFIED**

cc: HQ Foreign Visits and Assignments Team (AU-41)

WHEN COMPLETED MARK THIS MEMORANDUM AS OFFICIAL USE ONLY

MEMORANDUM FOR RECORD

(Must be retained for 5 years)

VISIT/ASSIGNEE INFORMATION

First Name: _____ Middle: _____ Last: _____
Date of Birth: _____ Place of Birth: _____
Citizenship Country: _____ Gender: ☐ Male ☐ Female
Home Address: _____
Passport Number: _____ Country of Issue: _____ Expiration Date: _____
Military Service ID (if applicable) _____
Arrival/Departure Card (I-94) Number: _____ Class: _____ Expiration Date: _____
Organization Represented (Employer): _____
Country of Employer: _____
Title/Rank (if part of agreement/treaty): _____
International Agreement or Treaty Under Which Visit Will Occur: _____
Location of Visit (Building or Facility Only): DO NOT INDICATE ROOM NUMBER
Date Security Assurance Received: _____
Estimated Start Date: _____ Estimated End Date: _____
Sponsoring Program Office: _____
Host Name and Telephone Number: _____
Program Office with Approval Authority: _____
Name of Approving Official: _____ Date of Approval: _____

CLOSE-OUT INFORMATION

Actual Start Date: _____ Actual End Date: _____

Visit Status: (Write "Complete" or explanation of why visit did not occur): _____

OFFICIAL USE ONLY

May be exempt from public release under the Freedom of Information Act
(5 U.S.C.), exemption number and category: Exemption 6, Personal Privacy
Department of Energy review required before public release
Name/Org: _____ Date: _____
Guidance (If applicable): DOE Guide 471.3-1, 4/9/03

This page intentionally left blank.

Section 602

Unclassified Foreign National Visits and Assignments

DOE supports unclassified visits and assignments by foreign nationals to DOE facilities for the benefit of its programs. The Secretary of Energy promulgates the policy according to the requirements established in DOE O 470.4B, *Safeguards and Security Program* and DOE Order 142.3A, *Unclassified Foreign Visits and Assignments Program*. AU-41 is responsible for oversight of unclassified foreign national visits and assignments to HQ facilities.

This section does not apply to visits or assignments where classified information is intentionally disclosed to a foreign national in accordance with U.S. treaty obligations. These procedures are described in Section 601, Foreign National Classified Visits.

HQ Implementation Procedures

General Requirements:

- These requirements apply to all unclassified visits/assignments by foreign nationals that occur within an HQ facility, except activities described in the Exemptions subsection below.
- These requirements apply to foreign national attendance at all meetings, conferences, events, and HQ element sponsored activities or official business occurring at an off-site location, except activities described in the Exemptions subsection below.
- All unclassified FV&A must be initiated by entering required data into the FACTS, except activities described in the Exemptions subsection below. Each HQ element must have at least one FACTS data entry person designated and trained. Training is available from the DOE National Training Center (see Helpful Websites at the end of this section).
- The HQ FV&A Team, within AU-41, must process all unclassified FV&A requests (see the Specific Headquarters Procedures subsection below for further details).
- The Head of Element (or his/her officially appointed delegate) approves unclassified FV&As to HQ facilities. The term "Approval Authority" is used throughout this section and means the Head of Element or his/her designee. A signed memorandum from the Approval Authority is required of each approved foreign visit/assignment.
- Current Foreign Visitor Assignment Delegation of Approval Authority memoranda (if any) must be on file with the HQ FV&A Team.
- Foreign nationals seeking admittance to an HQ facility without proper written and FACTS approval from the Approval Authority are denied admission.

- A foreign national cannot be designated as a host unless he or she is a DOE federal employee or a DOE contractor. A sensitive country national (to include nationals of state sponsors of terrorism) cannot be designated as a host of another foreign national.
- Escorts are required for all foreign visitors/assignees during Security Hours (see Section 106, Security Hours). Escorts are also required for all visitors/assignees entering an LA or VTR and for all High-Level Protocol visits. Escorts must be DOE permanently badged U.S. citizens and must remain with the foreign visitor/assignee for the duration of the visit.
- Foreign National visitors and assignees will not be processed for HSPD-12 credentials. Visits and assignments will be processed in line with the requirements of DOE O 142.3A Chg 1. Upon approval of all required documentation all foreign national visitors and assignees will be issued a Local Site-Specific Only (LSSO) badge.
- Specific Security Plans are required for FV&As meeting the criteria outlined in the Specific Headquarters Procedures subsection below. Generic security plans are not required; however, hosts and escorts must adhere to the minimum security requirements described in the Security Reference Document (see Attachment 602-10).
- Indices Checks of foreign visitors/assignees may be required (see the Indices Checks subsection below).
- Only the Secretary of Energy or cognizant Under Secretary can approve visits/assignments by nationals from countries on the list of State Sponsors of Terrorism (see State Sponsors of Terrorism Requests subsection below).
- Supporting documentation for FV&As must be retained for 5 years in accordance with the DOE RIDS. AU-41 reserves the right to request copies of visit/assignment requests and supporting documentation.

Exemptions:

- HQ elements seeking deviations or modifications to these requirements must obtain the approval of the Secretary of Energy or his/her designee. A copy of the request should be forwarded to the HQ FV&A Team (see Points of Contact subsection below).
- These requirements do not apply to events, activities, or locations open to the general public. The sponsoring Head of Element or his/her designee determines what events and activities are open to the public (See DOE O 142.3A, Chg 1.). Elements must coordinate with AU-41 prior to finalizing plans for public meetings held within an HQ facility. An approval memorandum signed by the Approval Authority must be provided to the HQ FV&A Team to pass the memorandum to AU-41 prior to the event.

- The Head of Element may exempt offsite events from these requirements when:
 - Events or activities are determined to be open to the general public (such as public lectures, community meetings, cultural or entertainment events, or open house events). Public events include only information unprotected by statute, regulation, or DOE policy, and determined to be releasable to the general public, held in locations accessible to the general public, and available for attendance by the general public. The Approval Authority determines exemptions for the hosting HQ element after coordinating with the HQ FV&A Team. The HQ FV&A Team helps facilitate necessary Subject Matter Expert (SME) reviews.
 - The exemption is documented in writing.
 - Copies of the exemption document must be provided to the HQ FV&A Team and the Office of Counterintelligence (IN-20).
- Access by foreign nationals 17 years of age or younger involved in non-work-related activities (school tours, family days, etc.) do not require prior approvals or documentation in FACTS. Access for work-related activities by foreign nationals 17 years of age or younger, however, must adhere to the requirements of this section.
- Unclassified events and activities occurring outside the United States or its territories do not require approval and need not be documented in FACTS, but may require documentation in the Foreign Travel Management System (FTMS – see the Helpful Websites subsection below) or reporting to IN-20 (see Points of Contact subsection below).
- Visits to the Deputy Administrator for Naval Reactors will be addressed by programs implemented by the Deputy Administrator, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (as prescribed by 42 U.S.C. 7158).
- Visits by foreign national delivery, service, and vendor personnel do not require prior approval or documentation in FACTS; however, these foreign nationals must be fully escorted the entire time they are within the HQ facility. If a foreign national in this category is left unescorted, he/she is removed from the facility and the matter reported as a security incident.

Definitions:

Approval Authority – The individual assigned the responsibility and accountability to approve requests for access by foreign nationals to DOE sites, programs, information, and technologies. Officials who assign approval authority are responsible and accountable for ensuring that the authority assigned is implemented consistent with the requirements of DOE O 142.3.

Assignee – A foreign national approved to access a DOE site, information, or technology for a period of more than 30 consecutive calendar days, but less than 24 consecutive months.

Assignment – Foreign national access for more than 30 consecutive calendar days, but less than 2 full 24 consecutive months. An assignment may be extended for an additional 2 years after required reviews and approvals are completed. Approval for assignments is suspended when a foreign national assignee is unable to prove that he/she is legally present in the United States.

Cancelled After Approval – A Foreign Access Central Tracking System (FACTS) closeout term for visits or assignments cancelled after a final access approval determination has been made.

Cancelled Before Approval – A Foreign Access Central Tracking System (FACTS) closeout term for visits or assignments cancelled before a final access approval determination has been made.

Closeout Information – The final action data in Foreign Access Central Tracking System (FACTS) for a visit or assignment. Closeout information includes the documentation of the visit as cancelled, no show, or complete. Closeout information is documented in FACTS within 15 days after the last day of access.

Completed – A Foreign Access Central System (FACTS) closeout term for visits or assignments which have taken place and ended.

Dual Citizenship – Recognition of a person as a citizen by more than one country.

Export Controlled Information – Certain unclassified government information, for which DOE is accountable and responsible, requiring a specific license or authorization to export and protected according to U.S. laws and regulations. Unrestricted dissemination of this information could adversely affect the U.S. national security and nonproliferation objectives.

Foreign National – An alien. For the purposes of DOE O 142.3 or its associated Contractor Requirements Document an alien is a person born outside the jurisdiction of the United States, is a citizen of a foreign government, and has not been naturalized under U.S. law.

Foreign National Status – The time a foreign national is authorized to be in the United States and what type, if any, work he/she can perform while in the United States as determined by his/her valid passport, entrance visa, Resident Card, or other U.S. Citizenship and Immigration Services (USCIS) documentation.

High-Level Protocol Visit – A one-day protocol meeting between a foreign national representative and a senior DOE official within the HQ Forrestal Building.

Host – The DOE or DOE contractor employee responsible for the day-to-day activities associated with the successful accomplishment of a visit or assignment. A foreign national who is a DOE employee or DOE contractor employee may be a host. A sensitive country national cannot host another foreign national from any sensitive country.

Indices Check – A procedure where a request is made to appropriate U.S. government agencies to determine whether information exists on a particular foreign national. Indices checks are valid for 2 years from the indices start date, as documented in FACTS by IN-20.

Legal Permanent Resident (LPR) – One who has the right to reside permanently and work in the in the U.S. Unlike a U.S. citizen, however, an LPR does not have the right to vote and can be deported if, for example, convicted of certain crimes. An LPR may also be known as a permanent resident alien or Green Card holder.

National of a State Sponsor of Terrorism – A foreign national, who was born in, is a citizen of, is employed by, or represents a government, company, institution, or other organization based in a country on the Department of State list of State Sponsors of Terrorism.

National Security – The national defense and foreign relations of the United States.

No Show – A FACTS closeout term for visits or assignments where a foreign national has been approved but fails to report.

Nonsensitive Country National – A foreign national who was born in, is a citizen of, is employed by, or represents a government, company, or organization, or institution that is located in a country not on the sensitive country list or the Terrorist Countries List.

Open Information – Information not protected by statute and, therefore, releasable to the general public.

Out of Status – A foreign national in the United States who has gone beyond the legal boundaries established by the USCIS. A foreign national who is out of status is denied access to DOE sites, programs, or information.

Passport – A travel document issued by one's country of citizenship. It can be used for Identification purposes and visa applications or entry to other countries.

Public Area – An area accessible by the general public, and for which there are no requirements for security clearances, security escorts, or security logs, as documented in the site security plan.

Sensitive Country List – A list of countries of which particular consideration is given for policy reasons during the DOE internal review and approval process for visits and assignments by foreign nationals. Countries may appear on the list for national security, nuclear nonproliferation, or terrorism support reasons. The list is maintained by The Office of Counterintelligence, Threat and Analysis Division (IN-21) maintains the list.

Sensitive Country National – A foreign national who was born in, is a citizen of, or is employed by a government, employer, institution or organization of a sensitive country.

Sensitive Subjects List – Unclassified subjects/topics identified in existing Federal regulations governing export control and by DOE as unique to work, information, activities, and or technologies relevant to national security. Disclosure of sensitive subjects has the potential for enhancing weapons of mass destruction capability and proliferation, divulging militarily critical technologies, or revealing other advanced technologies that may adversely affect U.S. national and economic security. These subjects require special management oversight before release to foreign nationals. NA-20 maintains the list of sensitive subjects.

Site – A geographical area where one or more facilities are located, or DOE-controlled land area including DOE-owned facilities (e.g., the Oak Ridge National Laboratory, the Nevada Test Site, the Hanford Site, Idaho National Laboratory, the Pantex Plant).

State Sponsors of Terrorism – Countries that have been identified by the Department of State as sponsors of group and /or activities which support terrorism or terrorist activities and are on the List of State Sponsors of terrorism.

Subject Matter Expert – An individual knowledgeable about the professional standards, requirements, and practices used within the discipline he/she represents (i.e., security, export control, technology transfer, counterintelligence, or intelligence).

Technology – Technical data, skills, know-how, or scientific knowledge. Technology is derived from basic or applied research, development, engineering, technological demonstration, economic and social research, or scientific inquiry into phenomena or technology applications. Technology may exist as machinery or equipment, be recorded or spoken, be represented in a medium for storage or communication, and could be contained in computer software with scientific and technical applications.

U.S. Citizen – As provided for in the U.S. Constitution, and a person entitled to all Constitutional rights and privileges of citizenship.

Visa – A permit granting entry to the United States and assigning a particular status (immigrant/nonimmigrant, student, exchange visitor, diplomat, etc.) evidenced by a stamp in the passport or the status described on USCIS Form I-94 or I-95. A visa is not a guarantee that the foreign national will be permitted to enter the United States. Admission is the responsibility of the USCIS at the point of entry.

Visa Waiver Program – A foreign national request to the USCIS that the requirements of his or her visa be waived (for example, a request to waive the 2-year return home requirement for Government J-1 visa holder). A waiver request is submitted to the USCIS for approval, and a receipt for that requests is obtained to verify that request was made. Whether the foreign national is permitted to work during the period after his or her visa has expired until USCIS make a determination on the visa waiver request is determined by the requirements of the visa involved.

Visit – Access by a foreign national for 30 calendar days or less. Approval for visits is suspended when a foreign national assignee is unable to prove he/she is legally present in the United States.

Visitor – A foreign national approved to access a site, information, or technology for 30 calendar days or less.

Work for Others – Research, development, testing, manufacturing, or experimentation conducted at a DOE facility for an agency other than DOE.

Delegation of Approval Authority:

- The Head of Element may delegate his/her unclassified FV&A approval authority to a management-level employee, provided that:
 - The delegation is made in writing
 - The employee is a U.S. citizen
 - A copy of the delegation is furnished to the HQ FV&A Team.
- The Head of Element is responsible for all activities occurring during the FV&A, regardless of who signed the approval (see Attachment 602-1).
- For an example of the Delegation of Approval Authority memorandum, see Attachment 602-6.

Specific Headquarters Procedures:

This subsection applies to all requests for unclassified FV&As, excluding High-Level Protocol Visits and requests involving foreign nationals from countries designated as state sponsors of terrorism.

- The person planning the FV&A must obtain verbal or written approval from his/her element's Approval Authority prior to initiating the visit/assignment request. This verifies that a valid need exists for the visit/assignment and that the Approval Authority will support it.
- A host for an FV&A must be identified. Hosts should complete a 90-minute, computer based training course, FIT-130D, Foreign Visits and Assignments Host Training, available through National Training Center Course Catalog portion of the Online Learning Center (OLC2) (see Helpful Websites at the end of this section). Contact the HQ FV& A Team for assistance in accessing the course. The element HSO records the host's completion of the training in the "CMPC Training Records" section of the element's Appendix to the HQFMSP.
- Escorts are required for all foreign visitors/assignees during Security Hours (see Section 106, Security Hours). Escorts are also required for all visitors/assignees that enter an LA or VTR and for all High-Level Protocol visits. Escorts must be DOE permanently

badged U.S. citizens and must remain with the foreign visitor/assignee for the duration of the visit. It is recommended there be one escort for every five visitors/assignees.

- Escorts are required to complete an escort briefing (see Attachment 602-2) prior to being assigned escort responsibilities. The element HSO will maintain the original briefing and enter the completion of it in the "CMPC Training Records" section of the Appendix to the HQFMSP.
- The host obtains the required information from the prospective foreign visitor/assignee. Hosts are encouraged to provide the visitor/assignee with the Unclassified Foreign National Visits & Assignments Questionnaire Part I (see Attachment 602-3) to complete and return to the host.
- The host completes the Unclassified Foreign National Visits & Assignments Questionnaire Part II (see Attachment 602-4).
- The host provides both parts of the Unclassified Foreign National Visits & Assignments Questionnaire to his/her element's FACTS data entry person. When the visitor is a citizen of a non-sensitive country, who was born in a non-sensitive country, and representing a non-sensitive country who will not be discussing sensitive subjects or meeting in an LA or VTR, only the sections in Parts I and II of the Questionnaire marked with an asterisk must be completed and entered into FACTS.
- The element's FACTS data entry person enters the required information into FACTS. Note that Forrestal and Germantown are considered two separate facilities within FACTS, so visits/assignments to these locations must be entered as separate requests.
- All required data includes: biographical information and visit/assignment information.
 - Biographical information includes, but is not limited to, personal data including employment, passport, and visa information.
 - Visit/assignment information includes, but is not limited to, the purpose of the visit/assignment, proposed and actual dates of the visit/assignment, topics of discussion, and access to LAs or VTRs.
 - For questions concerning FACTS data entry, contact the FACTS Help Desk (see Points of Contact subsection below).
- Visits/assignments requiring Indices Checks (see Indices Check subsection below) must be entered into FACTS at least 30 days prior to the visitor/assignee's arrival date.
- Visits/assignments not requiring an Indices Checks must be entered into FACTS not later than the first day of access.

- A Specific Security Plan (see Attachment 602-9) is required and must be prepared by the HQ element sponsoring the visit/assignment when the foreign visitor/assignee:
 - Will be accessing an LA, VTR, or SCIF at HQ
 - Will be discussing a sensitive subject (refer to the Sensitive Subjects List – see the Forms/Samples/Graphics subsection below)
 - Will be discussing sensitive information (definition provided in the Definitions subsection above) with the foreign national
 - Was born in, is a citizen of, is employed by or represents the government or an institution of a sensitive country or a country that is a state sponsor of terrorism.
- The Specific Security Plan, if required, must be attached online to the FACTS visit/assignment request for the HQ FV&A Team to review.
- The element's Approval Authority must approve the Specific Security Plan. Copies of the Specific Security Plan must be provided to any host and escorts.
- When a Specific Security Plan is prepared, the host – and escorts, when utilized – is responsible for compliance, and protecting DOE security interests during the visit/assignment.
- Specific Security Plans are specific to each FV&A. A separate Specific Security Plan is required for each visit/assignment meeting the above criteria. A Specific Security Plan can cover multiple foreign visitors/assignees staying together as a group during the visit/assignment. The Specific Security Plan is valid for the duration of the visit/assignment unless changes to the visit/assignment occur.
- FV&As failing to meet the criteria for a Specific Security Plan must follow the required security procedures outlined in this subsection. A synopsis of the security requirements can be found in the Security Reference Document (see Attachment 602-10). The Security Reference Document should be provided to hosts and escorts and used as a reference tool.
- The element's FACTS data entry person informs the HQ FV&A Team via e-mail at HQFV&ATeam@hq.doe.gov when a new visit/assignment request has been added to the FACTS database. The following statement can be used for this notification: "The Office of _____ (Org. Code) has submitted a new foreign national visit/assignment request in FACTS."
- The HQ FV&A Team verifies that the required information has been entered into FACTS and that a Specific Security Plan has been properly completed, and conducts necessary SME reviews.

- FV&As meeting specific criteria must undergo a formal SME review. SME reviews are obtained by the HQ FV&A Team (see the SME Reviews and IN Coordination subsection below).
- After all SME reviews are complete and the required information is entered in FACTS, the HQ FV&A Team notifies the element, via e-mail to the host, HSO, and FACTS data entry person, and provides relevant information from the SME reviews. The FV&A host must relay any information discovered during the SME review to the element's Approval Authority. The Approval Authority considers the results before deciding whether to approve the visit/assignment request.
- The element's Approval Authority must then approve the visit/assignment. The request for approval must be made in writing (see Attachment 602-7). The memorandum must include:
 - The dates, facility location, and purpose of the visit/assignment
 - The name and telephone number of the host for the visit/assignment
 - The name, citizenship, employer, job title, FACTS generated visitor number, and request ID of each prospective foreign visitor/assignee
 - A statement that FACTS data entry is complete, with reviews and approval entered prior to access
 - A statement that a Specific Security Plan has been prepared, if applicable, and is attached
 - When required, a statement that the HQ FV&A Team conducted an SME review regarding sensitive subjects or technology transfer issues
 - When required, a statement that an Indices Check or a counterintelligence consultation was completed
 - A statement that coordination was completed with the Office of the Chief Information Officer (IM-622) (or within the organizational Chief Information Officer) if computer access is requested for the visitor or assignee
 - The signature of the Approval Authority approving or denying the proposed FV&A and the associated Specific Security Plan, if applicable.
- After the Approval Authority approves or denies the request, the element's FACTS data entry personnel documents approval or denial within FACTS.
- A copy of the signed Approval Request must be provided to the HQ FV&A Team.
- The sponsoring organization in accordance with the DOE RIDS must maintain all

requests for approval memorandums.

- Before an approved visitor/assignee is admitted to HQ, the HQ protective force receptionists review the FACTS entry to ensure that the proper approvals are granted before issuing the proper security badge.
- The host or a representative from the sponsoring HQ element, with assistance from the protective force receptionists, verifies the visitor/assignee's passport, visa, and USCIS information. The foreign visitor/assignee must provide sufficient documentation to verify his/her identity, confirm he/she is permitted to work in the United States (if applicable), and ensure he/she is lawfully in the United States. The purpose of these reviews is to validate that the information in FACTS is accurate prior to granting access on the first day of his/her visit or assignment. The sponsoring HQ element is also responsible for annually re-verifying in FACTS the passport, visa or other USCIS information of all foreign assignees.
- The host must provide any USCIS information not entered into FACTS to the element's FACTS data entry person; the information must be entered by the end of the first day of the visit/assignment.
- All requests for visits/assignments must be "closed out" in FACTS. Sponsoring elements are responsible for close-out actions and entering the following data in FACTS within 15 days of the completion of the visit/assignment:
 - Enter data in the appropriate fields to indicate whether the visit/assignment was not approved, did not occur, was cancelled, or was completed
 - Enter the actual end date of the visit or assignment
 - Enter any changes to the original request, such as arrival/departure times, date(s) of visit, etc.
- The Security Requirements Decision Matrix (see Attachment 602-11) summarizes the above process for unclassified FV&A requests.

High-Level Protocol Visit Procedures:

- A High-Level Protocol Visit is used for foreign nationals visiting the Secretary, Deputy Secretary, Under Secretaries, Program Secretarial Offices, or other senior Department officials, and foreign national representatives of foreign governments or organizations of foreign governments in the HQ Forrestal building.
- A High-Level Protocol Visit is limited to one day and occurs solely at the Forrestal building.

- Advance approval reviews may be suspended if requested by these senior Departmental managers, subject to compliance with the security plans and procedures developed for High-Level Protocol visits.
- These visitors must be documented in FACTS within one working day of the visit. Justification for these visits must address the protocol nature of the visit.
- The Sample High-Level Protocol Approval Request form (see Attachment 602-8) should be used to obtain the necessary information and approvals for this type of request.
- The element's FACTS data entry person enters all required information into FACTS.
- The Specific Security Plan, if required, must be attached online to the FACTS visit/assignment request for the HQ FV&A Team to review.
- The element's FACTS data entry person informs the HQ FV&A Team via e-mail to HQFV&ATeam@hq.doe.gov when a new High-Level Protocol Visit is added to the FACTS database. The following statement can be used for this notification: "The Office of _____ (Org. Code) has submitted a new High-Level Protocol Visit in FACTS."
- The HQ FV&A Team verifies that all required information was entered into FACTS and verifies that a Specific Security Plan, if required, was completed properly. SME reviews are not required for High-Level Protocol Visits if the following conditions are met:
 - The foreign national visitor is not a citizen of a country on the Terrorist Supporting Countries List.
 - Discussions with the visitor will not involve export controlled technologies.
 - Discussions with the visitor will not include sensitive or classified matter relating to nuclear weapons, proliferation, intelligence collection, satellite imagery, or signals intelligence technology.
 - The foreign national visitor will not be permitted to operate, use, or service DOE information systems/equipment.
 - The foreign national visitor must be escorted at all times while on DOE grounds.
- If the sponsoring element cannot confirm the above requirements, the HQ FV&A Team obtains the required SME reviews.
- Indices Checks need not be completed prior to the approval of a High-Level Protocol visit.

- A Specific Security Plan (see Attachment 602-9) is required and must be prepared by the HQ element sponsoring the High-Level Protocol visit when the foreign visitor:
 - Will be accessing a Limited or n LA, VTR, or SCIF at HQ
 - Will be discussing a sensitive subject (see Sensitive Subjects List; refer to the Forms/Samples/Graphics subsection below)
 - Was born in, is a citizen of, is employed by, or represents the government or an institution of a sensitive country or a country that is a state sponsor of terrorism.
- High-Level Protocol visits that fail to meet the above stated criteria must follow the security procedures outlined in this subsection. A synopsis of the security requirements can be found in the Security Reference Document (see Attachment 602-10). Hosts and escorts should be given the Security Reference Document to assist them in performing their duties.
- These visits must be documented in FACTS on the day of the visit. Justification for these visits must address the protocol nature of the visit.
- After the Approval Authority approves or denies the request, the element's FACTS data entry personnel must document the approval or denial within FACTS.
- A copy of the signed approval request must be provided to the HQ FV&A Team.
- The sponsoring organization, in accordance with the DOE RIDS, must maintain all requests for approval memorandums.
- Before an approved visitor/assignee is admitted to HQ, the HQ protective force receptionists review the FACTS entry to ensure that the proper approvals were granted and then issue the proper security badge.
- Escorts are required for all High-Level Protocol visits. All High-Level Protocol visitors must be met in the Forrestal Lobby and remain under escort throughout their visit.
- VIP badges are issued to High-Level Protocol visitors to the Secretarial Suite.
- At the discretion of AU-41, DV badges are issued to High-Level Protocol visitors visiting Heads of HQ Elements (or in the case of NNSA, Deputy or Associate Administrators).

State Sponsors of Terrorism Requests:

- The site Approval Authority must approve access requests for nationals of state sponsors of terrorism who are not lawful permanent residents before final approval determination. The Secretary of Energy holds final approval authority and can assign it to only Deputy Secretary, Under Secretary for Nuclear Security Administration, Under Secretary of

Energy, or Under Secretary for Science. The Deputy Secretary or appropriate Under Secretary, in consultation with IN-20, makes the final approval determinations for these access requests. Subsequent assignment requests extending access to the hosting field site or HQ program, staff, or support office may be approved by the Approval Authority for that field site or HQ office.

- The Sensitive Country List & Terrorist Supporting Countries List identifies the countries designated as state sponsors of terrorism (see the Forms/Samples/Graphics subsection below). It is OUO and must be handled accordingly.
- The sponsoring element must prepare and document a request for approval of a visit/assignment by a national of a state sponsor of terrorism, Specific Security Plan, computer security plan (if cyber access is requested), visa, passport, or other USCIS information, the results of the SME reviews, and the risks and benefits of the proposed visit/assignment. More specific guidance for this type of request is available from the Office of Security Assistance (AU-52) (see Attachment 602-12).
- After approval by the Head of Element, the request is submitted through AU-52 to the HQ Management Panel for review and submission to the Secretary of Energy or cognizant Under Secretary for final approval determination.

Indices Checks:

- Indices Checks are conducted by IN-20 using pertinent data from FACTS. In coordination with other Federal agencies, IN-20 determines whether the foreign visitor/assignee poses a threat to national security.
- Indices Checks are requested automatically through the process of inputting visit/assignment data in FACTS.
- Indices Checks are valid for a period of 2 years from the indices completion date, as documented in FACTS by IN-20.
- Indices Checks are required for:
 - All FV&A requests involving nationals of state sponsors of terrorism
 - All FV&A requests involving sensitive country nationals
 - All FV&A requests involving the discussion of sensitive subjects
 - All FV&A requests that may occur within an LA or VTR.
- Refer to the Sensitive Country List and Terrorist Supporting Countries List and Sensitive Subject List (see the Forms/Samples/Graphics subsection below) for a listing of the applicable countries and subjects.
- Each element HSO should know where his/her LAs and VTRs are located.

- IN-20 enters Indices Checks results into FACTS.
- Completion of Indices Checks:
 - Indices Checks for sensitive country national visitors need not be completed prior to approval.
 - Indices Checks for High-Level Protocol visits need not be completed prior to approval.
 - Indices Checks for sensitive country national assignees must be completed prior to approval. The results of Indices Checks must be provided to the Approval Authority who must consider the results before deciding whether to approve the assignment.
 - Indices Checks for all visits/assignments requests by nationals of either sensitive or non-sensitive countries that involve access to sensitive subjects must be completed prior to approval. The results of Indices Checks must be provided to the Approval Authority who must consider the results before deciding whether to approve the visit/assignment.
 - Indices Checks for all visit/assignment requests involving access to an LA, VTR, or SCIF must be completed prior to approval. The results of Indices Checks must be provided to the Approval Authority who must consider the results before deciding whether to approve the visit/assignment.
 - Indices Checks for all visit/assignment requests involving nationals from state sponsors of terrorism must be completed prior to approval by the Head of Element. The results of Indices Checks must be provided to the Head of Element who must consider the results before deciding whether to approve the visit/assignment and submit it to the HQ Management Panel for review.
- When an Indices Check is required but cannot be completed before the visit or assignment is to take place, a Counterintelligence Consultation is available. Requests for consultations may be made through the IN-20 Forrestal Field Offices (FFO) at either the Forrestal Facility or the Germantown Facility (contact information is provided at the end of this subsection).
 - A Counterintelligence Consultation is a discussion between the sponsoring element's Approval Authority and an IN-20 representative and must be completed prior to the visit/assignment.
 - The Counterintelligence Consultation requires the Approval Authority to submit a memorandum to IN-20 that provides detailed information on the request and any concerns the host has (see Attachment 602-5).

- IN-20 contacts the Approval Authority to provide information about counterintelligence findings or concerns pertaining to the proposed visit/assignment. The Approval Authority then makes an informed decision on whether to approve the visit/assignment request.
- IN is required to enter the date the Counterintelligence Consultation was conducted into FACTS.
- AU-41 reserves the right to request copies of requests for Counterintelligence Consultations.
- IN-20 does not approve or disapprove requests for FV&A. The Approval Authority makes the final approval/disapproval decision.
- Counterintelligence Consultations should be used sparingly as an alternative to Indices Checks.
- Counterintelligence Consultations may not be used in lieu of Indices Checks for visits/assignments involving nationals of state sponsors of terrorism.

SME Reviews and IN-20 Coordination:

- An SME is an employee knowledgeable about the professional standards, requirements, and practices used within the discipline he/she represents. SME reviews are required for specific foreign national visits and assignments. SME reviews are conducted in areas of export control, technology transfer, counterintelligence and intelligence.
- SME reviews must be completed prior to the approval and admittance of the following foreign national requests:
 - All assignments to an HQ facility
 - All visits that involve the foreign national accessing an LA, VTR, or SCIF at HQ
 - All visits that will include the discussion of a sensitive subject (see the Sensitive Subjects List; refer to the Forms/Samples/Graphics subsection below)
 - All visits that will include the discussion of sensitive information (see the Definitions subsection above)
 - All visits that require the foreign national to access a DOE computer system
 - All visits that involve a foreign national who was born in, is a citizen of, is employed by, or represents the government or an institution of a sensitive country or a country that is a state sponsor of terrorism.

- Advanced SME approval reviews are not required for High-Level Protocol visits if the element can confirm all of the following:
 - The foreign national visitor is not a citizen of a country on the Terrorist Supporting Countries List.
 - Discussions with the visitor will not involve export controlled technologies.
 - Discussions with the visitor will not include sensitive or classified matter relating to nuclear weapons, proliferation, intelligence collection, satellite imagery, or signals intelligence technology.
 - The foreign national visitor will not be permitted to operate, use, or service DOE information systems/equipment.
 - The foreign national visitor will be closely escorted at all times while on DOE grounds.
- AU-41 established the HQ FV&A Team to centrally screen, review, or coordinate all requests for unclassified FV&As to HQ facilities. The HQ FV&A Team automatically screens all HQ-originated FACTS inputs for security, Operations Security (OPSEC), TSCM, export control, and technology transfer concerns. The HQ FV&A Team determines what SME reviews are required and ensures the necessary reviews are completed. The HQ FV&A Team also reviews the Specific Security Plans included in the FACTS request. The HQ FV&A Team cannot approve or disapprove a visit or assignment request. The Team's role is to provide security-related information and cautionary guidance to the Approval Authority before approval is granted. If the Team requires highly specialized assistance in subjects such as export control, technology transfer, or computer security, the Team refers the matter to personnel in the Office of Export Control, Policy, and Cooperation (NA-242) or IM-622, or to the element's Chief Information Officer. Those offices may provide additional guidance or comments to the Approval Authority (see Points of Contact subsection below).
- When a visit/assignment request involves computer access, coordination with either IM-622 or the element's Chief Information Officer must occur so that a cyber SME review is conducted. This information and date of the consultation/notification must be entered in FACTS. IM-622 or the element's Chief Information Officer provides a separate computer security plan that must be followed in addition to all other security requirements.
- Coordination with IN-20 must occur when information concerning an intelligence review was not entered into FACTS. The Approval Authority must consult with IN prior to approving any visit/assignment of a foreign national involving information related to nuclear weapons, nuclear weapons proliferation, intelligence collection, satellite imagery, or signals intelligence technology or when the possibility exists for those topics to be discussed. The date of the consultation must be entered into FACTS.

Points of Contact

FACTS Help Desk, 804-744-8800

For Forrestal Counterintelligence Officer (IN-20) support, call (202) 586-1378 or (202) 586-2297.

For Germantown Counterintelligence Officer (IN-20) support, call (301) 903-2039 or (301) 903-0434.

Office of the Chief Information Officer (IM-622), (202) 586-2883.

For the names and contact information for those occupying other positions identified in this chapter, call (202) 586-8075.

Forms/Samples/Graphics

Sample Approval Authority Certification (see Attachment 602-1)

Foreign National Visit and Assignment Escort Briefing (see Attachment 602-2)

Unclassified Foreign National Visits & Assignments Questionnaire Part I (see Attachment 602-3)

Unclassified Foreign National Visits & Assignments Questionnaire Part II (see Attachment 602-4)

Sample Counterintelligence Consultation Memorandum (see Attachment 602-5)

Sample Delegation of Approval Authority Memorandum (see Attachment 602-6)

Sample Foreign National Visit or Assignment Approval Request (see Attachment 602-7)

Sample High-Level Protocol Approval Request (see Attachment 602-8)

Sample Specific Security Plan (see Attachment 602-9)

Security Reference Document (see Attachment 602-10)

Foreign Visits and Assignments Security Requirements Decision Matrix (see Attachment 602-11)

Approval request for a Visit/Assignment by a Foreign National from A State Sponsor of Terrorism Package (see Attachment 602-12)

Sensitive Country List & Terrorist Supporting Countries List (this document is OUO and available from IN-20)

Sensitive Subjects List (this document is OUO and available from NA-242)

Helpful Website

<https://ntc.doe.gov/>

ATTACHMENT 602-1

Sample Approval Authority Certification

An Approval Memorandum, signed by the HQ Element's Approval Authority, is required before any Foreign National will be admitted to HQ facilities. By signing the Approval Memorandum, the Approval Authority is stating as follows:

I certify that I have reviewed the request for access approval for (Name of Foreign National), FACTS Visit/Assignment Number (Enter Numbers), and considered all the sensitivity factors associated with the requested access to DOE sites, programs, information, and technologies. I have reviewed the advice provided by the Subject Matter Experts in Security, Export Control, Technology Transfer, Security, Counterintelligence, and, when appropriate, Intelligence regarding this request. I have acknowledged receiving those reviews, and have addressed any concerns to the satisfaction of the Subject Matter Experts involved. My determination is consistent with the professional standards and practices used to ensure any risk to the Government associated with access approval is appropriately identified and evaluated.

Additionally, I certify that, in my opinion, the benefits to the Government are greater than the risks associated with the presence of the foreign national and that all legal and policy-related terms and conditions associated with the proposed Visit/Assignment have been met. These terms and conditions include, but are not limited to, other activities at the site, visa sponsorship requirements, visa status conditions and requirements, right-to-work requirements, and international agreements.

ATTACHMENT 602-2

Foreign National Visit and Assignment Escort Briefing

DOE Federal and contractor personnel responsible for escorting foreign nationals should use the following briefing in preparation for escorting:

- Foreign nationals entering an LA, VTR, or SCIF
- Foreign nationals within HQ during Security Hours (see Section 106, Security Hours)
- All High-Level Protocol visits.

The escort should maintain a signed copy of this briefing, while your element HSO maintains the original. Please review Section 602, Unclassified Foreign National Visits and Assignments, of the HQFMSP, for more detailed information regarding foreign national visit and assignment requests.

Definition: An escort is an authorized, DOE permanently badged U.S. citizen (Federal or contractor employee) assigned the responsibility of accompanying foreign nationals lacking need-to-know or access authorization within an LA, VTR, or SCIF to ensure they adhere to HQ security measures.

Escort Responsibilities:

Escorts are required to:

- Be familiar with the site/facility, including LAs and VTRs
- Have full understanding and knowledge of the FV&A security procedures and Specific Security Plan, if applicable (your element HSO should provide the Specific Security Plan)
- Have a security clearance, L or Q, commensurate with the level of information handled within the LA or VTR to be visited
- Have knowledge of specific information or technologies the foreign national has been authorized to access.

Meeting the Foreign Nationals

The escort must meet the foreign national, at the direction of the host, at either the lobby of the building or at the entrance to the LA or VTR. All High-Level Protocol visitors must be met in the Forrestal Lobby and be under escort at all times and in all places throughout their visit, as discussed below.

The escort must ensure that the foreign national was issued a foreign national badge by the building/facility receptionist. If not, the escort must direct the foreign national to the reception desk to obtain a foreign national badge.

The escort must instruct the foreign national to display the foreign national badge above his/her waist in an easily observable position, inform him/her of what articles are prohibited within the facility, and inform him/her of the controlled articles (e.g., cell phones, pagers, Blackberries, laptop computers, and other electronic devices) that are prohibited in LAs and VTRs. If the foreign national has a controlled article, the device must be turned off and stored in an RF bag or a storage container outside the LA or VTR. If no RF bag or storage container is available, the device must be returned to the visitor's vehicle.

If the visitor needs to leave the facility, the foreign national visitor badge may be retained temporarily at a manned protective force post. The foreign national will be given a token, which must be returned to the same protective force post to retrieve the visitor's badge.

Escorting the Visitor

The escort must escort the foreign national at all times while in an LA or VTR, during Security Hours or during all High-Level Protocol visits.

As a rule of thumb, one escort should not escort more than five foreign nationals. If there are more than five visitors, additional escorts should be available.

The escort must ensure that foreign nationals entering VTRs sign in and out on the visitor register and announce their presence.

The escort must ensure that the foreign national is not allowed to access any classified information by overhearing classified conversations, reading or copying classified information, observing classified computer processing, or any other means.

Escorts must ensure that the visitor/assignee does not attempt to obtain, copy, or otherwise access sensitive information. Escort responsibilities include preventing the foreign visitor/assignee from accessing desk drawers, filing cabinets, or other containers where such information could be located. Sensitive information includes, but is not limited to OOU, Unclassified Controlled Nuclear Information (UCNI), Export Controlled Information (ECI), Naval Nuclear Propulsion Information (NNPI), PII, Company Proprietary Information, personnel files, and other forms of information related to a person's privacy.

The escort must ensure that the foreign national does not remove any DOE property unless an authorized person issues a property pass.

If the foreign national needs to use a restroom, the escort must accompany the foreign national to the restroom door and remain outside until the foreign national is ready to return.

If there are multiple foreign nationals and they need to go in different directions, the escort must arrange for additional escorts. (**Note:** Intelligence collectors commonly use this approach to test or defeat visitor control measures.)

The escort must ensure that the foreign national badge is returned to the protective force reception desk or any manned protective force post when the visit is completed.

I acknowledge that I have read this briefing and understand my responsibilities and the requirements for escorting a foreign national:

Printed Name

Signature

Date

ATTACHMENT 602-3

Unclassified Foreign National Visits & Assignments Questionnaire Part I

Welcome to Department of Energy, Headquarters! We are looking forward to your visit or assignment with us. In order to comply with our security requirements and ensure that your time with the Department of Energy goes smoothly we need to obtain some information from you prior to your arrival.

Please take a few minutes to provide the information requested below for each member of your party that is not a U.S. citizen and then return the form(s) to your host.

Please be sure to comply with the deadlines your host has communicated to you for returning this form.

Part 1: Completed by Visitor

Please complete all questions below, as applicable. See listing of requested documents at end.

1*	Given Name/First Name (exactly as it appears on passport)	
2*	Middle Name (exactly as it appears on passport)	
3*	Surname/Last Name (exactly as it appears on passport)	
4*	Gender	☐ Male ☐ Female
5	Are you currently in the United States?	☐ Yes ☐ No
6	Are you Currently a Legal Permanent Resident (LPR) Immigrant Alien of the U.S.?	☐ Yes (go to question 7) ☐ No (skip question 7)
7	Immigration & Naturalization (INS A#) Number and Expiration Date	INS A#: Expiration Date:
8*	Primary Citizenship (Citizenship admitted to United States)	
9*	Dual Citizenship (if any)	☐ Yes ☐ No If yes, what Country?
10*	Birth Date	
11*	Country of Birth	
12*	City of Birth	

13*	Institution or Company Name	
14*	Institution or Company Address and Country	
15	Employer Telephone Number	
16	Employer Facsimile Number	
17	Employer E-mail Address	
18*	Title/Description of Duties with Employer/Company	
19*	What is the U.S. Visa Type you will have/require upon arrival in U.S. for this visit, assignment or employment?	☐ A2 ☐ H1 ☐ TN ☐ F1 ☐ J1 ☐ B1 ☐ O-1 ☐ E2 ☐ Visa Waiver Business (VWB) ☐ Other: ☐ Employment Authorization Document (EAD) Number and Expiration date:
20*	Visa Number and Expiration Date (This is the Form I-94 number; if J-1 or F-1 visa.	I-94 Number: Valid Until Date:
21*	Passport Number and Expiration Date (mm/dd/yyyy)	Passport Number: Expiration Date:
22	What Country Is Identified On Your Passport As Issuer?	
23	Other ID (specify type and number, if applicable)	

ATTACHMENT 602-4

Unclassified Foreign National Visits & Assignments Questionnaire Part II

Part 2: Completed by Host

24	Facility to be accessed	☐ Germantown ☐ Forrestal ☐ Other (must specify) ☐ Off Site
25	Will any Sensitive Information (see list at right) be shared with the visitor or assignee?	(Check at least one but all that apply) ☐ Official Use Only (OUO) ☐ Export Controlled Information (ECI) ☐ Unclassified Controlled Nuclear Information (UCNI) ☐ Personally Identifiable Information (PII) ☐ Company Proprietary Information ☐ Unclassified Naval Nuclear Propulsion Information (NNPI) ☐ N/A
26	Select the Security Area Type at the Facility (choose the highest area type in case multiple areas are to be visited)	☐ Property Protection Area (PPA) with Access to Sensitive Info ☐ Property Protection Area (PPA) w/out Access to Sensitive Info ☐ Limited Area ☐ VTR ☐ SCIF ☐ Non-Security Area (for off-site requests only)
27	Type of Request	☐ Visit ☐ Assignment ☐ Extension of an Assignment ☐ High Level Protocol Visit
28	Is this an IAP-66 (DS-2019) assignment?	☐ Yes ☐ No
29*	Is this an off site meeting?	☐ Yes ☐ No ☐ Both
30*	Will Sensitive Subjects be involved or discussed ("Sensitive Subjects" are not the same as "Sensitive Information" in row 25, above)	☐ Yes ☐ No If yes, please specify: (See 'Sensitive Subject List' document) If in doubt contact the HQ FV&A Team for clarification
31*	Host and Escort's Full Name(s) (Must be DOE federal staff or contractor. Sensitive country nationals CANNOT host or escort any foreign national visitors or assignees)	Host: Escort(s):
32*	Citizenship of Host	
33*	Host Office Phone Number	
34	Host Office Facsimile Number	

35	Does Host have a clearance?	☐ Yes ☐ No		
36*	Authorized Arrival and Authorized Departure Date	Arrival Date: Departure Date:		
37*	Meeting Subject	(see 'FACTS Subject Codes' spreadsheet)		
38*	Headquarters Departmental Element (HDE) Program Code: (e.g. SC-10, EM-45)			
39*	Justification for Visit/Assignment			
40*	Purpose of Visit	(see 'FACTS Purpose Codes' spreadsheet)		
41	Intermittent Access (Check "Yes" checkbox if Foreign National plans on leaving and returning intermittently for days at a time and will not be present continuously for entire period of request)	☐ Yes ☐ No If yes, number of days on-site?		
42	Number of Days On-Site			
43*	List Buildings and Rooms to be accessed:	Building	Room	Type
		Building	Room	Type
		Building	Room	Type
44	Cost to DOE			
45*	DOE Mission(s) that will be advanced by this Visit/Assignment			
46	Anticipated Benefits to DOE Programs			
47	DOE Contact	Full Name Phone Number		
48	Is an Export Control License Required?	☐ Yes ☐ No If in doubt contact the HQ FV&A Team for clarification		

49	Will this Visit or Assignment include transfer of technology? (Technology defined as technical data, skills, know-how, or scientific information. Technology is derived from basic or applied research, development, engineering, technological demonstration, economic and social research, or scientific inquiry into phenomena or technology applications. It may exist as machinery or equipment; it may be recorded, spoken, or represented in a medium for storage of communication; and it may be contained in computer software with scientific and technical applications.)	☐ Yes ☐ No Describe Technology Transfer, or provide reason for no Transfer of Technology (max length of 500 characters): If in doubt contact the HQ FV&A Team for clarification
50*	Will Visitor/Assignee be granted Computer Access?	☐ Yes ☐ No Is the computer access ☐ On-site ☐ Off-site If yes, please list all computers and software: and contact IM-622 at (301) 903-2883 or your organizational Chief Information Officer for further instructions
Additional comments:		

ATTACHMENT 602-5

Sample Counterintelligence Consultation Memorandum

MEMORANDUM FOR SENIOR COUNTERINTELLIGENCE OFFICER
FORRESTAL COUNTERINTELLIGENCE OFFICE
OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE

FROM: SPONSORING ELEMENT (INSERT APPROPRIATE NAME AND TITLE)

SUBJECT: Counterintelligence Consultation

This Counterintelligence Consultation memorandum is submitted to the Office of Counterintelligence in accordance with DOE Order 142.3, change 1, *Unclassified Foreign Visits and Assignments Program*, paragraph 4(g), which states: *In cases where there is insufficient time to complete an indices check before the first day of access, the approval authority may request a counterintelligence consultation in lieu of the completion of the indices check for sensitive country and non-sensitive country nationals. If the indices are completed in FACTS a consultation memorandum is not needed.*

Purpose/Reason for Visit: [A short explanation for the visit]

Example: the purpose of the visit is to meet with Russian representatives on the US/Russian Joint Steering Committee to discuss the plutonium disposition program in Russia.

Discussions: [Time, date, and location of the visit/meeting. Briefly describe the subject(s) of the discussion(s) and their sensitivities. **NOTE: This is an unclassified foreign national visit where classified information may not be discussed.** Indicate any LA or VTR that will be accessed.]

Example: The Steering Committee meeting will be held at 10:30 a.m., May 3, 2005, in Room GA-242, Forrestal. No sensitive subject information will be discussed and no LA or VTR will be accessed by the visitor(s). The attendance of the Russian visitor is essential for maintaining momentum in the plutonium disposition program discussions. This will be the second meeting since the signing of the government-to-government agreement in July 2000 on Technical Cooperation in Plutonium Disposition. There will be observers at the meeting from France, Germany, and Japan.

Visitor Database Entry: [Reason the visitor information could not be entered into FACTS 30 days prior to the visit]

Example: Although requested 45-60 days in advance of the meeting, the names of the Russian representatives were not known 30 days prior to the visit. Visitor information was entered into FACTS on (date). It is not expected that the indices results will be completed prior to the

meeting. This consultation letter is submitted for your review in lieu of the completed indices check(s).

Visitor Information: [List name, citizenship, place of birth, title, company/institution of visitor(s) and the FACTS ID number for each visitor]

Name:

Country of Citizenship:

Place of Birth:

Employer:

Title:

FACTS Request Identification Number:

Host Concerns: [Indicate any security or other concerns you may have as host of the visitor(s)]

ATTACHMENT 602-6

Sample Delegation of Approval Authority Memorandum

MEMORANDUM FOR (NAME), DIRECTOR
OFFICE OF HEADQUARTERS SECURITY OPERATIONS
OFFICE OF HEALTH, SAFETY AND SECURITY

FROM: HEAD OF HEADQUARTERS ELEMENT (*INSERT APPROPRIATE
NAME AND TITLE*)

SUBJECT: Unclassified Foreign Visit and Assignments

The purpose of this memorandum is to delegate approval authority in accordance with DOE Order 142.3, Change 1, *Unclassified Foreign Visit and Assignment Program*, for unclassified foreign visits and assignments requests by (*enter name of organization*):

(*Insert Name*), (*Insert Title*)

These individuals may not further reassign this authority. I understand that I remain responsible for all activities that occur during these visits and assignments.

The below listed individual(s) has/have been designated as Foreign Access Central Tracking System (FACTS) data entry personnel for (*enter name of organization*):

FACTS Data Entry Personnel - Enter Employee's Name,
Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

cc:
Headquarters Foreign Visit & Assignment Team
HSO

ATTACHMENT 602-7

Sample Foreign National Visit or Assignment Approval Request

MEMORANDUM FOR HEAD OF HEADQUARTERS ELEMENT or AUTHORIZED
DESIGNEE (INSERT APPROPRIATE NAME AND TITLE)

FROM: SPONSORING ELEMENT (INSERT APPROPRIATE NAME AND
TITLE)

SUBJECT: Unclassified Foreign Visit or Assignment Request

DOE Order 142.3, change 1, *Unclassified Foreign Visits and Assignments*, requires that the Head of a Program Office, or their delegated designee, approve all unclassified foreign visits and assignments to HQ. This memorandum is to request your approval of a proposed visit (*or assignment*) to HQ by the foreign national(s) identified below. The security plan for this proposed visit (*or assignment*) has been developed and is attached for your approval. *[If a Security Plan is not required omit this last sentence.]*

The following information is submitted:

1. Purpose of Visit/Assignment: [Example: The Office of ___ is hosting a meeting to discuss ____.]
2. Facility to be accessed: [Example: DOE Forrestal Building, Room 1G-042]
3. Dates/Times of Visit/Assignment: [Example: March 27 and 28, 2008; 8:30 AM to 5:00 PM]
4. Visitor Information:
Name:
Country of Citizenship:
Employer:
Title:
FACTS Visitor Number:
FACTS Request Identification Number:
5. Required data for the proposed visit (*or assignment*) has been entered into the Foreign Access Central Tracking System (FACTS).
6. The following Subject Matter Experts have been consulted:
 - The HQ Foreign Visit and Assignment Team SME Reviews in Security (OPSEC, TSCM, general) and Export Control/Technology Transfer: Not required for this visit (*or*

assignment) **or** Include a sentence describing the outcome of the SME reviews **or** The results of the SME reviews have been provided in a separate memorandum and are addressed in the Specific Security Plan.

- Office of Intelligence and Counterintelligence, Indices Checks: Not required for this visit (*or assignment*) **or** Indices Checks are being processed. As of this date, no negative information has been provided by the Office of Intelligence and Counterintelligence **or** The results of the indices checks have been provided in a separate memorandum and are addressed in the Specific Security Plan.
- Office of the Chief Information Officer (IM-622) (*or insert your organizational Chief Information Officer*): Not required for this visit (*or assignment*) **or** Computer access has been requested. IM-622 (*or insert your organizational Chief Information Officer*) has reviewed the proposed visit (*or assignment*) and their comments and requirements have been addressed in the Specific Security Plan.

7. Name and Telephone Number of Host:

8. Point of Contact for Visitor/Assignee:

It is recommended that this visit (*or assignment*) and the attached security plan (*if applicable*) be approved. [*Insert Name*] of my staff, is available on [*insert telephone number*] to answer any questions on this proposed request.

APPROVED: _____

DISAPPROVED: _____

DATE: _____

Attachment
Security Plan (*if applicable*)

cc:
Headquarters Foreign Visit & Assignment Team
HSO
Host (*insert name of host*)
Point of Contact (*insert name of point of contact*)

ATTACHMENT 602-8

Sample High-Level Protocol Approval Request

MEMORANDUM FOR RECORD

FROM: SPONSORING ELEMENT (INSERT APPROPRIATE NAME AND TITLE)

SUBJECT: Unclassified High-Level Protocol Foreign Visit Request

I approve the following foreign national(s) to access the DOE Forrestal Building for a 1 day unclassified high-level protocol visit. The security plan for this proposed visit has been developed and approved and is attached. *[If a Security Plan is not required omit this last sentence.]*

The following information is submitted:

1. Purpose of Visit: Must address the protocol nature of the visit
2. Dates/Times of Visit: Example: March 27, 2008; 8:30 AM to 5:00 PM
3. Visitor Information:

Name of Visitor:

Date of Birth:

Place of Birth (City & Country):

Passport # / Issuing Country / Exp. Date:

Country of Citizenship:

Employer and Country Location:

Title/Position:

Technology Areas to be discussed (specify):

4. Required data for the proposed visit has been entered into the Foreign Access Central Tracking System (FACTS).

The signature of the host indicated below certifies that:

- 1) The foreign national visitor is not a citizen of a country on the Terrorist Supporting Countries List;
- 2) Discussions with the visitor will not involve technologies that are export controlled;
- 3) Discussions with the visitor will not include sensitive or classified matter relating to nuclear weapons, proliferation, intelligence collection, satellite imagery or signals intelligence technology;

4) The foreign national visitor will not be permitted to operate, use, or service any DOE information systems/equipment; and,

5) The foreign national visitor will be closely escorted at all times while on DOE grounds.

Name of Host: _____ Organization: _____

Signature of Host: _____ Telephone Number: _____

Approving Official: _____
(Signature) (Position) (Date)

Attachment
Specific Security Plan (*if applicable*)

cc:
Headquarters Foreign Visit & Assignment Team
HSO

ATTACHMENT 602-9

Sample Specific Security Plan

MEMORANDUM FOR HEAD OF HEADQUARTERS ELEMENT or AUTHORIZED
DESIGNEE (INSERT APPROPRIATE NAME AND TITLE)

FROM: HEADQUARTERS SECURITY OFFICER (INSERT APPROPRIATE
NAME, TITLE AND ORGANIZATION)

SUBJECT: Specific Security Plan for Unclassified Foreign National Visit
(or Assignment)

This Specific Security Plan sets forth the minimum security measures that must be taken to protect DOE security interests during the visit (*assignment*) of a foreign national(s) to the (*Insert Office*) at HQ.

This Specific Security Plan is for a (*Insert origin, e.g., Chinese*) foreign national(s) from (*identify the designated Sensitive Country*). The foreign national will be meeting with (*Insert Host*) in a (*Insert type of security area*). The visitor (*assignee*) will (*will not*) be given access to sensitive unclassified information.

The following minimum security measures must be implemented during the visit:

1. Security Area to be Accessed: *Insert type of area and room location, if applicable, e.g., Limited Area in Room 1G-042, Forrestal Building*
2. Date/Time of Visit: *Insert specifics*
3. Sensitive Subjects to be Discussed: [*None* **OR** *provide explanation of sensitive subject and the export control/technology transfer issues that have been resolved*]
4. Verification of Visitor (*Assignee*) Status: The identity of the foreign national must be verified by reviewing the visitor's (*assignee's*) passports or other U.S. Citizenship and Immigration Services (USCIS) documents and validating the information in FACTS prior to granting access. The host or a representative from the sponsoring HQ Element, with assistance from the Front Desk Receptionists, will review these identity documents.

Assignee plans should also read:

Verification of USCIS documents must be recertified annually for non-sensitive country nationals and semi-annually for sensitive and terrorist country nationals in FACTS.

5. Badging Procedures: A HQ [*Insert type of badge, e.g.,: Foreign National, Distinguished Visitor (DV), or VIP*] badge will be issued to the foreign national visitor (*assignee*). The visitor (*assignee*) will need to report to the Forrestal (*Germantown*) Building Visitors

Desk to receive his/her badge and to present USCIS documentation. *[Insert if applicable: A representative from (Insert Element) will meet the visitor (assignee) at the Forrestal Building Visitors Desk to greet the visitor (assignee), act as their escort, and assist with the badging process. The (Insert Element) escort must possess a DOE standard security badge.]*

6. Briefing of Foreign Visitor (*Assignee*): The foreign visitor (*assignee*) will be advised by the escort and host of the following:
 - *Prohibited areas*: The foreign national may not enter any DOE approved LA, VTR, or SCIF. The host or escort also will ensure the foreign national is not permitted access to areas processing classified information.
 - *Proper display of the DOE badge*: The foreign national must wear the issued DOE badge at all times while in HQ. The badge must be displayed above the waist and the front of the badge must be observable.
 - *Prohibited items*: The following items are prohibited in all HQ facilities: any dangerous weapons, explosives, other dangerous instruments or materials likely to produce substantial injury or damage to persons or property, alcoholic beverages and controlled substances.
 - *Controlled items*: Cameras, privately owned radios, tape players, pagers, calculators, compact disc players, electronic toys, cellular telephones, other electronic devices, and computer hardware and software will be prohibited from being introduced into an LA or VTR.
 - *Use of Audio or Video Recording Devices*: The use of cameras and audio or video recording devices by the foreign national is strictly prohibited while at HQ.

7. Escort Procedures: An escort is not required for this visitor (*assignee*). *Or insert the following if applicable:*

The (*Insert Element*) escort has completed the mandatory foreign national escort briefing before being assigned as an escort of a foreign national who will enter an LA or VTR, who has access to HQ during Security Hours, or for all High-Level Protocol visits.

The foreign visitor (*assignee*) will be accompanied at all times by the (*Insert Element*) escort. The escort must ensure that the visitor does not attempt to access any LA or VTR (*if applicable: other than the one identified in paragraph 1, above*), obtain classified or sensitive but unclassified matter or remove DOE property.

8. Computer Access: The foreign visitor (*assignee*) may not be given access to any DOE-owned computer equipment or remote access to any DOE computer system. In addition, the visitor will be prohibited from attaching a personal computer to a DOE network.

or, The assignee may be permitted to access to DOE unclassified computer equipment on an as-needed basis. Use has been coordinated with the Office of the Chief Information Officer, IM-622, (or insert the identity of the Element's Chief Information Officer) and a

specific computer security plan and procedures have been developed. The assignee may not bring any personally-owned computer hardware or software into any HQ facility.

9. Security Responsibilities: The *(Insert Element)* host is responsible for implementing this security plan and protecting DOE security interests during the visit *(assignment)* and to ensure that no classified or sensitive unclassified information is provided to the foreign visitor *(assignee)*. A copy of this plan will be provided to the host and any escorts, if applicable.
10. Closeout Information: Within 15 days of the completion of the meeting, the *(Insert Element)* host must send an e-mail to the elements Foreign Access Central Tracking System (FACTS) data entry person confirming that the visit *(assignment)* occurred or did not occur. The FACTS data entry person, in turn, will ensure that required closeout information is entered into FACTS.

It is recommended that this security plan be approved. I am available on *(Insert telephone number)* to answer any questions on this security plan.

APPROVED: _____

DISAPPROVED: _____

DATE: _____

cc: Headquarters Foreign Visit & Assignment Team
Host Name, Element
Escort Name, Element

ATTACHMENT 602-10

Security Reference Document

This reference document should be used in conjunction with Section 602 of the HQFMSP when planning an unclassified foreign visit/assignment to an HQ facility. This document does not apply to foreign visits or assignments involving:

- Access by the foreign national to an LA or VTR
- Discussion of sensitive information
- Discussion of sensitive subjects
- Any request involving a foreign national who was born in, a citizen of, employed by, or represents the government or an institution of a sensitive country or a country that is a state sponsor of terrorism.

For requests that fall within the above parameters, a Specific Security Plan must be developed and followed.

Below are the basic security measures for the protection of DOE classified and sensitive unclassified matter during the visit/assignment of foreign national to HQ. The following minimum security measures are implemented during the visit/assignment:

1. **Verification of Identity:** A representative from the sponsoring HQ element, with assistance from the protective force receptionists, verifies the visitor/assignee's passport, visa, and USCIS information and validates it in FACTS prior to granting access. Any USCIS information that was not previously received and inputted into FACTS must be provided by the sponsoring HQ element to their FACTS data entry person, and the information must be inputted by the end of the first day of the visit/assignment.
2. **Badging Procedures:** An HQ foreign national badge is to be issued for this visit/assignment. The visitor/assignee reports to the reception desk to receive his/her badge and must show his/her identification to the receptionist for identity verification.
3. **Briefing of Foreign Nationals:** The host and/or escorts advise the foreign national of the following:
 - *Proper display of the DOE badge:* The DOE badge must be worn at all times while in HQ and must be displayed above the waist and with the front of the badge facing away from the foreign national.
 - *Prohibited items:* The following items are prohibited in all HQ facilities: dangerous weapons, explosives, other dangerous instruments or materials likely to produce substantial injury or damage to persons or property, alcoholic beverages, and controlled substances.
 - *Use of Audio or Video Recording Devices:* The use of cameras, audio or video recording devices by the foreign national is strictly prohibited while at HQ.

4. Escort Procedures: Escorts are required for all foreign visitors/assignees to a HQ facility during Security Hours (see Section 106, Security Hours). Escorts are also required for all visitors/assignees entering an LA or VTR and for all High-Level Protocol visits. When an escort is required, the assigned escort must complete the Foreign National Visit and Assignment Escort Briefing prior to escorting any foreign nationals. This briefing needs to be completed only one time and need not be re-submitted for each visit/assignment.

Escorts must be DOE permanently badged U.S. citizens and must remain with the foreign visitor/assignee at all times. The escort ensures that the visitor does not attempt to access any LA or VTR, obtain classified or sensitive but unclassified matter, observe the processing of classified information, or remove DOE property.

5. Access to Sensitive Information: For the purposes of an FV&A to HQ, sensitive information includes OUO, UCNI, ECI, NNPI, PII, Company Proprietary Information, personnel files, and other forms of information related to a person's privacy. Escorts must ensure that the visitor/assignee does not attempt to obtain, copy, or otherwise access sensitive information. This includes preventing the foreign visitor/assignee from accessing desks drawers, filing cabinets, or other containers where such information could be located.
6. Computer Access: Foreign visitors are denied access to any DOE-owned computer equipment or remote access to any DOE computer system. Visitors are prohibited from attaching a personal computer to a DOE network. Use of removable electronic media, to include but not limited to flash drives, CDs, diskettes and mini hard drives, by the visitors or on their behalf is prohibited. When computer access is requested, the Office of the Chief Information Officer, IM-622 (*or insert the identity of the Element's Chief Information Officer*), must be notified. The date of the consultation/notification must be entered in FACTS. A separate computer security plan, provided by IM-622 (*or insert the identity of the Element's Chief Information Officer*), must be followed in addition to all other security requirements.
7. Security Responsibilities: The sponsoring hosts and escorts are responsible for following all security requirements and for protecting DOE security interests during the visit/assignment. The host or escort must ensure that no classified or sensitive unclassified information is provided to the foreign national and that the foreign national is not permitted access to areas processing classified information unless prior arrangements have been made and approval has been granted.
8. Closeout Information: Within 15 days of the completion of the visit/assignment, the sponsoring host must notify his/her FACTS data entry personnel confirming that the visit/assignment did or did not occur. The FACTS data entry personnel ensure that required closeout information is entered into the FACTS.

ATTACHMENT 602-11
Foreign Visits and Assignments Security Requirements Decision Matrix

	Approval Required		Type of Security Plan		FACTS Data Entry Required	Escort Required	Indices Check	Required Subject Matter Expert Reviews			
The Visitor/Assignee:	S-1	Head of Element (or designee)	Specific Security Plan	Review Security Reference Document				Security (includes OPSEC & TSCM)	Export Control/ Technology Transfer	Office of Intelligence	Computer Security
Will visit S-1	X				X	X					
High-Level Protocol Visit (Forrestal only)		X	X -- when office is in LA or VTR	X -- when office in non-security area	X	X					
Will enter an LA or VTR		X	X		X	X	X	X	X	X	
Will discuss a Sensitive Subject		X	X		X		X	X	X	X	
Will access Sensitive Information		X	X		X			X	X	X	
Will use a computer or access the HQ computer network		X	X		X						X
Is from a State Sponsor of Terrorism	X		X		X		X	X	X	X	
Is from a Sensitive Country		X	X		X		X	X	X	X	
Will do only maintenance, delivery, or vending				X		X					
Will attend a Public Event at HQ		X									
None of the above, Visitor		X		X	X						
None of the above, Assignment		X		X	X			X	X	X	X

ATTACHMENT 602-12

State Sponsor of Terrorism Package

The following information is provided to assist in preparing packages for visits and assignments to DOE facilities by foreign nationals from state sponsors of terrorism. This information is consistent with DOE Order 142.3, change 1, *Unclassified Foreign Visits and Assignments Program*, dated February 28, 2008.

A visit and/or assignment request for a foreign national from a state sponsor of terrorism must be fully documented and entered into FACTS by the hosting site. The requests must have the concurrence of Subject Matter Experts, as well as completed indices checks, prior to being approved by the approval authority for the hosting site. Approval determination will be made based on the extraordinary nature of the potential visit/assignment (i.e., the desired outcome of the visit/assignment by the foreign national would be impossible to achieve through any other means).

Once the DOE facility requesting a visit/assignment for a foreign national from a state sponsor of terrorism has assembled a completed package, they must forward this package to their HQ Program Secretarial Office (PSO). The PSO will then review the package and, if supported, forward it to the Office of Intelligence and Counterintelligence (IN-20) for further review and final approval determination by the Secretary of Energy or the cognizant Under Secretary.

Package contents:

1. Approval Request. This document represents the pertinent information that needs to be provided by the DOE facility regarding the foreign national who will be visiting or assigned to the facility, along with the certification of the site approval authority.
2. Subject Matter Expert Certifications
3. Cyber Security Plan (if computer access is requested)
4. Specific Security Plan
5. Copies of Immigrant/Nonimmigrant Status Documentation and Passport (or other government-issued photo identification document if passport not required)
6. Copy of FACTS request
7. Additional/Miscellaneous Information - Optional (Curriculum Vitae, list of publications, other supporting documentation, etc.)

SAMPLE

**APPROVAL REQUEST FOR A VISIT/ASSIGNMENT BY A FOREIGN NATIONAL
FROM A STATE SPONSOR OF TERRORISM**

Date:

To: Director
Office of Security Assistance, AU-42

From: Site Requesting the Visit/Assignments

Subject: Approval of a Foreign National from a Country Identified as a State
Sponsor of Terrorism

FACTS REQUEST#: _____
Visitor # _____

_____ Visit
_____ Assignment
_____ Extension of Assignment
(Please Check one)

1. Visitor Name:
2. Start and End Dates:
3. DOE Facility to be Visited/Assigned to:
4. Purpose: (Include Technologies to be accessed and whether or not Sensitive Subjects will be discussed)
5. Justification for Visit/Assignment: (Approval determination will be made based on the extraordinary nature of the potential visit/assignment, i.e., the desired outcome of the visit/assignment by the foreign national would be impossible to achieve through any other means)
6. Benefit and Impact (to DOE): (How will DOE benefit from having this Foreign National at it site?)
7. Site Point of Contact:
8. International Agreement Involved: Y/N (If yes, list agreement)
9. Date of Birth:
Country of Birth:
Country of Citizenship:
10. Date of Last Visit to Place of Birth:

11. Country of Current Residence:
12. How Long at Current Residence:
13. Status:
_____ Immigrant Alien
_____ Lawful Permanent Resident
_____ Other

(Documentation to include INS number)

Passport Number:
Passport Expiration date:
Country of Issuance:

Status Number:
Status Expiration date:
Immigrant/Nonimmigrant Status:

14. Indices Check Completed*:
_____ Yes _____ No
15. Date of Completed IC:
16. Date of IC Expiration:

***If Indices Checks are not completed, packages will not be processed until Indices Checks are completed, and documented, in FACTS. Counterintelligence Consultations will not be accepted in lieu of the completion of indices checks for Terrorist Supporting Country packages.**

17. Current Employer: (Include Name, Address, Phone Number, and Location)
18. Length of Service with current Employer:
19. DOE Host: (Name and Telephone Number)
20. Site Host's Organization and Telephone Number:

Sample

SITE APPROVAL AUTHORITY CERTIFICATION

I certify that I have reviewed the request for access approval for *Foreign National Visitor Name*, FACTS Visitor #11111, Request #AAA111111111, and considered all the sensitivity factors associated with the requested access to DOE sites, programs, information and technologies. I have reviewed the advice provided by the Subject Matters Experts in Security, Cyber Security, OPSEC, Export Control and Counterintelligence, and have addressed any concerns to the satisfaction of the Subject Matter Expert involved. My determination is consistent with reasonable standards and practices used to ensure risk to the Government associated with access approval is appropriately identified and evaluated.

Additionally, I certify that any approval certifies that, in my opinion, the benefits to the Government are greater than the risks associated with the presence of the foreign national and that the legal and policy-related terms and conditions associated with the proposed *Visit/Assignment* have been met. These terms and conditions include, but are not limited to, other activities at this site, visa sponsorship requirements, visa status conditions and requirements, right-to-work requirements, and international agreements.

Requesting Facility:

Approving Official:
Signature:

Title:
Date:

Sample

SUBJECT MATTER EXPERT CERTIFICATION

Counterintelligence

The Subject Matter Expert (SME) has reviewed the request for access approval for *Foreign National Visitor Name*, FACTS Visitor #11111, Request #AAA1111111111, and considered all the sensitivity factors associated with the requested access to DOE sites, programs, information, and technologies, including building access and surrounding activities. I have provided advice to the approval authority regarding this request, that he/she acknowledged receiving my advice, has addressed any concerns to my satisfaction. My review was consistent with the reasonable standards and practices used to ensure risk to the Government associated with access approval is appropriately identified and evaluated.

John Doe
Name

Signature and Date

Sample

SUBJECT MATTER EXPERT CERTIFICATION

Security

The Subject Matter Expert (SME) has reviewed the request for access approval for *Foreign National Visitor Name*, FACTS Visitor #11111, Request #AAA1111111111, and considered all the sensitivity factors associated with the requested access to DOE sites, programs, information, and technologies, including building access and surrounding activities. I have provided advice to the approval authority regarding this request, that he/she acknowledged receiving my advice, has addressed any concerns to my satisfaction. My review was consistent with the reasonable standards and practices used to ensure risk to the Government associated with access approval is appropriately identified and evaluated.

John Doe
Name

Signature and Date

Sample

SUBJECT MATTER EXPERT CERTIFICATION

Export Control

The Subject Matter Expert (SME) has reviewed the request for access approval for *Foreign National Visitor Name*, FACTS Visitor #11111, Request #AAA1111111111, and considered all the sensitivity factors associated with the requested access to DOE sites, programs, information, and technologies, including building access and surrounding activities. I have provided advice to the approval authority regarding this request, that he/she acknowledged receiving my advice, has addressed any concerns to my satisfaction. My review was consistent with the reasonable standards and practices used to ensure risk to the Government associated with access approval is appropriately identified and evaluated.

John Doe
Name

Signature and Date

Sample

SUBJECT MATTER EXPERT CERTIFICATION

Technology Transfer

The Subject Matter Expert (SME) has reviewed the request for access approval for *Foreign National Visitor Name*, FACTS Visitor #11111, Request #AAA1111111111, and considered all the sensitivity factors associated with the requested access to DOE sites, programs, information, and technologies, including building access and surrounding activities. I have provided advice to the approval authority regarding this request, that he/she acknowledged receiving my advice, has addressed any concerns to my satisfaction. My review was consistent with the reasonable standards and practices used to ensure risk to the Government associated with access approval is appropriately identified and evaluated.

John Doe
Name

Signature and Date

Sample

SUBJECT MATTER EXPERT CERTIFICATION

OPSEC

The Subject Matter Expert (SME) has reviewed the request for access approval for *Foreign National Visitor Name*, FACTS Visitor #11111, Request #AAA1111111111, and considered all the sensitivity factors associated with the requested access to DOE sites, programs, information, and technologies, including building access and surrounding activities. I have provided advice to the approval authority regarding this request, that he/she acknowledged receiving my advice, has addressed any concerns to my satisfaction. My review was consistent with the reasonable standards and practices used to ensure risk to the Government associated with access approval is appropriately identified and evaluated.

John Doe

Name

Signature and Date

Sample

SUBJECT MATTER EXPERT CERTIFICATION

Cyber Security

The Subject Matter Expert (SME) has reviewed the request for access approval for *Foreign National Visitor Name*, FACTS Visitor #11111, Request #AAA1111111111, and considered all the sensitivity factors associated with the requested access to DOE sites, programs, information, and technologies, including building access and surrounding activities. I have provided advice to the approval authority regarding this request, that he/she acknowledged receiving my advice, has addressed any concerns to my satisfaction. My review was consistent with the reasonable standards and practices used to ensure risk to the Government associated with access approval is appropriately identified and evaluated.

John Doe
Name

Signature and Date

SUBJECT MATTER EXPERT CERTIFICATIONS
(Sample – All reviews on one page)

The Subject Matter Expert (SME) states that they have reviewed the request for access approval for *Foreign National Visitor*, FACTS Visitor #11111, Request #AAA1111111111, and considered all the sensitivity factors associated with the requested access to DOE sites, programs, information, and technologies, including building access and surrounding activities. I have provided advice to the approval authority regarding this request, that he/she acknowledged receiving my advice, has addressed any concerns to my satisfaction. My review was consistent with the reasonable standards and practices used to ensure risk to the Government associated with access approval is appropriately identified and evaluated.

Subject Matter Expert Reviews:

Counterintelligence

John Doe
Name

Signature and Date

Security

Jane Doe
Name

Signature and Date

Foreign Intelligence

John Doe
Name

Signature and Date

And etc., for Cyber Security, Export Control, OPSEC and Technology Transfer, as required.

Specific Security Plan Sample 1

Full Name:

Citizenship:

Place of Birth:

Employer/Affiliation: University of Southern California

FACTS Visitor Number: 111111

FACTS Request Number: AZY2008212432

Dates of Assignment: June 1, 2008 to October 15, 2009

1. References:

- A. Thompson National Laboratory Director's Memorandum, Subject: Sensitive Subjects Review dated March 31, 2004.
- B. Thompson National Laboratory Procedure 4231, Thompson National Laboratory Procedure for Processing Foreign National Visits and Assignments, dated November 4, 2006.
- C. DOE O 142.3, Unclassified Foreign Visits and Assignments Program, dated June 18, 2004.

2. Immigration Status:

Non-immigrant

2a. Passport Information:

Passport Number: J21232121

Issuing Country:

Expiration Date: May 1, 2014

2b. Visa Information:

Visa Number: L1243211234355

Visa Type: F-1 Student Visa

Expiration Date: June 15, 2010

3. Assignment Information:

a. Foreign National Title or Expertise: Doctoral Student

b. On-site Location/Phone Number: Building 94, Electrical Engineering Research, Room 321, phone 555-555-5555

4. Purpose of the Assignment:

_____(Name) is currently a PhD student in the Electrical Engineering Department of the University of Southern California working under the supervision of Professor Susan Jones. Mr. _____ has unique expertise in manipulation and trapping of ultra-small objects such as metallic nanoparticles, polystyrene beads, and cells using the optoelectronic tweezers (OET) method. The goal of the proposed collaboration is to explore the potential of combining OET with “plasmonic” effects for particle trapping and assembly of optoelectronics devices. “Plasmonics” has emerged as an area in the optoelectronics field due to its promise of high-speed information processing using optical fields confined to nanometer length scales. The applications of plasmonics in fields such as optical interconnects, single-molecule imaging, and spectroscopy will prove to be groundbreaking and far-reaching. Because of their extremely small and intricate designs, only recently have plasmonic structures and devices been realized experimentally. The Thompson National Laboratory Electrical Engineering Department was one of the first to design, fabricate, and characterize one class of such devices, plasmonic nanoantennas.

5. Justification

To the best of our knowledge, Mr. _____ is the only individual possessing the skills and ability to use OET to trap plasmonically-active nanoparticles less than 100 nm in diameter – skills required to meeting our scientific goal mentioned above. Mr. _____ will be working under the supervision of Dr. Thomas Smith, head of the Thompson Lab Electrical Engineering Department, to study the potential of plasmonics for trapping and fabrication of optoelectronic devices. For example, OET is capable of trapping individual semiconductor and metallic nanowires, which is important since nanowires are, in many ways, ideal fundamental building blocks for these devices. By combining OET with plasmonic nanoantennas, trapping resolution as well as optical characterization of the nanowires can be improved down to the nanometer length scales.

1500 – Nano-technology and Fabrication
3232 – Spectroscopy

6. Sensitive Subjects:

Thompson National Laboratory conducts work and possesses information that require additional security measures beyond that of published fundamental research. There are laws and procedures in place to protect this information, and we are committed to adhering to these requirements. The Sensitive Subjects Review Group provides ongoing oversight related to information or activities requiring additional controls.

7. Initial Verification and Access Procedures (Badging):

The assignee will report to the Thompson National Laboratory Site Access Office for identification and access processing. In accordance with the Thompson National Laboratory Site Security Plan, badges will be issued and worn in areas designated in the plan. Card access will be granted only to those areas authorized with the Local Security Access Manager. Badges for

foreign nationals will have an expiration date that is either the end date of the assignment at Thompson Lab or the visa expiration date, whichever is sooner.

8. Areas to be Accessed:

Building 94, Electrical Engineering Research

Building 95, Electrical Engineering Research

Building 32, Thompson National Laboratory Meeting Facility

Building 2, Cafeteria

9. Additional Security Safeguards:

10. Briefing of Foreign National Assignee:

New Employee Orientation: This briefing includes requirements for Cyber and Physical Security, as well as emergency procedures.

11. Foreign Assignee Escorts and Procedures:

Whatever your site escort procedures are

Specific Security Plan Sample 2

Full Name:

Citizenship:

Place of Birth:

Employer/Affiliation: University of Southern California

FACTS Visitor Number: 111111

FACTS Request Number: AZY2008212432

Dates of Assignment: June 1, 2008 to October 15, 2009

Sponsoring Department/Division: Electrical Engineering Department

Host Responsible for the Assignment: Thomas Smith

Host Phone Number: 555-555-5555

Description of Assignment: _____ (*Name*) is currently a PhD student in the Electrical Engineering Department of the University of Southern California working under the supervision of Professor Susan Jones. Mr. _____ has unique expertise in manipulation and trapping of ultra-small objects such as metallic nanoparticles, polystyrene beads, and cells using the optoelectronic tweezers (OET) method. The goal of the proposed collaboration is to explore the potential of combining OET with “plasmonic” effects for particle trapping and assembly of optoelectronics devices. “Plasmonics” has emerged as an area in the optoelectronics field due to its promise of high-speed information processing using optical fields confined to nanometer length scales. The applications of plasmonics in fields such as optical interconnects, single-molecule imaging, and spectroscopy will prove to be groundbreaking and far-reaching. Because of their extremely small and intricate designs, only recently have plasmonic structures and devices been realized experimentally. The Thompson National Laboratory Electrical Engineering Department was one of the first to design, fabricate, and characterize one class of such devices, plasmonic nanoantennas.

Mr. _____ will be working under the supervision of Dr. Thomas Smith, head of the Thompson Lab Electrical Engineering Department, to study the potential of plasmonics for trapping and fabrication of optoelectronic devices. For example, OET is capable of trapping individual semiconductor and metallic nanowires, which is important since nanowires are, in many ways, ideal fundamental building blocks for these devices. By combining OET with plasmonic nanoantennas, trapping resolution as well as optical characterization of the nanowires can be improved down to the nanometer length scales.

Buildings and Rooms to be Accessed:

Building 94, Electrical Engineering Research, Rooms 232, 233, 234, 237

Building 95, Electrical Engineering Research, Rooms 109, 110

In addition, the foreign national may have access to the cafeteria, open meeting rooms, the Research Library and recreational facilities.

The Host identified above will ensure the following:

I. This assignment will involve access only to unclassified, non-sensitive, government information. There will be no access by the foreign national to any security area, including Property Protection Areas, unless specified in this Specific Security Plan. There will be no access to Export Control Information.

II. Any deviations to the planned scope of this assignment that result in an incident of security concern involving credible information that foreign national or an agent of a foreign power is involved will be reported to the Thompson National Laboratory (TNL) Security Office or the Office of Counterintelligence in accordance with current DOE requirements. Security incidents having any association with foreign nationals will be clearly identified and reported on the initial DOE F 471.1.

III. The foreign national will be instructed during the check-in process on the access and security requirements at BNL. The foreign national will be issued a guest badge and vehicle registration, if applicable. The badge will be scanned upon entry at the Main Gate and the badge expiration date will correspond to the expiration date of the foreign national's immigrant/nonimmigrant status or the end date of the assignment, whichever comes first. Computer access will only be allowed to the systems identified in the Cyber Security Plan for nationals of state sponsors of terrorism. Upon termination, all Laboratory credentials, keys, and other issued TNL equipment will be collected by the hosting Department, and the Information Technology Department will be notified to terminate computer access.

IV. Additional Provisions: This is an assignment request for a national of a state sponsor of terrorism. Site access will not be granted until final approval by the Secretary of Energy as been received.

Operational Security Plan**1. Verification**

The foreign national's identity and immigrant/nonimmigrant status is verified at the time of arrival.

2. Badging

The foreign national will be issued a photo ID badge, and will be required to possess and display the badge while on the Laboratory site.

3. Transportation on-site

The foreign national will use vehicular and foot modes of transportation.

4. Role of Host

- The Host will ensure that the assignee understands his responsibilities and limitations on the assignment.
- The Host will ensure compliance with required training, including safety.
- The Host will ensure that the assignee is issued a TNL identification badge, and will advise the assignee that it must be worn photo side out above the waist at all times while the assignee is on-site.
- The host will retain information on the assignee's residence, phone number, and person to be notified in the event of emergency.
- The host will ensure the return of the TNL ID badge upon completion of the assignment. The host will advise the assignee as to any restrictions regarding use of communications, telephones, computers, and facsimiles if any exist. There are no areas within the foreign national's assigned buildings identified as sensitive or classified.
- The Host will be vigilant about discussions with foreign nationals that could divulge proprietary details concerning the work to be completed.
- The host will inform employees in the work area about this assignment and remind them to deflect inquiries that attempt to seek information not appropriate to the assignment, to include personal information, other personnel, or government programs. Such inquiries and any close and continuing contact will be reported to the TNL Counterintelligence Officer.

5. Cyber Access

See attached Cyber Security Plan.

6. Role of Escort

The assignee will not require access to any areas requiring an escort during Non-Security Hours. In the event an escort becomes necessary, the host or an appropriate designee will work with the foreign national to ensure the established requirements of an escort are maintained. The assignment will not include access to sensitive facilities, sensitive subjects, LAs or VTRs.

7. Laboratory Security Officers

Laboratory security will be notified when the assignee arrives on-site at TNL, and will be advised of his workstation location.

8. Designation of Specific Buildings/Facilities

Building 94, Electrical Engineering Research

Building 95, Electrical Engineering Research

In addition, the foreign national may have access to the cafeteria, open meeting rooms, the Research Library and recreational facilities

9. Classified Activities

Classified activities will not be accessible to the assignee. There is no need to suspend ongoing classified site activities.

10. Briefing of Foreign National Regarding Rules of Conduct

This briefing is carried out during orientation.

11. Access to Site Outside Normal Business Hours

After normal business hours, the assignee will be granted access to the cafeteria, open meeting rooms, the Research Library and recreational facilities. The assignee must be accompanied by the Host or a designed escort in order to access Buildings 94 and 95 after normal business hours.

12. Briefing of All Personnel Who Will Be Involved with the Assignee

The assignment does not involve a sensitive subject area, and the assignee's building is not a security facility. The Host will inform employees in the work area about this assignment, and will remind them to deflect inquiries that attempt to seek information not appropriate to the assignment, to include personal information, other personnel, or government programs. Such inquiries, and any close and continuing contact, will be report to the TNL Counterintelligence Officer.

Section 603

Foreign Travel

Official or personal travel by DOE Federal or contractor personnel raises potential counterintelligence, security, and or personal welfare concerns. This section identifies some of those concerns and discusses DOE foreign travel requirements and procedures.

The Office of International Travel and Exchange Visitor Program (MA-45) is responsible for managing the process for obtaining DOE approval for DOE HQ employees performing official travel to foreign countries.

IN-20 is responsible for reviewing proposed sensitive travel and assessing the potential threat to the traveler and or to DOE security interests.

HQ Implementation Procedures

Official Foreign Travel:

Any proposed official foreign travel must be approved through normal supervisory channels before travel may commence. The approval process requires the entry of all official travel data into the Department's Foreign Travel Management System (FTMS) and securing country clearance (refer to DOE Order 551.1C, *Official Foreign Travel*, for process and time requirements). The traveler is responsible for ensuring that travel requests are initiated in a timely manner and entered into FTMS. All HQ elements should have FTMS-trained personnel to enter foreign trips into the system. FTMS training can be obtained by contacting the FTMS Program Manager, MA-45.

Official Travel to Sensitive Countries or to Discuss Sensitive Topics:

Sensitive official travel is travel to a foreign country included on the current Sensitive Countries List or travel to a country where sensitive topics will be discussed. A copy of the list may be obtained from IN-20. FTMS automatically notifies IN-20 of the proposed travel, and that office assesses the potential threat to the traveler and to DOE security interests.

Unofficial Foreign Travel by Cleared Employees:

DOE Federal and contractor employees holding a Q or L security clearance are encouraged to report planned personal foreign travel to sensitive countries to their HSO and to review appropriate security and counterintelligence briefing material. The HSO, in turn, refers the traveler to a servicing Counterintelligence Officer for threats or other information useful to the traveler.

Travel to Sensitive Countries by Formerly Cleared DOE Federal and Contractor Employees:

Former DOE Federal and contractor employees who have held a DOE security clearance within the last 5 years may request a defensive counterintelligence briefing from IN-20. The former employee can contact IN-20 through the telephone numbers shown in the Points of Contact subsection, below.

Required Briefings:

All HQ travelers scheduled or proposed for official sensitive travel (sensitive country or sensitive topics involved) must be informed of the security and counterintelligence concerns related to their travel. These travelers are required to consult IN-20 before departure to complete a defensive counterintelligence briefing and may be required to complete a counterintelligence debriefing upon return. IN-20 advises the traveler on their debriefing requirements.

Recommended Briefings:

Although not required, it is recommended that all DOE Federal and contractor employees undertaking official or personal foreign travel refer to the State Department website and review the most current country guidance for their destination. For example, travel warnings, travel alerts, and country specific foreign travel advisories, are accessible through the State Department web page identified at the end of this section. A foreign travel advisory provides valuable advice and enables the traveler to avoid common risks, improve their personal safety, protect sensitive information, and enhance their overall enjoyment of foreign travel. HSOs may refer travelers within their organization to the Foreign Travel Advisory web page for more information about the selected destination.

In addition, any traveler may contact IN-20 for more detailed information about current foreign travel restrictions, warnings, or other matters of security concern.

Points of Contact

For information about the FTMS, call (202) 586-4048.

For Forrestal Counterintelligence Officer support, call (202) 586-1378 or (202) 586-8592.

For Germantown Counterintelligence Officer support, call (301) 903-0434.

Forms/Samples/Graphics

Sensitive Countries List (this document is OUO and available from IN-20)

Helpful Website

<https://in.doe.gov/>

This page intentionally left blank.

Chapter 7 Revision History: Revisions by date (Newest to oldest):

March 4, 2020: Revised entire document

January 8, 2019: Revised entire document

April 16, 2018: Added the root cause analysis tool

This page intentionally blank.

Chapter 7 Department of Energy Headquarters Safeguards and Security Survey Program

PURPOSE

The purpose of this chapter is to describe the responsibilities, requirements and methodology for the implementation of the Safeguards and Security (S&S) Survey Program at Department of Energy (DOE) Headquarters (HQ) in accordance with DOE Order 470.4B, Chg. 2, *Safeguards and Security Program, Appendix A, Section 2, Survey, Review, and Self-Assessment Programs*, requirements. The S&S Survey Program documents the required evaluation of DOE HQ S&S programs, identifies strengths and weaknesses, and provides for timely identification and correction of program deficiencies and noncompliant conditions for the purpose of preventing adverse events and improving the overall S&S posture of DOE HQ.

The S&S Survey Program provides assurance to the Secretary of Energy, Departmental Elements, and other government agencies (OGAs) that DOE S&S interests and activities are protected at the required levels. These programs also provide a basis for line management to make decisions regarding S&S program activities, including the allocation of resources, acceptance of risk, and mitigation of vulnerabilities.

PROGRAM DESCRIPTION

RESPONSIBILITIES

The DOE Office of Headquarters Security Operations (AU-40) Director, as the Officially Designated Federal Security Authority (ODFSA) and the Cognizant Security Authority for DOE HQ, is responsible for oversight of the S&S Survey Program.

The Office of Information Security (AU-42) is responsible for maintaining an S&S Survey Team and conducting all S&S surveys of Departmental Elements.

The S&S Survey Team is comprised of the following:

Survey Program Manager – The Survey Program Manager is responsible for leading and participating as a member of the S&S Survey Team. The Survey Program Manager provides oversight and management of each security survey, which includes the development of survey criteria, data collection, analysis, in-briefing, out-briefing, final reporting, recommendations, tracking findings, and trending analysis based on the survey results.

Survey Team Lead – The Survey Team Lead is responsible for the overall conduct of the survey, ensuring that the topical areas of the S&S program are reviewed and that any findings or deficiencies identified are fully supported by documentation and validated data.

Survey Team Members – The Survey Team Members have hands-on access to the information to be reviewed, interview appropriate personnel to determine knowledge levels and compliance, and help with performance testing.

SURVEY SCHEDULE

AU-42 coordinates and develops an annual survey schedule of Departmental Elements based on planned DOE HQ operations. However, the survey schedule may be adjusted based on unplanned changes to DOE operations.

TYPES OF SURVEYS

Surveys and special reviews are conducted by the S&S Survey Team to confirm that a Federal, or contractor facility meets all security requirements appropriate to the activities conducted at the respective facility.

The AU-42 S&S Survey Team performs the following types of surveys:

- S&S Initial Surveys (SSISs) are required as one of the conditions for granting a facility clearance (FCL). SSISs are conducted to determine whether facilities in question meet established standards for the protection of the security interests and activities covered by the FCL. SSISs will be completed not more than six months prior to the granting of an FCL. (DOE O 470.4B Chg.2 App. A, Sect. 2. 5.b & 6.a.)
- S&S Periodic Surveys (SSPSs) are conducted for facilities with an approved FCL to ensure the satisfactory protection and control of DOE security assets and interests. (DOE O 470.4B Chg.2 App. A, Sect. 2. 6.b.) The S&S Survey Team conducts SSPSs on an annual basis. (DOE F 470.8, Survey/Inspection Report Form).
- S&S Termination Surveys (SSTSs) are conducted to confirm that all S&S activities have been terminated, that access authorizations have been properly terminated or dispositioned, and/or that no DOE property or classified information/matter remains within the facility. (DOE O 470.4B Chg.2 App. A, Sect. 2. 5.b. & 6.c.)
- Although no longer referenced in the DOE O 470.4B, occasionally Special Surveys (SPECs), or special reviews, may be conducted as directed by the AU-40 Director or at the request of other AU line management.

TOPICAL AREAS

The S&S Survey Team will conduct surveys of Departmental Elements and evaluate them against the following six topical areas identified on DOE Form 470.8. The S&S Survey Team will also use past surveys/inspections, incidents, infractions, and findings to identify areas of special emphasis for upcoming surveys. (DOE O 470.4B Chg.2 App. A, Sect. 2. 9.a.)

The six topical areas include:

- Program Management Operations
- Physical Security
- Information Security; including Classified Matter Protection and Control (CMPC) and Operational Security (OPSEC)
- Personnel Security
- Unclassified Foreign Visits and Assignments

- Protective Force

SURVEY METHODOLOGY

COORDINATION AND PREPARATION

The S&S Survey Team Lead will contact the Departmental Element point of contact (POC) to coordinate the survey dates and activities. The Departmental Element POC is responsible for coordinating survey activities within the element to ensure that the S&S Survey Team are provided access to necessary information and personnel. The Departmental Element POC is also responsible for establishing meeting spaces for the S&S Team to utilize for their in-briefing, and other security activities.

The S&S Survey Team will develop Lines of Inquiries (LOIs), or requirements, based off of the memorandum from then Deputy Secretary Dan Brouillette, *Headquarters Facilities Master Security Plan and Headquarters Security Officer Program*, dated November 9, 2018, (S-2 Memo), relevant chapters of the HQFMSP, and DOE S&S Orders for each topical area they will review. The S&S Survey Team will use the LOIs as a benchmark when surveying Departmental Elements.

NOTIFICATION AND DATA CALL

The S&S Survey Team will formally notify the Departmental Element of the upcoming survey. This notification will identify what is to be surveyed, dates of the survey, the process of the survey, as well as the information that will be requested (data call). Prior to the commencement of an S&S Survey, the Survey Team will request the assessed Departmental Element provide records and documents for review of their S&S program(s). This request will be sent prior to the planned survey via official correspondence. Submitted data should arrive to the S&S Survey Team by the date specified in the correspondence. Reviewing requested documentation prior to the S&S Survey Team's arrival will help reduce the overall operational impact and required completion time for the survey.

SCHEDULE AND TIMELINE OF EVENTS DEVELOPMENT

During the data call and review, the S&S Survey Team will develop a survey schedule based on the LOIs and will coordinate the schedule with the Departmental Element POC. This coordination ensures an efficient use of time and reduces production impact to the surveyed element.

IN-BRIEFING

Prior to initiating survey activities, the S&S Survey Team will conduct an in-briefing for the surveyed Departmental Element. The Departmental Element POC may invite any member of their element for the in-briefing. The purpose of the in-briefing is to discuss the intent of the survey, review the planned activities (i.e., scope, LOIs, personnel interviews, etc.) and initiate the survey activities.

SURVEY CONDUCT

The S&S Survey Team verifies, by evaluation of objective evidence, whether applicable S&S program topical areas are being implemented by the Departmental Element in compliance with DOE requirements.

During the course of performing surveys, the S&S Survey Team will:

- Review the LOIs and interview the POCs on their roles and responsibilities;
- Immediately report any conflicts or difficulties with individual(s) being surveyed to the Survey Program Manager or designee;
- Report any conditions requiring prompt corrective action to the Departmental Element's POC, Survey Team Lead, and the Survey Program Manager or designee;
- Identify and document findings including repetitive or programmatic issues of noncompliance;
- Record/document assessment results in a manner that facilitates expeditious completion of the survey report;
- Investigate an observed deficiency; and,
- Assign topical area/sub-topical area ratings in accordance with DOE F 470.8 (see attachment 7-1) based upon survey results.

NOTE: If the S&S Survey Team makes a determination that a security interest is at risk, they will cease operations, make all necessary notifications, and take necessary steps to safeguard and secure the security interest.

RECOMMENDATIONS AND FINDINGS

As part of the survey report, the S&S Survey Team may come across processes or performance matters that the surveyed Departmental Element needs to address.

Recommendations: An opinion-based statement submitted by the S&S Survey Team to identify ways in which the safeguard and security topical area might be improved. The recommendation can be linked to a requirement but does not identify a failure to meet the requirement.

Finding: A finding is a factual statement of a failure to meet a documented legal, regulatory, performance, compliance, or other applicable requirement in the S&S program. If left uncorrected, a finding has the potential to result in near-term significant adverse consequences to the health, safety, or security of personnel or property, or the achievement of the mission. When findings are issued, they are assigned to the specific Departmental Element where the deficiency was identified. The S&S Survey Team will write all findings in a manner that will allow them to be corrected.

OUT-BRIEFING

The S&S Survey Team will conduct an out-briefing with the Departmental Element's POC and their management to discuss the results of the survey, including any identified findings. Any logistical arrangements will be coordinated through the Departmental Element POC to conduct the out-briefing.

REPORT DEVELOPMENT

Reports will describe what the S&S Survey Team assessed, what was observed, and what was identified as not in compliance with all applicable DOE policy.

The draft report will be sent from the Director, AU-42 or designee to the Departmental Element POC to conduct a factual accuracy review of the draft report. The surveyed Departmental Element will be given a specified timeframe by the S&S Survey Team to respond with comments. If responses/comments are not received within the specified timeframe, the report will be finalized as is. Disagreements during the factual accuracy review should be mutually resolved between the S&S Survey Program Manager and the surveyed Departmental Element POC.

FINAL REPORT

The S&S Survey Team will publish the final report after the factual accuracy review. The final survey report will be sent from the AU-42 Director or designee to the Departmental Element POC.

ENTERING SURVEY DATA INTO SSIMS

All final survey reports must have the completed and approved DOE F 470.8, *Survey/Inspection Form*, and findings entered into Safeguards & Security Information Management System (SSIMS). All surveys must provide ratings for topical and sub-topical areas reviewed and designate an overall composite rating. The definitions of the ratings, as defined in DOE O 470.4B are:

- Satisfactory - Indicates the Departmental Element evaluated by the S&S Survey Team meets protection objectives or provides reasonable assurance that protection objectives were being met at the time of the survey.
- Marginal - Indicates the Departmental Element evaluated by the S&S Survey Team partially meets protection objectives or provides questionable assurance that protection objectives were being met at the time of the survey.
- Unsatisfactory - Indicates the Departmental Element evaluated by the S&S Survey Team does not meet protection objectives or does not provide adequate assurance that protection objectives were being met at the time of the survey.

CORRECTIVE ACTION PLAN

A corrective action plan (CAP) must be developed and implemented in a timely and effective manner for all findings identified in S&S surveys. CAPs are required to be developed within 30 days of issuance of the final survey report and must include a determination of the causal analysis of findings and milestone sheets if steps are required to address findings. The CAP is required to be approved and signed by the Departmental Element's management. Final CAPs are forwarded to the S&S Survey Program Manager for entry into SSIMS. The S&S Survey Team will then monitor all findings and the status of the CAP until all items have been completed.

Once the surveyed Departmental Element has completed a CAP item or milestone, the surveyed Departmental Element POC will contact the S&S Survey Team to conduct a validation of the actions taken and ensure the security issue has been resolved. The S&S Survey Team will document CAP closures in SSIMS.

SURVEY NOTES AND DOCUMENTATION

The S&S Survey Team will scan all survey notes and retain all records in accordance with DOE requirements. (DOE O 470.4B Chg.2 App. A, Sect. 2. 10.) All documentation from surveys will be retained as historical documentation.

Point of Contact

Contact the S&S Survey Team with any questions regarding this Chapter at (301) 903-0213.

References

DOE Order 470.4B, Change 2, *Safeguards and Security Program, Appendix A, Section 2, Survey, Review, and Self-Assessment Programs*

Headquarters Facility Master Security Plan

S-2 Memorandum, dated November 9, 2018, subject: *Headquarters Facilities Master Security Plan and Headquarters Security Officer Program*

Forms/Samples/Graphics

DOE F 470.8, *Survey/Inspection Report Form* (Attachment 7-1)

Corrective Action Plan Sheet (Attachment 7-2)

Instructions for Completing a Corrective Action Plan Sheet (Attachment 7-3)

Corrective Action Plan Milestone Sheet (Attachment 7-4)

Instructions for Completing a Corrective Action Plan Milestone Sheet (Attachment 7-5)

Corrective Action Validation Report (Attachment 7-6)

This page intentionally blank.

ATTACHMENT 7-1

U.S. Department of Energy

SURVEY / INSPECTION REPORT FORM

1. Survey Type: ☐ Initial ☐ Periodic ☐ Special ☐ Termination ☐ EPR ☐ NPR ☐ OA		3. Report #:	
3. Facility Name:		4. a. Facility Code:	
		b. RIS Code: -	
5. Survey Date(s):	6. a. Findings: ☐ Yes ☐ No	7. Composite Rating:	
	b. Findings Against Other Facilities:		
8. Previous Survey Date(s):	9. Unresolved Findings: ☐ Yes ☐ No	10. Previous Rating:	
11a. Surveying Office:	11b. Cognizant Security Office:	11c. Other Offices with Interests:	
12. Ratings:			
a) PROGRAM MANAGEMENT AND SUPPORT PROTECTION PROGRAM MANAGEMENT _____ Program Management and Administration _____ Resources and Budgeting _____ Personnel Development and Training _____ S&S PLANNING AND PROCEDURES _____ MANAGEMENT CONTROL _____ Surveys and Self Assessment Programs _____ Performance Assurance Program _____ Resolution of Findings _____ Incident Reporting and Management _____ PROGRAM WIDE SUPPORT _____ Facility Approval and Registration of Activities _____ Foreign Ownership, Control or Influence _____ Security Management in Contracting _____ OVERALL RATING _____		e) CYBER SECURITY CLASSIFIED CYBER SECURITY _____ Leadership, Responsibilities and Authorities _____ C&A, Risk Management & Planning _____ Policy, Guidance and Procedures _____ Technical Implementation _____ Performance Eval Feedback & Continuous Improvement _____ TELECOMMUNICATIONS SECURITY _____ UNCLASSIFIED CYBER SECURITY _____ Leadership, Responsibilities and Authorities _____ C&A Risk Management and Planning _____ Policy, Guidance and Procedures _____ Technical Implementation _____ Performance Eval Feedback & Continuous Improvement _____ OVERALL RATING _____	
b) PROTECTIVE FORCE MANAGEMENT _____ TRAINING _____ DUTIES _____ FACILITIES AND EQUIPMENT _____ OVERALL RATING _____		f) PERSONNEL SECURITY PROGRAM ACCESS AUTHORIZATIONS _____ HUMAN RELIABILITY PROGRAM _____ CONTROL OF CLASSIFIED VISITS _____ SAFEGUARDS AND SECURITY AWARENESS _____ OVERALL RATING _____	
c) PHYSICAL SECURITY ACCESS CONTROLS _____ INTRUSION DETECTION & ASSESSMENT SYSTEMS _____ BARRIERS AND DELAY MECHANISMS _____ TESTING AND MAINTENANCE _____ COMMUNICATIONS _____ OVERALL RATING _____		g) UNCLASSIFIED VISITS & ASSIGNMENTS BY FOREIGN NATIONALS SPONSOR PROGRAM MANAGEMENT & ADMIN _____ COUNTERINTELLIGENCE REQUIREMENTS _____ EXPORT CONTROLS/TECH TRANSFER REQUIREMENTS _____ SECURITY REQUIREMENTS _____ APPROVALS AND REPORTING _____ OVERALL RATING _____	
d) INFORMATION PROTECTION BASIC REQUIREMENTS _____ TECHNICAL SURVEILLANCE COUNTERMEASURES _____ OPERATIONS SECURITY _____ CLASSIFICATION GUIDANCE _____ CLASSIFIED MATTER PROTECTION & CONTROL _____ Control of Classified Matter _____ Special Access Programs and Intelligence Information _____ OVERALL RATING _____		h) NUCLEAR MATERIALS CONTROL & ACCOUNTABILITY PROGRAM ADMINISTRATION _____ MATERIAL ACCOUNTABILITY _____ MATERIALS CONTROL _____ OVERALL RATING _____	
13. Report Prepared by:		14. Report Approved by:	
Date:		Date:	
15. Distribution:			
16. General Comments:			

SURVEYS: S = Satisfactory M = Marginal U = Unsatisfactory D = Does Not Apply NR = Not Rated (SPEC only)
INSPECTIONS: EP = Effective Performance NI = Needs Improvement SW = Significant Weakness D = Does Not Apply

ATTACHMENT 7-2

PART I CORRECTIVE ACTION PLAN SHEET		
Finding Number:		Facility Code:
Responsible HQ Element Surveyed:		
Topical Area:	Sub-topical Area:	
Reference(s) (i.e., Orders, Requirements, etc.):		
Description of Deficiency:		
PART II		
Causal Analysis Process Used:		
Causal Code(s):		
Corrective Action Description:		
Estimated Completion Date:		
Surveyed POC: Print Name Signature Date		
Federal Management Approval is Required: Print Name Signature Date		
PART III (If Applicable)		
Revised Completion Date:		
Reason for Revised Completion Date:		
If Revising Completion Date, Federal Management Approval is Required: Print Name Signature Date		

Unclassified Until Filled In, Then Handle Appropriately

ATTACHMENT 7-3

Instructions for Completing a Corrective Action Plan Sheet

Surveyed POC is responsible for completing the Corrective Action Plan and implementing the Causal Analysis.

Part I Place finding information from Survey Report into Part I.		
PART II Causal Analysis Process Used: Identify the technique used to identify the Causal Code. The preferred DOE Headquarters tool is using the causal analysis tree to help in identifying the root cause outlined below.		
Causal Code(s): More than one code is acceptable but not common, except if one of the codes is human error, which is generally supported by a second code.		
Corrective Action Description: High-level description of corrective action to include clear concise information. If multiple steps are required, a separate Milestone Sheet should be completed.		
Estimated Completion Date: Enter the date the action is expected to be completed.		
Surveyed POC: Insert name of the Element POC.		
Federal Management Approval is Required: By signing, the surveyed Federal Management concurs and approves the CAP.		
Print Name	Signature	Date
Part III (If Applicable)		
Revised Completion Date: Update completion date, initial form submission will not have information in this block, however additional submissions may include adjustments required by a delay in corrective action efforts.		
Reason for Revised Completion Date: A brief narrative on why the date must be revised, not for the purposes of approval by the surveying organization, but for informational purposes.		
If Revising Completion Date, Federal Management Approval is Required:		
Print Name	Signature	Date

CAUSAL ANALYSIS TREE



ATTACHMENT 7-4

CORRECTIVE ACTION PLAN MILESTONE SHEET		
Finding Number:	Date:	
Milestone Number:		
Milestone Description:		
Milestone Due Date:	Date Milestone Completed:	
Surveyed POC:		
Print	Signature	Date
Federal Management:		
Print	Signature	Date
Milestone Number:		
Milestone Description:		
Milestone Due Date:	Date Milestone Completed:	
Surveyed POC:		
Print	Signature	Date
Federal Management:		
Print	Signature	Date

Unclassified Until Filled In, Then Handle Appropriately

ATTACHMENT 7-5

Instructions for Completing a Corrective Action Plan Milestone Sheet

SECTION	INSTRUCTIONS
Finding Number	Enter the finding number.
Date	Enter the date the form is completed.
Milestone Number	Enter milestone number (consecutive starting with 1). If more than two milestones are identified, an additional milestone sheet(s) will be required.
Milestone Description	• Write milestone with clear deliverables that solve the problem. Ensure that the milestone address and correct the deficiency. • Limit individual milestone instructions to brief, concise statements describing logical segments of the specified milestone. • Write a realistic and achievable milestone that can be verified. • Do not overextend a milestone beyond your control. Ensure that resources are available. • If completion of the milestone is required by persons outside of the responsible manager's authority, the responsible manager coordinates the milestone with the supporting program Element.
Milestone Due Date	Enter the due date for each milestone.
Date Milestone Completed	Enter the actual date each milestone was completed.
Surveyed POC Signature	Surveyed POCs sign for concurrence of each assigned milestone.
Federal Management Signature	Federal Management sign for concurrence of each assigned milestone.

ATTACHMENT 7-6

THIS FORM IS TO BE COMPLETED BY THE HQ SURVEY TEAM

CORRECTIVE ACTION PLAN VALIDATION REPORT			
Finding Number:			
Finding Short Description:			
Validation Requested By:		Phone #:	Date:
Conducted By:		Phone #:	Date:
CAP Validated?	Yes:	No:	
Comments:			
SSIMS Closure:		Date:	
Evaluator(s) Print and Sign:			Date:
Survey Program Manager Approval:			Date:
AU-42 Director Print and Sign:			Date:

UNCLASSIFIED UNTIL FILLED IN, THEN HANDLE APPROPRIATELY

Chapter 8 Revision History as of 03/25/2020:

3/31/2020

- OPSEC heading, 1st paragraph (page 8-1 line 9) Added: Official Use Only (OUO) and Unclassified Controlled Nuclear Information (UCNI).
- OPSEC Appointments (page 8-1 line 9) Added: The head of each element updates the appointment memorandum each time there is a change to their OPSEC Representative. In the absence of a duly appointed OPSEC Representative, the Headquarter Security Officer (HSO) will carry out the duties of the Representative.
- Element OPSEC Representatives (page 8-2 line 13) Added: Conduct OPSEC assessments within their element and brief their management on the results of the assessment.
- OPSEC Assessments (page 8-3 line 8) Added: The OPSEC assessment is conducted by the program element's OPSEC Representative (at intervals not to exceed 36 months for HQ program elements possessing Top Secret and/or Special Access Program information within their facility(s)). Although the OPSEC Representative conducts the OPSEC assessment of their program element, the HQ OPSEC Program Manager may assist with the assessment if requested to do so by the program element OPSEC Representative (refer to DOE O 471.6, *Information Security*, Section 4 f(3), for more on OPSEC Assessments).
- OPSEC Reviews (page 8-3) Added paragraph: OPSEC Reviews – explanation, requirements, and protocols.
- Information on Publicly Posted Websites (page 8-4 line 5) Added: For this reason, each HQ program element shall review information before it is posted on their agency's web site or released to the general public. This review is necessary to ensure that no CI is released unknowingly and without proper authorization.
- Attachment 800-2 (page 6) Added: Sample OPSEC Assessment Report and Checklist

12/5/2019

- Points of contact (page 8-3) Updated to read: "...call (301) 903-7189 or (301) 903-1974."
-

Chapter 8

Operations Security Program

This chapter covers the Operations Security (OPSEC) Program in place at U.S. Department of Energy (DOE) Headquarters (HQ) to fulfill the requirements of DOE Order 471.6, Section 4.f, *Information Security*.

The goal of the OPSEC Program is to assist HQ program elements in identifying and protecting their Critical Information (CI) from inadvertent and unauthorized disclosure and assisting in the protection of classified information. CI includes those classified or sensitive unclassified areas, activities, functions, data or information about an activity or organization deemed important to protect from an adversary. CI, if disclosed, would have a negative impact on national security and/or departmental operations if unauthorized disclosure should occur. Examples of CI are Official Use Only (OUO), Unclassified Controlled Nuclear Information (UCNI), personnel files (personally identifiable information (PII)), proposal and contract documents, and financial data regarding a project. CI is supported by indicators that are clues or paths that, when analyzed or combined, could lead an adversary to items contained in the Critical Information List (CIL). The HQ OPSEC Program provides senior managers with information to make sound risk management decisions concerning the protection of CI and ensure that OPSEC techniques and measures are implemented throughout HQ.

HQ Implementation Procedures

HQ OPSEC Program Manager:

The Director, Office of Headquarters Security Operations (AU-40), is responsible for appointing, in writing, a HQ OPSEC Program Manager. The Program Manager oversees the HQ OPSEC program and is the focal point for all OPSEC related issues. The HQ OPSEC Program Manager is responsible for all aspects of the program including:

- Providing OPSEC techniques and measures to program element OPSEC Representatives.
- Assisting HQ elements in identifying their organization's CI and maintaining their CIL.
- Developing and executing an OPSEC awareness program that includes regular briefings to ensure that personnel are aware of their responsibilities in support of the OPSEC program.
 - These briefings may be integrated into, or provided in conjunction with, required security briefings (e.g., Initial Security Briefings, Comprehensive and the Annual Security Refresher Briefings) and related meetings, training, and workshops throughout the HQ.

- At the request of the program element OPSEC Representative, assisting in OPSEC assessments/reviews of HQ elements to ensure that CI is being protected, element personnel are aware of their responsibilities for protecting CI, and ensuring that element leaders are aware of assessment results.
- Act as a technical advisor and expert on all matters affecting the HQ OPSEC program.
- Assign and document approved responsibilities for OPSEC direction, management, and implementation throughout the HQ.

Element OPSEC Representatives:

The head of each element, or their designee, shall appoint, in writing, an OPSEC Representative. The OPSEC Representative *should* possess a “Q” or “L” clearance. The appointment memorandum is formatted and addressed as described in the *Sample Appointment Memorandum* included in the Forms/Samples subsection below. The head of each element updates the appointment memorandum each time there is a change to their OPSEC Representative. In the absence of a duly appointed OPSEC Representative, the Headquarter Security Officer (HSO) will carry out the duties of the Representative. The Element OPSEC Representative will:

- Assist in the implementation of current and newly developed OPSEC procedures throughout their organization.
- Make certain that employees in their organization are aware of their OPSEC responsibilities.
- Review information generated by or for the Federal Government that is being placed on any website or made available to the public to ensure it does not contain CI.
- Internally coordinate and develop the CIL for their organization.
- As is necessary, prioritize and update their organization’s CIL and ensure it reflects current assets, threats, operations and other relevant factors. Submit the information to the HQ OPSEC Program Manager as necessary.
- Conduct OPSEC assessments within their element and brief their management on the results of the assessment. See *OPSEC Assessments* below for specifics on these requirements.
- Assist in implementing corrective measures to mitigate vulnerabilities identified during OPSEC assessments. Ensure these measures are implemented in a timely manner.
- Routinely check offices to ensure there are no OPSEC vulnerabilities, i.e., computer screens unlocked, PII posted in plain view in unattended offices, CUI material in waste baskets and recycle bins (all are common OPSEC vulnerabilities).

- Maintain OPSEC Program data and ensure it is current. Program data should include, but is not limited to, current appointment memos, pertinent OPSEC directives, assessments/reviews, and actions taken to enhance the element's OPSEC Program.

OPSEC Assessment:

OPSEC assessments are conducted to ensure CI holdings are not inadvertently made available to unauthorized personnel. These assessments may be conducted as part of an OPSEC assessment or included in a HQ Survey Team survey/review activities. Results must be documented and shared with the program element/site being assessed. It is important for the element's OPSEC Representative to be an active participant in these actions. The results of OPSEC assessments should be documented and shared with interested stakeholders such as the HQ Foreign Visits and Assignments Team, Headquarters Security Officers, security program managers, and senior officials within the element. The OPSEC assessment is conducted by the program element's OPSEC Representative (at intervals not to exceed 36 months for HQ program elements possessing Top Secret and/or Special Access Program information within their boundaries). Although the OPSEC Representative conducts the assessment of their program element, the HQ OPSEC Program Manager may assist with the assessment if requested to do so by the program element OPSEC Representative (refer to DOE O 471.6, *Information Security*, Section 4 f(3), for more on OPSEC assessments).

OPSEC Review:

An OPSEC review is a broad scope review of a specific facility, program, or activity to determine the level of OPSEC support required. The review is a management tool usually conducted by the program element's OPSEC Representative with assistance from the OPSEC Program Manager if requested. However, the OPSEC Program Manager may elect to conduct an OPSEC review if he/she believes it to be necessary to ensure the protection of sensitive information.

In some cases, activities, programs, or facilities may have no sensitive security interests while others may be highly sensitive. Thus, the level of support may range from simply documenting that no further OPSEC support is required to the establishment of a formal OPSEC program. DOE O 471.6, *Information Security*, Section 4 f(3), will be the determining factor.

It is recommended that an OPSEC review of sensitive activities and facilities be conducted when one or more of the following criteria arise:

- New construction is planned for a facility that will process or store classified or sensitive information.
- New sensitive activities are initiated or significant changes occur to existing programs.
- The element sponsors unclassified FV&As to HQ facilities.

Information on Publicly Posted Websites:

Certain categories of unclassified information are generally recognized as unsuitable for public release. These include, but are not limited to, controlled unclassified information such as Official Use Only (OUO), Unclassified Controlled Nuclear Information, personally identifiable information (PII), protected Cooperative Research and Development Agreements (CRADA), and export control sensitive subjects. For this reason, each HQ program element shall review information before it is posted on their agency's web site or released to the general public. This review is necessary to ensure that no CI is released unknowingly and without proper authorization. The review ensures the information does not place at unacceptable risk to national security, DOE personnel, and or assets, mission effectiveness, or the privacy of individuals. The responsible program element's OPSEC Representative should periodically review published information to confirm appropriateness and continued compliance with DOE directives. Although not suggested, should it become necessary to post CI on a public site, or otherwise make it available to the public, the element should get approval by the OSFSA and the Office of Public Affairs, General Counsel, and/or Office of Classification, as appropriate, prior to releasing this information. For more information on information review and public release of DOE information see DOE O. 471.6, *Information Security*, Section 4 f(3), and the DOE Handbook, OPSEC, June 2019.

Points of Contact

AU-41 is the office of primary responsibility for the Headquarters OPSEC Program. For more information on OPSEC or questions regarding this chapter, call (301) 903-7189 or (301) 903-1974.

Forms/Samples

Sample Appointment Memorandum (see Attachment 800-1)
Sample OPSEC Assessment Report format (see Attachment 800-2)

Helpful Website

The Powerpedia Website offers additional information and can be found at the following link:
https://powerpedia.energy.gov/wiki/Operations_security

ATTACHMENT 800-1

Sample Appointment Memorandum

MEMORANDUM FOR KURT RUNGE
DIRECTOR
OFFICE OF PHYSICAL PROTECTION
OFFICE OF ENVIRONMENTAL HEALTH, SAFETY AND
SECURITY

FROM: (NAME)
NAME OF ELEMENT

SUBJECT: Appointment Memorandum for (Enter name of organization)

This memorandum notifies you of the (enter name of element) employees appointed to the following security-related positions:

Headquarters Security Officer (HSO) - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

Alternate HSO(s) - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

HSO Representative(s) - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

Operations Security (OPSEC) Representative - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

Alternate OPSEC Representative - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

cc: HSO
Alternate HSO(s)
HSO Representative(s)
OPSEC Representative
Alternate OPSEC Representative
HSO Program Manager (AU-41)

ATTACHMENT 800-2***Sample OPSEC Assessment Report & Checklist*****I. ASSESSMENT REPORT****A. Location Date and Purpose**

During the period of _____, an OPSEC assessment was conducted by _____, the OPSEC Representative for _____. The OPSEC assessment identifies the organization's Critical Information (CI) and any vulnerability to this information as a result of the conduct of daily activities. It also provides recommendations, to upper level management, on how to protect this organization's CI.

The OPSEC Representative (hereafter referred to as the assessor) conducted the assessment by utilizing two methods. Under the first method, the assessor attempted to gain access to CI through processes that would be available to someone outside of the organization with building access. It also involved observing patterned behavior and activity of members of the organization to reveal information about its activities and capabilities. The purpose was to reveal what access an unauthorized individual could gain to the program element's workspaces and information. The second method involved the face-to-face review with members of the organization to determine if CI is being adequately protected.

II. RESULTS**A. Internet Search**

An OPSEC assessment Internet search was performed of the organization's website and the information available on the Internet.

Results: *List findings*

B. Public Media/Public Releases

An OPSEC assessment search was performed on open source organization's public media and public releases available on the Internet. Provisions for review of information released to the public are/are not in place.

Results: *List findings*

OFFICIAL USE ONLY (when filled in)

C. Trash/Recycle Containers (Dumpster Diving)

The OPSEC assessor looked in the Forrestal/Germantown recycle and trash containers maintained by Office of Management personnel.

Results: *List findings*

D. Office/Workspace Entry and Search

Germantown/Forrestal Building (*identify the facility (s) where the assessment took place*)

Office/Workspace Entry and Search

The OPSEC assessor entered offices/workspaces and copy rooms to determine if CI or other sensitive information was inadequately protected.

Results: *List findings*

Recommendations: *List recommendations for each deficient finding and or observation.*

E. Foreign Visits & Assignments (FV&As)

The program office has/does not have a security plan in place for foreign national visitors. The plan is deemed to be/not to be adequate in accordance with established security requirements and Chapter 6, Foreign Interaction, Headquarters Facilities Master Security Plan (HQFMSP). The program office has escort procedures in place and escorts all foreign nationals during visits (*if applicable*).

Results: The OPSEC assessor did not have any FV&A concerns.

F. Critical Information List

The program office maintains a critical information list (CIL) which is current and correct (or, is not current and is not correct). The CIL was reviewed for accuracy during this assessment. Prior to this assessment the last review of the CIL was accomplished on _____. The assessor has determined that the organization's CI is/is not being adequately protected. A random sampling of assigned personnel indicated that employees know/do not know what a CIL is and are familiar/not familiar with means required to protect the organization's CI.

Observations: *List observations*

Recommendations: *List recommendations*

OFFICIAL USE ONLY (when filled in)

CATEGORY	YES	NO	N/A
Program Management			
Has an OPSEC Representative for the Program Element (PE) been appointed, in writing, by the PE director (reference Chapter 8, OPSEC, Headquarters Facilities Master Security Plan (HQFMSP))? - Is the memo current/correct? Has a copy of the memo been provided to AU-41?			
Does the OPSEC Representative have a copy of the current <i>Threat Statement</i> on file and are PE personnel aware of the local threat to DOE HQ?			
Has the OPSEC Representative received any formal OPSEC training and/or certification?			
Does the OPSEC Representative regularly attend quarterly HSO meetings (reference “HSO Duties & Responsibilities”, HQFMSP)? - Does the OPSEC Representative pass on relevant security information to his/her assigned personnel?			
OPSEC ASSESSMENTS & REVIEWS			
Has an OPSEC Assessment and/or OPSEC Review been conducted of the PE? - When was the last Assessment conducted? - Was the Assessment documented and on file? - When was the last Review conducted? - Was the Review conducted and on file? NOTE: IAW Chapter 8, OPSEC, HQFMSP and DOE O. 471.6, <i>Information Security</i>, OPSEC Assessments are required for HQ organizations maintaining Top Secret (TS) materials and Special Access Programs (SAP) at intervals not to exceed 36 months.			

OFFICIAL USE ONLY (when filled in)

CATEGORY	YES	NO	N/A
CRITICAL INFORMATION			
Does the OPSEC Representative maintain a critical information listing (CIL) of their organization's critical information (CI) IAW Chapter 8, OPSEC, HQFMSP and DOE O. 471.6, <i>Information Security</i>. - Is the CIL current/correct? - Has a copy of the CIL been provided to AU-41 (NOTE: at a minimum, the CIL is <i>Official Use Only</i>)? - Is the CIL reviewed, at a minimum, annually and is the review documented in the PE's Appendix to the HQFMSP?			
Do PE personnel know what information is critical? - Are employees aware of their PE's CIL NOTE: this can, and should, be determined by a random sampling/interview process of assigned personnel.			
COUNTERMEASURES			
Are sensitive documents/information properly disposed of (reference Chapter 5, CMPC, Chapter 8, OPSEC, and Chapter 13, CUI, HQFMSP)? - Is CUI shredded and/or placed in a plain brown paper burn bag and sent to the Classified Central Destruction Facility (CCDF) for disposal? - Are precautions taken to ensure CUI is never placed in a trash can or recycle bin (e.g., dumpster diving, warning sign placed on recycle bins/receptacles, etc.)?			
Is CI displayed in plain view and visible in common areas for all to see, e.g., bulletin boards, desk tops, left unattended on top of printers, copy machines, etc.?			
Is CUI properly protected in unattended work stations/offices and after duty hours (reference Chapter 8, OPSEC, and Chapter 13, CUI, HQFMSP)?			
Are procedures in place for electronically sending/receiving OOU, PII, and UCNI data to ensure this information is protected? - Are procedures for electronically transmitting CUI information documented/in writing?			

OFFICIAL USE ONLY (when filled in)

CATEGORY	YES	NO	N/A
Do PE personnel know how to report (and who to report to) security concerns and/or security incidents (reference Chapter 11, Incidents of Security Concern)?			
Do all personnel properly display their DOE badge? Do employees question personnel not properly displaying their DOE badge?			
Are procedures in place to review PE/DOE information posted on social media sites and prior to public release to ensure the data does not contain CUI (OUO, PII, UCNI) information (reference Chapter 8, OPSEC, HQFMSP, and DOE O. 471.6, <i>Information Security</i>)?			
HOSTING FOREIGN VISITORS & ASSIGNEES			
Are procedures in place to process and host foreign visitors (reference Chapter 6, Foreign Interaction and Chapter 8, OPSEC, HQFMSP)? - Has a FACTS Data Entry Person been appointed, in writing, IAW DOE Order 142.3, Change 1, <i>Unclassified Foreign Visit and Assignment Program</i>, and Chapter 6, Attachment 602-6, HQFMSP? - Are FACTS entries made properly and in a timely manner? - Does the host approve all foreign visitors in FACTS? - Are visit memos prepared and sent to the Office of Physical Protection in a timely fashion and IAW Chapter I, Physical Security, Section 107, HQFMSP? - When required (e.g., High-Level Protocol Visit) has a security plan been developed for hosting foreign visitors and is the plan adequate and adhere to the requirements outlined in Chapter 6, Attachment, 602-9, HQFMSP? - Are escorts properly briefed on their escort duties IAW Chapter 6, Attachment 602, HQFMSP (required for LA/VTR access and during security hours)? - Is the escort's briefing recorded in the organization's Appendix to the HQFMSP (listed under the CMPC Training Records section) IAW Chapter 6, page 601-2, HQFMSP?			
Are Indices Checks of foreign visitors/assignees conducted if and when required and IAW Chapter 6, HQFMSP?			

OFFICIAL USE ONLY (when filled in)

Chapter 9 Revision History: Revisions by date (Newest to oldest):

July 22, 2024: Chapter was reformatted to be in alignment with the Chapter Guide.

April 15, 2024: Updated office code to EHSS-54 and changed “OUO” references to “CUI.”

March 20, 2021: Added Attachment 900-4 *Modified Secure Phone Work Order*

February 2, 2021: Added Attachment 900-3 *Medical Device Worksheet*

September 3, 2019: Revised “Points of Contact”

November 2, 2018: Revised “Available TSCM Services” section

November 2, 2018: Added Attachment 900-2 *TSP Gift Review Worksheet*

October 16, 2018: Added revised Attachment 900-1 *Equipment Worksheet*

October 16, 2018: Attachment 900-1 removed.

June 28, 2017: Updated Points of Contact

Chapter 9

Technical Surveillance Countermeasures

This chapter of the U.S. Department of Energy (DOE) Headquarters (HQ) Facilities Master Security Plan (HQFMSP) describes technical security requirements and processes for requesting technical security services at DOE HQ facilities. Additionally, personnel responsibilities are detailed below and must be followed to ensure the safeguard and security of classified information. The requirements within this chapter are the implementation of [DOE Order 470.6, Technical Security Program](#) (TSP) and various national policies. This chapter is applicable to all DOE personnel, visitors, and tenants located in DOE HQ areas where classified information is discussed, processed, viewed, or stored. This chapter is maintained by the Office of Technical Security (OTS), EHSS-54.

Section 901 – TSP Support Services and Request Processes

Section 902 – TSP Requirements for Headquarters Elements

Section 903 – TSP Requirements for Personnel with Access to Classified Areas

Attachments – Listing of DOE HQ Technical Security Services Request Worksheets

Definitions:

Certified TEMPEST Technical Authority (CTTA): An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with the Committee on National Security Systems (CNSS) approved criteria and has been appointed by the head of a U.S. Government Department, Agency, or designee to fulfill CTTA responsibilities.

Communications Security (COMSEC): Designed to protect and control the means and materials used to provide encrypted communications.

Compromising Emanations (CE): Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information system equipment.

Controlled Cryptographic Item (CCI): Secure telecommunications or information system, or associated cryptographic component, that is unclassified and handled through the COMSEC Material Control System (CMCS), an equivalent material control system, or a combination of the two that provides accountability and visibility. Such items are marked “Controlled Cryptographic Item”, or, where space is limited, “CCI.”

Medical Electronic Device (MED): Medically prescribed electronic devices having the capability to store, record, and/or transmit text, images/video, or audio data. Examples of such

devices include, but are not limited to: hearing aids, blood glucose monitors, external heart monitors, etc. These devices should not be confused with life-saving devices such as implanted defibrillators or pacemakers.

Officially Designated Federal Security Authority (ODFSA): Federal employees that possess the appropriate knowledge and responsibilities for each situation to which they are assigned through delegation. The ODFSA is charged with responsibility for physical, technical, personnel, and information security matters affecting the location identified in the delegation.

Delegation authority for these positions is originated according to direction from the accountable Undersecretary who also provides direction for further delegation of the ODFSA designations. All delegations of authority must be documented in writing.

Portable Electronic Device (PED): Electronic devices having the capability to store, record, and/or transmit text, images/video, or audio data. Examples of such devices include, but are not limited to: pagers, laptops, cellular telephones, radios, compact disc and cassette players/recorders, portable digital assistant, audio devices, watches with input capability, and reminder recorders.

Protected Distribution Systems (PDS): Designed to protect unencrypted classified signal/data lines that exit secure areas and traverse through areas of lesser security.

Technical Surveillance Countermeasures (TSCM): Designed to detect, deter, isolate, and nullify technical surveillance penetrations and technical security hazards.

Technical Surveillance Penetrations: Any instance of information leaving an area by unauthorized technical means for monitoring by unauthorized entities, either through installation of a technical surveillance device, manipulation of software, interception and monitoring of fortuitous emanations, or intentional creation of a hazard.

TEMPEST: Designed to prevent the unauthorized intercept of compromising emanations that may be present in information processing communication equipment, systems, and components. A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

Wireless Security (WiSec): Designed to test/evaluate the impact of mobile and fixed wireless communication devices used in or near classified and sensitive unclassified activity areas for the purpose of determining risks and countermeasures.

Section 901

TSP Support Services and Request Processes

The Office of Technical Security (OTS), EHSS-54 provides operational support for technical security activities at HQ facilities. Support includes TSCM, TEMPEST, WiSec, PDS, and COMSEC. Personnel who frequent DOE HQ locations must be familiar with HQ technical security requirements to ensure the protection of classified information.

Technical Surveillance Countermeasures

TSCM services are tailored to meet local operating conditions based on the threat level and potential vulnerabilities. TSCM services are conducted by the HQ DOE technical security team with oversight from the Office of Technical Security Team (OTS), EHSS-54.

The following TSCM services are available at DOE HQ facilities:

- **TSCM Survey** – A TSCM Survey, which includes instrumented anomaly resolution and technical penetration investigations, is the most comprehensive of the TSCM operational activities. The TSCM Survey includes a thorough technical, physical, and visual examination of the area to identify technical and physical security hazards and the presence of technical surveillance devices.
- **TSCM Inspection** – A TSCM Inspection is a limited activity addressing specific concerns. An inspection evaluates the changes to an operating environment to identify if vulnerabilities were inadvertently created due to modifications or upgrades of the area. Inspections are required to assess the technical integrity of furnishings, electronic equipment, proposed or completed construction, gifts, or installation of items not previously examined by the DOE HQ technical security team. Medical devices are considered electronic equipment and must be inspected prior to bringing these items into a Limited Area (LA), Vault-Type-Room (VTR), or a Sensitive Compartmented Information Facility (SCIF) – [Attachment 900-3 OTS WS - Medical Device Review Worksheet](#). Areas subject to recurring services are required to have TSCM inspections of equipment, furnishings, etc., when items enter the facilities – [Attachment 900-1 OTS WS – Equipment Inspection Request Worksheet](#). TEMPEST and TSCM item inspections are usually accomplished simultaneously.
- **TSCM In-Conference Inspection** – A TSCM In-Conference Inspection is a limited service, normally provided in conjunction with classified/sensitive briefings, conferences, meetings, and seminars, in an area that is not normally secured but must be employed due to the size of the specific activity or the unavailability of suitable space in secure areas. This is primarily a limited inspection of the technical attributes of the facility before, during, and (as necessary) after the activity.
- **TSCM Advice and Assistance** – TSCM Advice and Assistance is a service conducted before and or during construction or renovation of a new or existing area to ensure that

appropriate physical and technical security standards or vulnerabilities are addressed prior to procurement to avoid costly modifications. This service is also appropriate prior to the purchase, replacement, installation, and going “live” with electronic systems, such as video teleconferencing systems and telephone systems.

- **TSCM Education** – TSCM educational efforts include presentations, briefings, literature, or other means by which the HQ personnel become familiar with the TSCM Program and the technical threat to their facilities, equipment, or activities to minimize the possibility of compromising sensitive information.
- **Special TSCM Services** – These services occur infrequently. They are conducted to meet unforeseen circumstances or protection needs according to conditions of local threat or vulnerabilities, regardless of classification level, and are usually event driven. These services do not nullify the requirements of other security disciplines where a temporary increase in protection levels must be applied because of the specific nature of the activity (classified or sensitive).

Request Process: It is critical that TSCM requests are appropriately controlled to ensure the integrity of the TSCM service. **TSCM SERVICES AND REQUESTS ARE GENERALLY CLASSIFIED AND WILL REQUIRE REVIEW BY A DERIVATIVE CLASSIFIER PRIOR TO SUBMISSION.** Foregoing the derivative classifier review could result in a classified information spillage resulting in a security infraction. Routine and general requests for TSCM services should be submitted via the DOE HQ TSCM Service Request worksheet [Attachment 900-5 OTS WS – TSCM Service Request](#) through the elements TSCM Officer (TSCMO). Requests should be made as far in advance as possible to account for scheduling conflicts. Telephonic or in-person requests for time sensitive TSCM services are authorized; however, must **NOT** occur in the area where the service is to be conducted (refer to section 903 of this chapter for specific requirements), must occur over a classified medium, and must be followed with a written request using the DOE HQ TSCM Service Request worksheet. Discussions and emails of pending TSCM activities must **NOT** occur in the requested inspection area prior to the service.

After a request is submitted, validated, and approved by the OTS, a member of the DOE HQ technical security team will coordinate details of the service with the TSCMO or designated point of contact identified in the request.

NOTE: All items and systems (personal and government-owned) located in an area undergoing a TSCM service are subject to inspection by the DOE HQ technical security team. All unauthorized items presenting a vulnerability are subject to confiscation. The item may be sent to a laboratory for analysis, including destructive analysis, if necessary.

TEMPEST

TEMPEST is the study of unintentional CE, which is produced by all electronic / electromechanical telecommunications and automated information processing equipment. These

emanations may possess intelligence-bearing information, that if intercepted and analyzed, may disclose classified information.

The following TEMPEST services are available or are required at DOE HQ facilities:

- **TEMPEST Reviews** – Classified facilities, information systems, activities, and discussion areas, will be evaluated by a CTTA to determine compliance with CNSS policies and what, if any, TEMPEST countermeasures are necessary.
 - TEMPEST Reviews are required:
 - TEMPEST facility countermeasure reviews must be conducted by a CTTA annually.
 - If wireless technologies operate within 100' of areas where classified information is discussed or processed.
 - Prior to the procurement of National Security Systems; computers, laptops, printers, servers, etc.
 - Prior to construction or modification of a facility or area designated to process classified information.
 - Upon a change in approved classified activities.
 - Additions or changes to National Security Systems equipment.
 - Reviews may also be required due to a change in threat level or national policy.
- **TEMPEST Inspection** – Electrical/Electronic equipment, Portable Electronic Devices (PEDs) and Medical Electronic Devices (MEDs) with wireless, recording, or microphonic technologies must be reviewed prior to entering a security area. TSCM and TEMPEST item inspections are often conducted simultaneously by the DOE HQ technical security team or CTTAs.

Request Process: Request for TEMPEST reviews or inspections can be accomplished by submitting the appropriate request (Attachments 2,3,4) to [TecSec](#).

NOTE: TEMPEST plan development and reporting must be accomplished in accordance with the TEMPEST checklist for SCIFs, regardless of the classification of the designated space, contained within the [IC Technical Specifications for Construction and Management of SCIFs](#) or successor documents when appropriate

Wireless Security (WiSec)

WiSec is generally referred to the protection of wireless National Security System (NSS) information, most notably classified and unclassified wireless access points, but also encompasses wireless devices in proximity to areas where classified information is discussed, displayed, or processed.

Transmitters to be installed within classified facilities, buildings, etc., or in proximity to classified facilities, must not be installed, or powered on until the CTTA has conducted a review and the cognizant security authority has accepted any residual risk in writing.

The following WiSec services are available at DOE HQ facilities:

- **Transmitter Reviews** – Unclassified and classified transmitters reviews must be conducted within DOE HQ facilities, to include tenants, for transmitters that will operate within 100' of classified systems, activities, or discussion areas.
 - Only approved CIO provided wireless access points and cellular repeaters are authorized at HQ facilities. Cellular Hotspot and personally owned wireless access points are not authorized in HQ facilities.

Request Process: It is the requestors responsibility to submit a completed transmitter review request [Attachment 900-4 OTS WS – Transmitter Review Worksheet](#) to [TecSec](#).

Protected Distribution Systems

PDSs are designed to protect unencrypted classified signal/data lines that exit secure areas and traverse through areas of lesser security.

PDS's must be approved by the ODFSA and maintained in accordance with CNSSI 7003. Installation of a PDS should **NOT** be common practice and only used as a last resort to meet mission requirements.

Request Process: Contact [TecSec](#) with questions related to PDS requirements.

Communications Security

EHSS-54 is the DOE Central Office of Record (COR), the Command and Controlling Authority of all COMSEC material and activities for DOE to include NNSA. EHSS-54 provides information and requirements for the operation and maintenance of DOE, to include NNSA, secure communications activities for the acquisition, storage, assignment, distribution, inventory, control, and accountability of COMSEC material applicable to COMSEC activities of DOE federal and contractor employees.

Some COMSEC equipment is designated as controlled cryptographic items (CCI) and must be accounted for by element COMSEC personnel. These items include secure telecommunications, such as ViPer desktop phones, information systems, or associated cryptographic components. Additional information regarding secure desktop phones can be found in [Chapter 2](#) of the HQFMSP.

Section 902

TSP Requirements for Headquarters Elements

The Head of each HQ element must appoint, in writing, a TSCMO to serve as the liaison between the EHSS-40 and the DOE OTS for all activities requiring TSCM support.

TSCMO responsibilities are fully identified in DOE O 470.6, *Technical Security Program*, but the following responsibilities are emphasized:

- Prior to the beginning of each fiscal year and or when an area requiring TSCM service is identified or deactivated, provide a list of these areas requiring recurring TSCM services to EHSS-40 as outlined in the Memorandum of Agreement between the OTS, EHSS-54 and EHSS-40.
- Coordinate onsite assistance for the DOE HQ technical security team to ensure strict adherence to need-to-know and Operations Security (OPSEC) principles for TSCM activities.
- Ensure that all permanent personnel located within an area designated for a TSCM service are aware of TSCM requirements, with emphasis on reporting procedures and OPSEC.
- Coordinate unrestricted access within service areas during TSCM services.
- Coordinate the introduction of any equipment necessary for TSCM activities or services to be carried out.

NOTE: TSCMO training is provided periodically by OTS, DOE HQ technical security team or upon request by a TSCMO.

Section 903

TSP Requirements for Personnel with Access to Classified Areas

Adherence to technical security protocols by personnel and visitors that frequent DOE HQ facilities is integral to the success of the technical security program. The unintended introduction of controlled/prohibited articles or audible comments of TSCM operational activities could result in the compromise of classified information or a classified activity. Alternatively, personnel and visitors at DOE HQ facilities are ideal reporters to changes in their daily working environments. These keen observers can detect subtle changes in their work areas which may be indicative of a concealed technical surveillance device.

Prompt and discrete reporting is required when addressing a suspected technical surveillance device to ensure the integrity of a thorough technical investigation. The success of most technical security activities requires strict adherence to OPSEC practices. The below are requirements of all personnel and visitors that frequent DOE HQ facilities:

OPSEC

OPSEC is a systematic and proven process intended to deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: (1) identification of critical information; (2) analysis of threats; (3) analysis of vulnerabilities; (4) assessment of risks; and (5) application of appropriate countermeasures. OPSEC practices are a critical component to the DOE technical security program and must be exercised by all DOE contractors, employees, and visitors.

- TSCM activities are generally classified and must be restricted to personnel with the appropriate clearance and need-to-know as established by the DOE OTS Director or staff when delegated by the OTS Director.
- Never discuss TSCM services in areas where the TSCM activity will occur.
 - If a concealed surveillance device was present in the area, the adversary would become aware of the TSCM service and power off the device making it infinitely more difficult to detect.
- Never audibly acknowledge ongoing TSCM activities.
 - Do not ask questions about TSCM equipment or make comments referring to; sweeps, bugs, ghosts, etc. These actions could result in the termination of the TSCM service and a security infraction.
- Always maintain a normal working environment during TSCM activities.

- Keep computers, printers, and other information technology systems powered on.
- Do not excuse yourself from the work area due to the TSCM survey.
- If you need to speak with the TSCM technician during a TSCM service, write your question on a piece of paper and hand it to the technician. The technician will respond in writing or accompany you outside the survey area to further discuss this issue.
 - All TSCM services are conducted by cleared personnel and approved by the DOE HQ ODFSA.

Discovery of a Suspected Technical Surveillance Device

Discovery of a technical surveillance device, or suspicion of the existence of such a device in any DOE HQ facility, to include tenant areas, must be reported immediately to the OTS, EHSS-54. The report should be made in person but may be made via a secure/encrypted medium such as a STE or ViPer phone. The report must be made from outside the facility where the suspected surveillance device exists. Do not voice the discovery within the immediate area, which includes the suspect room and all other rooms/areas above, below, and adjacent to it. Secure the area to preclude any attempts to remove the discovered device(s) and continue normal activity in the area without discussing classified information. OTS, EHSS-54 will provide further instructions on how to proceed.

A TSCM Survey is requested immediately upon the discovery of a technical surveillance device or evidence that a technical surveillance device was present, regardless of the type of facility where the condition was discovered.

TSCM/TEMPEST Item Inspections

Controlled Articles: items that possess cameras, microphones, storage, recording capability, or wireless technologies are prohibited in classified discussion, viewing, and processing areas unless approved by the DOE HQ ODFSA. Controls to mitigate the threat posed by these devices range from administrative to prohibition and must be approved by the DOE HQ ODFSA. Personnel working in classified areas must submit a completed item inspection request ([Attachment 900-1 OT WS – Equipment Inspection Request Worksheet](#)) to [TecSec](#) for all items listed in the [Controlled Articles Matrix](#) found in the HQFMSP Chapter 2 attachments. **NOTE:** There are additional inspection requirements listed below specific to TSCM areas. These items are not permitted into security areas until the inspection is completed and any residual risk is accepted in writing by the DOE HQ ODFSA.

Please note the following additional information related to TSCM/TEMPEST inspections and controlled articles:

- Personnel working in TSCM areas must submit inspection requests through their TSCMO or HSO for inspections of personal and government owned office furnishings which includes electronic devices, appliances, furniture, etc.

- Requests must be initiated for medical devices with cameras, microphones, storage, recording capability, or wireless technologies.
 - Life-saving devices such as implanted defibrillators must be declared via [Attachment 900-3 OTS WS – Medical Device Review Worksheet](#) and will be administratively reviewed.
- Requests must be submitted for gifts received from non-US personnel whose relationships were developed during official business, or when the item was received through unusual circumstances (provided by a stranger, left in hotel room, discovered in luggage, etc.), regardless of electronic/electric capability.
- DOE provided electronics that have not previously been inspected must be inspected to determine if mitigations are required or sufficient.
- Requests are required for equipment that will process or destroy classified information; classified printers, shredders, scanners, etc.
- All wireless transmitters that will operate within 100' of classified activities (may also require an [Attachment 900-4 OTS WS - Transmitter Review Worksheet](#)).
- Technical security personnel are authorized to confiscate and conduct destructive and non-destructive examinations of devices, to determine if the device poses a threat to classified or sensitive information.

Desktop VTCs

- Desktop VTCs must be approved in accordance with the DOE HQFMSP, [Chapter 2](#).
- Desktop VTCs must be installed, configured, and comply with CNSSI 5000, Annex J, *Softphone Security Requirements*, or successor documents.
- Desktop VTCs approved for use in classified areas must have a TSG disconnect device between the computer and camera/headset.
- Desktop VTCs must use approved TSG devices as specified in the [TSG-6 Telephone List](#). **NOTE:** The TSG-6 Telephone List is usually updated monthly via email distribution and the online link is not always the most current. Contact the DOE HQ technical security team for the current listing.

COMSEC

- In the event of *suspected* loss of possession, control, or physical compromise of COMSEC items (CCI, ViPer, etc.), the DOE OTS, EHSS-54 will be notified immediately. At the DOE OTS's discretion, a formal report must be completed by the COMSEC account custodian in accordance with national policies.

- **Secure Desktop Communications**
 - Secure desktop phone (ViPer, etc.) users may not connect, disconnect, reconfigure, transfer, or relocate these devices on their own. These actions may only be performed by authorized personnel affiliated with the DOE OTS and are coordinated between the DOE HQ element HSOs and the DOE HQ Secure Phone Group via email to [HQ Secure Phone](#) using the [Attachment 900-6 - Secure Phone Work Order Request](#).

Points of Contact

For TSCM, TEMPEST, PDS, WiSec or General technical security requests and support, email [TecSec](#) or call 202-586-8437 / 301 903-9992 / 301 903-6581.

For secure phones support (maintenance, installation, removal), email [HQ Secure Phone](#) or call 301-903-6581 / 301-903-5062.

For all COMSEC specific inquiries, email [Telcom Security](#) or call 301-903-6581 / 301-903-8317.

Attachments

[900-1 OTS WS – Equipment Inspection Request Worksheet](#)

[900-2 OTS WS – Gift Inspection Request Worksheet](#)

[900-3 OTS WS – Medical Device Review Worksheet](#)

[900-4 OTS WS – Transmitter Review Worksheet](#)

[900-5 OTS WS – TSCM Service Request](#)

[900-6 OTS WS – Secure Phone Work Order Worksheet](#)

Chapter 10

Security Awareness Program

This chapter describes the DOE HQ Security Awareness Program. It implements the requirements of:

- Title 32, CFR, Part 2001, Classified National Security Information
- Executive Order 13526, *Classified National Security Information*
- DOE Order 470.4B, *Safeguards and Security (S&S) Program*, Appendix B. Section 3
- DOE Order 475.2A, *Identifying Classified Information*
- DOE Order 475.1, *Counterintelligence Program*

The Security Awareness Program Manager, within HS-92, manages the HQ security awareness program. The goal of the HQ Security Awareness Program is to assist Federal and contractor employees in understanding DOE security requirements, their individual security responsibilities, and security procedures specific to HQ. This goal is accomplished by providing HQ employees with information tailored to their duties. For example, HQ employees with Q and L security clearances receive information about accessing and protecting classified information or SNM.

HQ Implementation Procedures

A variety of security awareness briefings and materials (described below) has been developed to help HQ employees fulfill their security duties.

Required Security Briefings:

1. Initial Security Briefing – An Initial Security Briefing is required for new HQ Federal and contractor employees. The servicing badge office provides a briefing (a video presentation) that the employee must view before receiving his/her security badge. The briefing includes an overview of HQ security programs, access control procedures, escort procedures, property protection measures, prohibited articles, reporting requirements, and other relevant subjects.
2. Comprehensive Security Briefing – The Comprehensive Security Briefing is required for HQ Federal and contractor employees granted a Q or L security clearance. Employees possessing a security clearance that is extended or transferred from another DOE facility to HQ must also receive the HQ Comprehensive Security Briefing. The servicing badge office provides the briefing (a video presentation), which the employee must view before receiving his/her security badge and before

he/she can access classified information, Limited Areas, or VTRs. The briefing describes access control procedures for Limited Areas and VTRs, escort requirements, penalties for mishandling classified information, controlled articles, and other topics associated with the protection of classified matter.

Upon completion of the Comprehensive Security Briefing, the employee must read and sign the SF-312, *Classified Information Nondisclosure Agreement*. The briefing official signs as the witness for the employee signing the SF-312. A signed SF-312 verifies the employee's completion of the Comprehensive Security Briefing. Failure of any employee to complete the SF-312 results in the termination of his/her security clearance and denial of access to classified matter. The badge offices maintain records of the signed SF-312s. In accordance with 32 CFR Part 2001, these records must be kept on file and readily available for 70 years.

By completing the Comprehensive Security Briefing, the employee satisfies the requirement for an initial CMPC briefing.

3. Annual Security Refresher Briefing (ASRB) – The ASRB, required for HQ Federal and contractor employees with a Q or L security clearance, emphasizes information on security policies and information related to the protection of classified information. Contents of the briefing change from year to year based on lessons learned from HQ security incidents, major policy changes affecting the handling of classified information, changes in threats, and renewed emphasis on certain security procedures. HS-92 develops and administers the ASRB and strives to achieve a 100% completion rate for this briefing.

Each HQ element's HSO is given access to the website that administers the ASRB to monitor his/her element's completion rate. HQ employees generally have 30 days to complete the ASRB once they are notified that the briefing is available. When an HQ employee fails to complete the ASRB within the allotted time, his/her HSO is expected to resolve the issue. This applies to both Federal and contractor employees.

4. Security Termination Briefing – A Security Termination Briefing is required when an HQ Federal or contractor employee no longer needs security clearance – for example, on his/her last day of employment, when the need for access expires, or on the day it becomes known that the individual no longer requires access to classified information or SNM. The Security Termination Briefing involves a discussion of the contents of DOE F 5631.29, *Security Termination Statement*.

The employee's servicing badge office, at either the Forrestal or Germantown facility, should perform the Security Termination Briefing because those offices have standard procedures in place to complete the DOE F 5631.29 and distribute it to HS-93.

In special situations, the HSO is requested to conduct a Security Termination Briefing. The HSO is then responsible for providing the DOE F 5631.29 to the

servicing badge office. A Security Termination Briefing is available in DVD format from the HSO Program Manager. The DVD is especially useful in processing large numbers of employees departing in a short time span, such as when a presidential administration ends. (HQFMSP Chapter 15, Outprocessing, contains additional information on outprocessing departing employees.)

When an employee cannot complete a DOE F 5631.29, such as death of the employee, the responsible HSO must complete the form on behalf of the employee, indicate the reason it is not signed by the employee, and submit it to the servicing badge office or HS-93.

Employees with access to Special Access Programs, NATO, and SCI must receive an additional individual termination briefing from representatives of those programs. The individual termination briefing is completed during outprocessing (see Chapter 15, Outprocessing, for additional instructions).

Need-Based Security Briefings:

Special security briefings may be needed. For example, an element may require briefing on such subjects as a counterintelligence threat, travel advisories, cyber security, specialized handling requirements for classified matter, or understanding OOU or other types of sensitive information. The Security Awareness Program Manager can assist HSOs and employees by identifying HQ personnel or organizations that can develop and present such briefings.

Points of Contact

For the names and contact information for the positions identified in this chapter, call (301) 903-9990 or (301) 903-7198.

Forms/Samples/Graphics

SF-312, *Classified Information Nondisclosure Agreement* (for a copy of this form go to <http://www.gsa.gov/portal/forms/download/116218>)

DOE F 5631.29, *Security Termination Statement* (for a copy of this form go to http://energy.gov/sites/prod/files/cioprod/documents/DOE_F_5631.29_Admin_Update_03-2011.fillable.pdf)

Helpful Websites

Security Awareness Special Interest Group (SASIG), <https://www.ora.gov/sasig/>

HQ Security Awareness Program,
http://www.hss.energy.gov/HQSecOp/security_awareness.html

Powerpedia DOE Security Awareness, https://powerpedia.energy.gov/wiki/Security_Awareness

Chapter 11 Revision History as of 07/03/2023:

July 3, 2023: Updated organization name and abbreviation. Additional revisions under “Initial Reporting” section.

August 12, 2022: Revised revision history, formatting, and hyperlinks.

November 22, 2019: Sections on identifying and categorizing incidents and tracking and trending has been added. A fillable form “Initial Report of Headquarters Security Incident” was created.

January 5, 2018: This entire chapter has undergone a major revision. As changes are too extensive to itemize, please review Chapter 11 in its entirety.

Chapter 11

Incidents of Security Concern

This chapter covers the DOE HQ implementation of [DOE Order 470.4B, Chg. 3, *Safeguards and Security Program, Attachment 4, Incidents of Security Concern*](#). The Office of Headquarters Security Operations (EHSS-40) in the Office of Environment, Health, Safety and Security manages the HQ Security Incidents Program.

Incidents of Security Concern (henceforth referred to as Incidents) are actions, inactions, or events that are believed to:

- Pose threats to national security interests and/or DOE assets or degrade the overall effectiveness of DOE's protection program.
- Create potentially serious or dangerous security situations.
- Significantly affect the safeguards and security program's capability to protect DOE safeguards and security interests.
- Indicate failure to adhere to security procedures.
- Reveal the system is not functioning properly, by identifying and/or mitigating potential threats (e.g., detecting suspicious activity, hostile acts, etc.).

Incidents require follow up to:

- Ensure management awareness.
- Determine the facts and circumstances of the incident.
- Ensure corrective actions are taken to mitigate the incident.
- Develop actions to correct underlying weaknesses and prevent recurrence.
- Track and trend incidents to improve the health of the security program.
- Document whether a security infraction or other disciplinary action is needed.

Headquarters Implementation Procedures

Identifying and Categorizing Incidents:

DOE uses a graded approach for identifying and categorizing incidents as described in DOE Order 470.4B, Chg. 3, *Safeguards and Security Program, Attachment 4, Incidents of Security Concern*, and provides greater detail on incident categorization and incident criteria. An Incident Categorization Matrix has been developed to assist with identification and categorizing of Incidents based on the type of incident event and is provided within this chapter.

[DOE Standard Incidents of Security Concern, DOE-STD-1210-2012, September 2012](#), contains additional information and guidance on identifying and categorizing security incidents. Links to these documents are provided in the "Helpful Website" section of this Chapter.

Initial Reporting:

HQ personnel must promptly report suspected incidents of security concern to their respective Headquarters Security Officer (HSO), or a Contractor Protective Force (CPF) officer. CPF will notify the HSIPM of a possible security concern. The HSIPM will alert the HSO of the program office involved.

The discovering organization's HSO will perform the initial reporting to the HQ Security Incidents Program Manager (HSIPM), which may be done telephonically ensuring that only unclassified information is communicated unless a Secure Terminal Equipment (STE) or Viper is being used. If the initial report is made telephonically or verbally, it must be followed by a formal written initial report. Formal reporting can be accomplished by sending an unclassified/ encrypted e-mail to, HQIOSCProgram@hq.doe.gov. The notification e-mail **MUST** contain the word **Incident** in the subject line. The e-mail should include the [Initial Report of a Headquarters Security Incident](#). If the template is not used, the information provided in the Initial Report must correspond to all fields in the template. Reports made in writing must be properly classified.

***CAUTION:** Details of security incidents may be classified. Consult with a classifier before preparing or submitting these messages.*

If a potential incident crosses multiple program or staff office jurisdictions, then the office that suspects that the security incident occurred must take primary responsibility and execute the necessary reporting and notification processes. After reviewing the suspected incident, the HSIPM determines whether it should be handled as an incident or an administrative matter.

***EXAMPLE:** Unless there was a compromise or aggravating circumstance (such as a repeat offense), failing to use a "Candy Stripe" envelope to carry classified matter within HQ should be handled as an administrative matter and the employee retrained, not as an Incident of Security Concern.*

Incident Identification and Categorization

Within 5 calendar days of being confirmed as an Incident, the HSIPM categorizes the incident in coordination with the reporting entity based on guidance contained in Attachment 4 to DOE Order 470.4B, Chg. 3. The Incident will be categorized as:

Category A: Incidents, which meet a designated level of significance relative to the potential impact on the Department and/or national security, require the notification of the DOE/NNSA CSO and the contractor CSO. The involvement of the DOE/NNSA CSO for Category A incidents is imperative for assessing impacts, coordinating with external agencies, and/or notifying senior management.

Category B: Do not meet the Category A criteria, are managed, and resolved by the contractor CSO; however, this does not preclude the DOE/NNSA CSO from exercising its oversight responsibilities.

Incident Type:

- Security Incident (SI),
- Procedural Interest (PI)
- Management Interest (MI)

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. If the final inquiry reveals additional details and facts, the incident can be re-categorized.

The HSIPM ensures that all HQ Incidents of Security Concern categorized as an A/SI or A/PI are logged into SSIMS and assigned unique tracking numbers.

Based on the information involved and the likelihood of compromise, the HSIPM, the program office reporting the incident, and EHSS-40 management are consulted to determine whether a Damage Assessment (DA) and/or Notification to Congress as a “Significant Nuclear Defense Intelligence Loss,” per 50 U.S.C. Section 1656 is required.

***NOTE:** DAs and/or Notification to Congress may be required for confirmed or suspected compromises of Top Secret, SCI, SAP, and RD Nuclear Weapon Data. Weapon Data is Sigma 14, 15, 18, or 20 information as defined by DOE Order 452.8. The organization with programmatic responsibility for the information/material would handle the reporting requirements and conduct of the DA. Also see Section 1, Attachment 4 of DOE Order 470.4B, Change 3, for reporting guidance.*

Assignment of Inquiry Official:

A formal documented inquiry to determine the facts and circumstances of the incident is required for all SI and PI incidents. Once the reporting element designates an Inquiry Officer from within their organization, the HSIPM formally assigns responsibility for performing the inquiries by memorandum that states the details of the incident and provides associated documentation. However, the HSIPM may assign an Inquiry Officer from a different organization to perform the inquiry if the organization doesn't have an Inquiry Officer or by request of the reporting organization.

Inquiry officers must meet the requirements of and be knowledgeable of Section 1, Attachment 4 to DOE Order 470.4B, Change 3, i.e., they must have previous investigative experience or Departmental Inquiry Official training through the DOE National Training Center, Learning Nucleus site; *PMC-300DE, Legal Aspects Overview, and the PMC-310, Incidents of Security Concern Fundamentals*. The individual must be knowledgeable of appropriate laws, executive orders, Departmental directives, and/or regulatory requirements.

Inquiry officers are appointed by their management based on the criteria above. Copies of appointment memoranda are provided to the HSIPM along with either a training certificate or description of investigative experience.

The inquiry officer's priority is to ensure that appropriate action is taken to mitigate the incident, e.g., securing documents, sanitizing e-mail servers, etc. Once mitigating actions have been completed, the inquiry officer tries to determine the cause of the incident, what actions must be taken to address any underlying weaknesses, and recommend the appropriate follow up actions including retraining, issuance of a security infraction, or other disciplinary action.

Should the inquiry officer believe during the investigation that a criminal act may have occurred or that an agent of a foreign power is involved, the inquiry officer must immediately cease the inquiry and notify the HSIPM.

NOTE: *Although inquiry officers may be Federal or contractor employees, only Federal employees are authorized to contact outside agencies/organizations (e.g., Postal Service; FBI; or Federal, State, or local agencies) regarding an ongoing inquiry. Such contact should be coordinated with the HSIPM.*

Completed Category A incident reports must be submitted to the HSIPM within 90 days of assignment. If additional time is required, the HSIPM must be notified, and an extension requested.

Inquiry/Closeout Reports:

A formal closeout report is required for all security incidents with the interest type of SI or PI. Templates for the most common security incidents may be used to help Inquiry Officers complete their reports and can be obtained from the HSIPM. Closeout Reports should remain unclassified if possible. If the Inquiry Officer chooses not to use the templates, he/she must create a report that details the following information:

- A full description of the incident (i.e., “who, what, where, why, when, and how”) providing more detail than contained in the initial report.
- For all incidents, the report must include the name of the individual(s) primarily responsible for the incident, including a record of prior incidents for which the individual(s) had been determined responsible. Other involved individuals must also be named. Access authorization levels (for all individuals involved) must be clearly stated.
- The report must identify mitigating factors that reduce the potential impact of the incident (such as confirmation that affected computer systems were immediately sanitized) or any other action that reduces the potential impact of the incident.
- The report must identify aggravating factors that increase the potential impact of the incident (for example, a security container was left unsecured for an undetermined period).
- The report must identify any corrective actions that will be taken to preclude recurrence, including retraining, issuance of a security infraction, or other disciplinary action.

A copy of the [DOE F 5639.3, Report of Security Incident/Infraction](#) must be completed by the Inquiry Officer. If it is determined that no infraction is warranted, the basis for that determination must be documented in the inquiry report. DOE F 5639.3 must be attached to the inquiry report and signed by the responsible individual’s Office Director. Infractions can be issued to cleared and non-cleared individuals who violate security requirements.

For Information Protection incidents, the inquiry officer determines the likelihood of compromise per the definitions below:

- Loss/Compromise did Occur. Compromise was confirmed. Information was disclosed to an unauthorized person(s) (e.g., published by media, briefed to unauthorized individuals, etc.).
- Probability of Compromise is not Remote. Compromise is suspected. Lacking a clear indication of compromise (i.e., no direct recipient), the circumstances are such that there is an obvious possibility of unauthorized disclosure (e.g., classified information is transmitted by

e-mail outside of the organization's firewall, classified information is communicated on an unsecure phone line, etc.).

- **Probability of Compromise Is Remote.** A low possibility exists that information was disclosed to unauthorized personnel (e.g., classified information is left unsecured and unattended for a limited amount of time in an area accessed only by personnel with the appropriate clearance level, classified information is transmitted by e-mail inside the organization's firewall and is discovered and isolated within a specified timeframe).
- **Loss/Compromise Did Not Occur.** No possibility of compromise exists (e.g., although an open storage area was not secured, the access control system shows the door was not opened).

For example, when determining the extent of compromise the following table should be used:

Likelihood Of Compromise Guidelines	
Non-Secure Transmittal of Classified Matter Over Electronic Networks (i.e., e-mail)	
Circumstances of the non-secure transmittal	Likelihood of Compromise is:
Any addressee is uncleared to have received the information	Confirmed
Transmittal within the firewall, encrypted and sanitized within 24 hours	Remote
Transmittal within the firewall, not encrypted and sanitized within 8 hours	Remote
For all other transmittals	Is not Remote

For any confirmed or suspected compromise as mentioned above, the extent of dissemination (e.g., number of individuals and their citizenship; global disclosure via cyber media; open-source publication; etc.) should be identified.

If applicable, a determination is made as to whether an unauthorized disclosure was willful (i.e., intentional vs. inadvertent disclosure).

Incident Closure:

The HSIPM reviews the inquiry report to ensure that it is complete and adequately addresses date of occurrence, individuals involved, cause, actions to contain incident, corrective actions, and actions to prevent recurrence.

When all requirements of closure are met, the HSIPM has the SSIMS database updated, if applicable. The report is distributed with a copy of the DOE F 5639.3 to DOE Personnel Security and EHSS-80 management.

Tracking and Trending:

Each security incident must be assigned a tracking number by the HSIPM. The HSIPM is responsible for maintaining a spreadsheet that contains a tracking number and additional information to include the incident date, category, incident type, HSO or Inquiry Official, completion date, and whether the incident resulted in disciplinary action, such as a security infraction. (Organizational elements at Headquarters may also maintain their own local tracking number to track/trend their incidents should they choose to do so.)

The HSIPM will provide the Director, Office of Physical Protection, with information from the spreadsheet for the purpose of monitoring security program performance and to gauge deficiencies where site security procedures may need to be modified or whether corrective actions need to take place to enhance Headquarters' security posture.

Retention of Files:

The HSIPM maintains a 5-year history file of HQ security incidents in accordance with RIDS requirements. Additional incident records are maintained in the SSIMS database.

Points of Contact

For the names and contact information for the positions identified in this chapter, call (301) 903-0885.

Forms/Samples/Graphics

[*Initial Report of a Headquarters Security Incident – fillable pdf*](#)

[*Incident Categories and Types*](#)

[*Sample Memo – Appointment as Inquiry Officer*](#)

[*Deputy Secretary of Energy Memorandum, Security Incident \(Including Cyber\)
Congressional Notification Protocol, June 24, 2011*](#)

Helpful Websites

[*DOE Order 470.4B, Chg. 3, Safeguards and Security Program, Attachment 4, Incidents of Security Concern*](#)

[*DOE F 5639.3, Report of Security Incident/Infraction*](#)

Inquiry officer training is available at: [*National Training Center*](#)

[*DOE Standard Incidents of Security Concern, DOE-STD-1210-2012, September 2012*](#)

Chapter 12

Special Access Programs

This chapter describes the DOE Special Access Program (SAP) at DOE HQ and implements the requirements of:

- Executive Order 13526, *Classified National Security Information*, Section 4.3, Special Access Programs, and Section 5.4, General Responsibilities, subparagraph (d).
- DOE Order 471.5, *Special Access Programs*.

A SAP is a program established for a specific class of classified information that imposes safeguarding and access requirements exceeding those normally required for information at the same classification level.

Terms and activities such as Limited Access, Controlled Access, and Limited Distribution programs are not authorized.

HQ Implementation Procedures

SAP administration for both DOE and NNSA is handled through the Executive Secretary of the Special Access Program Oversight Committee (SAPOC). SAPOC activities are conducted in accordance with the requirements of DOE Order 471.5. This directive is OUO and available only to authorized personnel.

Points of Contact

For contact information about DOE SAPs, call (202) 586-3345 or (301) 903-2644.

This page intentionally left blank.

Chapter 13

Controlled Unclassified Information

This chapter describes the security procedures adopted by DOE HQ to implement the requirements of the following DOE regulations and directives:

10 CFR Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*

DOE Order 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*

DOE Order 471.3, *Identifying and Protecting Official Use Only Information*

DOE Manual 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*

Within DOE, Controlled Unclassified Information (CUI) refers to unclassified information identified and marked as sensitive.

CUI also describes information identified and safeguarded under Executive Order 13556, CUI. Executive Order 13556 mandates a government wide uniform program to identify and protect sensitive but unclassified information. Policies for CUI under Executive Order 13556 are being developed. No timetable has been established for implementation, which will take place over years. Until a national directive is issued and DOE issues its own implementing directive, DOE personnel must continue to follow the regulations and directives for UCNI and OUO information.

Within DOE, CUI includes:

- Unclassified Controlled Nuclear Information (UCNI)
- OUO, which encompasses Personally Identifiable Information (PII), Export Controlled Information (ECI), and other unclassified sensitive information not governed by specific directives
- Unclassified Naval Nuclear Propulsion Information (U-NNPI).

Note: Confidential Foreign Government Information-Modified Handling Authorized (C/FGI-MOD) is classified under Executive Order 13526 and does not fall under this section (see Section 504, Foreign Government Information).

Transmission

UCNI:

A document containing UCNI may be transmitted by (1) U.S. First Class, Express, Certified, or Registered mail; (2) any other means approved for transmitting a classified document; (3) an authorized individual as long as physical control of the package is maintained; or (4) mail services internal to the facility. The document must be packaged in a single, opaque envelope or wrapping. The address of the recipient and the sender must be indicated on the outside of the envelope or wrapping along with the words “TO BE OPENED BY ADDRESSEE ONLY.”

Encryption must be used when transmitting UCNI over a telecommunications circuit (e.g., telephone, facsimile, radio, e-mail, Internet).

OUO:

A document containing OUO may be transmitted by (1) First Class, Express, Certified, or Registered mail as well as by any commercial carrier; (2) a person authorized access to the OUO so long as the person can control access to the document being transported; or (3) mail services internal to the facility. For documents sent outside a facility, the document must be packaged in a sealed, opaque envelope with the recipient’s address, a return address, and the words “TO BE OPENED BY ADDRESSEE ONLY” on the front. For documents sent within a facility, the document must be packaged in a sealed, opaque envelope with the words “TO BE OPENED BY ADDRESSEE ONLY” on the front, but only the recipient’s address is required.

Encryption, when possible, should be used to transmit OUO over a telecommunications circuit. If encryption is not available and transmission by mail is not a feasible alternative, the document should be sent password protected, and the password communicated by separate e-mail or by phone to the recipient. If OUO is transmitted by unencrypted facsimile, the transmission must be preceded by a telephone call to the recipient so that he or she can control the document once received.

Destruction

Documents containing CUI must be destroyed by shredding. CUI must not be put in the recycle bins. A document containing CUI may be destroyed using a cross-cut shredder producing particles no larger than ¼ inch x 2 inches. Shredders meeting this requirement are available in the self-service supply stores.

Bulk paper waste and plastic and metal waste containing CUI may be placed in plain brown paper bags and delivered to the Burn Bag Rooms (Forrestal GI-007 and Germantown R-002) for destruction. The name, routing symbol, telephone number, and room number of the person responsible for the burn bag and the type of material contained within (i.e., paper, plastic, or metal) must be clearly marked on each bag for identification. The weight limit for each bag is 10 pounds for bags generated at Forrestal and 15 pounds for those generated at Germantown.

The difference in weight limitation results from transportation and handling requirements. The top of the bags should be folded over at least once and stapled shut every 2 inches. Burn bags must be protected as CUI until they are destroyed.

Documents and material containing CUI may also be destroyed by methods approved for the destruction of classified matter.

HQ Implementation Procedures

Requirements for access to and protection of UCNI and OUO are contained in the respective DOE regulations and directives listed above. The following points are included here for emphasis:

A clearance is not required for access to CUI. Requirements for access to UCNI are contained in 10 CFR Part 1017. In general, OUO may be granted to a person needing the information to perform a DOE-authorized function. However, some OUO (e.g., Export Controlled Information, Source Selection Information) has additional access restrictions.

Documents containing UCNI or OUO must not be posted on websites available to the public. For requirements concerning posting UCNI and OUO on internal DOE websites, contact the Office of the Chief Information Officer (IM-622).

Documents and material containing UCNI or OUO must be reviewed in accordance with program office policies prior to public release (e.g., posted on a website), and the appropriate personnel must remove the UCNI and OUO.

Accountability is not required for CUI.

The originating agency establishes protection requirements for other-agency CUI – for example, Sensitive But Unclassified (SBU), For Official Use Only (FOUO), and Administratively Controlled Information (ACI). In most cases, when other-agency protection requirements cannot be determined, documents bearing these markings should be protected within DOE HQ as OUO. However, exceptions exist, such as the Nuclear Regulatory Commission's Safeguards Information (SGI) and the Department of Homeland Security's Sensitive Security Information (SSI). If unsure how to handle other-agency CUI, contact the person who transmitted the information for clarification and direction.

Points of Contact

For information about CUI, call (301) 903-4861 or (301) 903-7567.

Additional Information

The Office of Classification's website has a page with information concerning OUO (<http://www.hss.doe.gov/classification/QualityMgt/ouo.html>) and another on UCNI (<http://www.hss.doe.gov/classification/ucni/index.html>). These pages contain information, resources, and links to the DOE regulation and directives concerning CUI.

The DOE CMPC Marking Resource has additional information concerning marking documents containing CUI. To access the DOE CMPC Marking Resource go to:

http://www.hss.energy.gov/SecPolicy/DOE_CMPC_Marking_Resource.pdf

Chapter 14

Cyber Security

The DOE Cyber Security Program aims to protect the Department's diverse missions in a cost-effective manner; identify threats, risks, and mitigations; and remain flexible in a changing environment. Key Departmental directives, policies, and procedures governing the implementation of the Cyber Security Program at DOE HQ are:

- DOE Order 205.1B, *Department of Energy Cyber Security Management*
- DOE Policy 205.1, *Department of Energy Cyber Security Management Policy*
- *Headquarters Program Cyber Security Plan (HQ PCSP)*

HQ Implementation Procedures

The head of each HQ element is responsible for implementing a cyber security program within his or her element that conforms to the policies and procedures set forth in the HQ PCSP. Each Head of Element must appoint, in writing, an Information Systems Security Officer (ISSO) and as many Alternate ISSOs as necessary, to support the organization's classified and unclassified systems (see Attachment 1400-1).

The appointment memorandum must be addressed and distributed as shown (see Attachment 1400-1).

Each ISSO receives guidance and assistance from IM-622 through the point of contact identified below.

Points of Contact

For cyber security-related matters, call (202) 586-6691.

Forms/Samples/Graphics

Sample ISSO Appointment Memorandum (see Attachment 1400-1)

ATTACHMENT 1400-1

Sample ISSO Appointment Memorandum

MEMORANDUM FOR (NAME)
DIRECTOR
CYBER SUPPORT DIVISION
OFFICE OF THE CHIEF INFORMATION OFFICER

FROM: (NAME)
NAME OF ELEMENT

SUBJECT: Information Systems Security Officer Appointment Memo

This memorandum notifies you that (enter employee's name) has been appointed as Information System Security Officer (ISSO)/Alternate ISSO at (enter name of element) effective (enter date of appointment).

She/he will perform ISSO/Alternate ISSO duties as assigned in the Headquarters Program Cyber Security Plan section 5.13 (PCSP) November 2011 and NIST SP 800-37 Rev 1, Appendix D.

For further information, please contact me at (enter email address, phone number)

cc:
HQ AO
HQ ISSM/CA
AU-42

Chapter 15

Outprocessing

No DOE directive specifically requires a formal security outprocessing procedure; however, numerous directives require termination actions that are best accomplished through a formal process. For example:

- DOE Order 472.2, *Personnel Security*, Paragraph 4q, requires the termination of security clearances when they are no longer needed.
- DOE Order 471.6, *Information Security*, Paragraph 4b(5)(d)4, requires that safe combinations be changed when a person who had access to that safe no longer requires access.
- DOE Order 473.3, *Protection Program Operations*, Attachment 3, Section A, Paragraph 7c, requires that DOE security badges be recovered when no longer needed.

The Office of the Chief Human Capital Officer (HC) has a formal process for notifying DOE HQ elements when a Federal employee terminates employment. However, there is no formal process for notifying HQ elements when a contractor terminates employment or when a Federal or contractor employee transfers to another element. Element HSOs must establish close working relationships with the Human Resource specialists within their element, CORs, and contractor project managers to be notified when any of their employees terminate or transfer to another element.

Every HQ element should develop an individualized outprocessing procedure to ensure that access to HQ facilities and classified matter is terminated when an HQ employee or contractor terminates his/her employment with DOE or transfers to another element within HQ. Elements that handle classified matter need a more robust outprocessing procedure than does an element without classified interests.

HQ Implementation Procedures

When to Outprocess an Employee:

HQ personnel should be outprocessed by their element when they terminate their employment with DOE or transfer to another element in HQ. There is no need to outprocess someone who is deployed as a result of his/her military obligations or transfers to another office within the same element, unless the individual no longer needs his/her security clearance.

Who is Responsible for Outprocessing an Employee:

The HQ element losing the terminating or transferring employee is responsible for his/her outprocessing. The losing element is responsible for terminating the employee's security clearance, security badge, special accesses, etc. If the employee is transferring to a different HQ element, the gaining element is responsible for requesting the transfer of security clearance, reactivating his/her security badge, reestablishing special accesses, etc., as needed.

Security Outprocessing Actions:

The HSO for each element is responsible for developing an outprocessing procedure specific to his/her organization. In general, the procedure should only address security issues. The following security outprocessing actions are recommended:

- Terminate security clearance
- Terminate SCI access
- Terminate SAP access
- Terminate NATO access
- Terminate visit requests
- Cancel classification/declassification officer authority
- Destroy or return classification guides
- Remove name from Classification Guidance Distribution System
- Recover law enforcement badges and credentials
- Recover keys to doors, desks, and filing cabinets
- Arrange for safe and door combination changes
- Revise access lists for rooms controlled by C-CURE card readers and TESA locks
- Revise SF-700, *Security Container Information*
- Change custodianship of accountable documents and media
- Recover and secure KSV-21 cards (Fortezza cards) for STEs
- Notify the HQ COMSEC Program Manager of changes in STE custodianship

- Recover or destroy hand carry cards for classified documents that may have been issued to the individual
- Return security badges
- Update the organization's Appendix to the HQFMSP to reflect needed changes.

A sample *Security Outprocessing Checklist* is available to element HSOs from the HSO Program Manager.

Termination of Security Clearances:

When a Federal or contractor employee with a security clearance terminates employment or transfers to another HQ element, his/her security clearance must be terminated and a DOE F 5631.29, *Security Termination Statement*, must be completed. The Forrestal and Germantown badge offices have procedures in place to automatically obtain the DOE F 5631.29 from employees with security clearances who are terminating or transferring. Once the DOE F 5631.29 is completed, the badging office automatically provides a copy to AU-43.

Special situations may arise when an HSO is requested to conduct a security termination briefing. HSOs may do so, but the HSO is then responsible for providing the DOE F 5631.29 to the servicing badge office. A security termination briefing is available in DVD format from the HSO Program Manager. The four minute long DVD is especially useful in processing large numbers of employees who depart in a very short period of time, such as at the end of a Presidential administration. (See Return of Security Badges subsection below for actions related to the collection and return of security badges.)

Return of Security Badges:

One of the final and most important outprocessing actions is return of the terminating or transferring individual's security badge. When any Federal or contractor employee departs DOE HQ or a contractor transfers to another HQ element, the employee must return his/her badge to DOE control. The badge should be turned in to either the Forrestal or Germantown badge offices. Alternatively, it may be turned in to the element's HSO, who in turn must provide it to the servicing badge office.

If a Federal or contractor employee is departing DOE, the badge office determines if the badge should be retained or destroyed.

When a contractor employee transfers to another HQ element, that employee must inform the badge office of that fact when he/she turns in the badge. The badge office temporarily retains the badge until notified that the contractor is now supporting another HQ element. That notification could come in one of two ways:

- If the contractor becomes a Federal employee, the badge office receives an accession list from HC showing that the contractor has been hired by DOE and requires a new security badge.
- If the contractor remains a contractor employee but will support a different HQ element, the HSO of the gaining element must generate a new DOE F 473.2, *Security Badge Request*, and send it to AU-43. AU-43 performs certain verification actions and passes the DOE F 473.2 to the badge office. When the badge office receives the DOE F 473.2, they re-issue the security badge to the transferred employee.

Prohibition Against Removal of Records:

All classified and unclassified matter, including “extra copies,” is the property of the U.S. Government and may not be removed from DOE control by any departing or terminated official or employee. DOE Federal or contractor personnel who retire or otherwise terminate employment and wish to take documents or material (e.g., memorandums, personal records, diaries, etc.) that fall wholly or partially within areas that are classified are personally responsible for ensuring that all such documents or material are unclassified and fully releasable. A Derivative Classifier – not the departing individual – must determine whether such documents and material are unclassified and releasable to the public. Public releasability should be determined in accordance with Freedom of Information Office applicable directives and local procedures.

Unclassified documents are also the property of DOE and may not be taken by departing personnel without the approval of the Program Manager who owns the information contained in the documents. A Derivative Classifier must review the documents to ensure that they are unclassified, and an appropriate official must ensure they do not contain information exempt from release under the provisions of the Freedom of Information Act.

NOTE 1: Federal records are defined as “all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other data in them.”

NOTE 2: Personal papers are defined as “papers of a private or non-official character which pertain only to an individual's personal affairs that are kept in the office of a Federal official.”

Use of HQ Form 3293.1, *Employee Final Separation Clearance*:

HQ Federal employees who are terminating are given an HQ F 3293.1, *Employee Final Separation Clearance*, by their element's HC representative. This form must be completed and returned to the HC representative before the Federal employee departs HQ. Failure to do so could delay the employee's final paycheck.

The HQ F 3293.1 contains two sections for security outprocessing. Block 7B is signed by the departing employee's HSO, and Block 13 is typically completed and signed by the badge office personnel who performed the employee's security termination briefing and collected his or her security badge. If an HSO collected the terminating employee's security badge and conducted the security clearance termination briefing, the HSO could sign Block 13. Completing Block 13 is usually the final step in outprocessing Federal employees.

Other Outprocessing Actions:

As a courtesy, HSOs may adapt their security outprocessing procedure to notify other elemental officials responsible for non-security termination actions. For example, the element's APR or ISSO may request that they be notified of impending departures. Common non-security outprocessing actions include:

- Cancelling Local Area Network (LAN) and database accesses (e.g., SSIMS, FACTS, Travel Manager, Management Information System)
- Returning government property, including laptop computers, cell phones, pagers, Blackberries, RSA tokens, etc.
- Returning government-issued credit cards
- Returning parking permit.

Points of Contact

Element HSO

For the names and contact information for those positions identified in this chapter, call (301) 903-7189 or (301) 903-2644.

Forms/Samples/Graphics

DOE F 473.2, *Security Badge Request* (go to <http://energy.gov/cio/downloads/security-badge-request> for a copy of this form)

DOE F 5631.29, *Security Termination Statement* (The following link may only be accessible by use of the Internet Explorer browser.
<http://energy.gov/cio/downloads/security-termination-statement> for a copy of this form)

DOE HQ F 3293.1, *Employee Final Separation Clearance* (go to <http://energy.gov/cio/downloads/employee-final-separation-clearance-form-hq-32931> for a copy of this form)

This page intentionally left blank.

Chapter 16 Revision History: Revisions by date (Newest to oldest):

December 12, 2019: Revised entire document

July 3, 2018: Revised contact information on Page 16-3

March 27, 2018:

- Revised Page 16-2 to include Office of Primary Interest (OPI) and General Counsel (GC)
- Revised Attachment 1600-1
- Revised Attachment 1600-2

This page intentionally left blank.

Chapter 16

Equivalencies and Exemptions (Deviations)

Purpose

The U.S. Department of Energy (DOE) safeguards and security (S&S) orders require implementation of measures to protect DOE security interests. Due to a variety of reasons, a DOE organization may be unable to comply with a directive's specified methodology, but can achieve the security intention in another equally effective manner; or the organization may not be able to comply with the requirement at all.

DOE Order 251.1D, *Departmental Directives Program*, Appendix E, establishes a process for requesting and approving "equivalencies and exemptions" to DOE requirements. DOE Headquarters (HQ) equivalencies and exemptions must be approved by the Associate Under Secretary for Environment, Health, Safety, and Security (AU-1) or designee, which for DOE HQ is the Director of the Office of Headquarters Security Operations (AU-40), designated as the DOE HQ Officially Designated Federal Security Authority (ODFSA). All approved S&S equivalencies and exemptions are maintained in the Safeguards and Security Information Management System (SSIMS) database.

This chapter describes the requirements, processes, and responsibilities for managing DOE HQ S&S equivalencies and exemptions.

Requirements

Definitions:

1. Equivalencies – Alternatives to how a requirement in a directive is met in cases where the "how" is specified. These represent acceptable, alternative approaches to achieving the goal of a directive's requirement.
2. Exemptions – A release from compliance with one or more requirements in a directive, as granted by the exempting organization's Head of the Departmental Element.

Equivalency and Exemption Request Process:

The Headquarters Security Officer (HSO) of the DOE HQ element requesting an equivalency or exemption should first consult with the DOE HQ Equivalency and Exemption Program Manager, in the Office of Information Security (AU-42). The DOE HQ Equivalency and Exemption Program Manager ensures that the subject matter expert (SME) within AU-40 is informed of the element's inability to meet the S&S requirement and their intention to submit a request.

The DOE HQ element HSO and the AU-40 SME will evaluate the circumstances associated with the proposed request. If it is verified that an equivalency or exemption is warranted, the DOE HQ element HSO and the AU-40 SME will determine whether an equivalency or an exemption is needed. The AU-40 SME will assist the DOE HQ element HSO to identify and justify the use of the chosen equivalency or exemption including the identification of compensatory measures and residual risks, as applicable.

Equivalencies must demonstrate that the alternate method will provide an acceptable level of protection, with no increased risk to public health and safety, the environment, workers, or security. Exemptions must clearly delineate compensatory measures, if any, to reduce risk to a reasonably achievable level and identify residual risks.

The DOE HQ element HSO will need to obtain advice from the Office of General Counsel (GC) and the Office of Primary Interest (OPI) (DOE Order 251.1D) prior to submitting the Equivalency and Exemption memorandum to the DOE HQ ODFSA.

The Head of the DOE HQ element is responsible for submitting a equivalency and exemption request via memorandum (see Attachment 1600-1) to the DOE HQ ODFSA that:

- Identifies the requirement(s) for which the equivalency/exemption is being sought;
- Explains the equivalency/exemption;
- Justifies the reasons for the equivalency/exemption.
- Identifies the locations of the offices (Germantown (GTN), Forrestal (FORS), Room Number, etc.) for which the equivalency/exemption is being sought;
- Confirms that the application of the exemption or equivalency does not conflict with applicable Federal law or regulations;
- Indicates when compliance will be achieved in cases of an equivalency;
- Describes alternative or mitigating actions, including associated risks, that have been or will be taken to ensure adequate protection of the public, workers, and the environment for the period during which the exemption will be effective, when applicable; and
- Describes conclusions and recommendations from the OPI review of the exemption/equivalency and resolution of recommendations.

The DOE HQ ODFSA may coordinate with AU-1 before approving or disapproving S&S equivalency or exemption requests.

If the request is approved, the DOE HQ Equivalency and Exemption Program Manager issues an equivalency/exemption number, which is added on the request memo. A copy of the approved request is forwarded to the SSIMS data entry specialist for entry into SSIMS, to generate the active Equivalency and Exemption form. The approved request will be provided to AU-40 for inclusion in the DOE HQ Site Security Plan. A response memorandum will be provided to the requesting element, to include a copy of the SSIMS active Equivalency and Exemption form.

Expiration Dates of Equivalencies and Exemptions:

The DOE HQ Equivalency and Exemption Program Manager will establish a system to review equivalencies and exemptions that have expiration dates as not all require an expiration date. For example, if the equivalencies or exemptions is linked to a deficiency regarding a contract the expiration date may be identified as the end of contract. If a equivalencies or exemptions is associated with a construction project, the construction completion date may be identified as the expiration date.

If it is determined that the approved equivalency or exemption is no longer needed prior to an assigned expiration date, the DOE HQ element HSO should notify AU-40 before discontinuing the approved alternative or compensatory measure(s).

Upon closure of the equivalencies and exemptions in SSIMS, a confirmation will be sent to the DOE HQ element HSO, as well as AU-40, to update the DOE HQ Site Security Plan.

Points of Contact

For the names and contact information for the positions identified in this chapter, call (301) 903-0213 or (301) 903-5287.

Forms/Samples/Graphics

*Template **Equivalency or Exemption** Request Memorandum* (see Attachment 1600-1)

ATTACHMENT 1600-1
Template Equivalency or Exemption Request Memorandum

MEMORANDUM FOR JAMES HUTTON, DIRECTOR
OFFICE OF HEADQUARTERS SECURITY
OPERATIONS
OFFICE OF ENVIRONMENT, HEALTH, SAFETY AND
SECURITY

FROM: (NAME), (HEAD OF ELEMENT)
NAME OF ELEMENT

SUBJECT: (Name of Element) Request for Equivalency (or Exemption)

This memorandum is to request your approval of an (equivalency) or (exemption) to the requirement identified in DOE Order _____, (Title), Paragraph _____.

Executive Summary – Number of equivalencies/exemptions requesting. Confirmation of application of exemption/equivalency does not conflict with federal law or regulations. Describe conclusion and recommendations from the OPI review of the exemption/equivalency and resolution of recommendations.

Background – Explain the equivalencies/exemptions. Identify location of office for which the exemption/ equivalency is being sought.

Standard – DOE Order and wording of actual citation (Ex., DOE O 470.4B, 1.a)
Justification – Why the requirement cannot be met.

Mitigation (Protective measures) – describe any alternative or mitigating actions, to include associated risks, that have been or will be taken to ensure adequate protection of the public, workers, and the environment for the period during which the exemption will be effective. Indicate when compliance will be achieved in cases of an equivalency.

If you have any questions related to this request, please contact (Name), the Headquarters Security Officer for (Element). (Name) can be contacted at phone number _____.

APPROVED: _____ Date: _____

DISAPPROVED: _____ Date: _____

EQUIVALENCY/EXEMPTION NUMBER: _____

EXPIRATION DATE (if applicable): _____

cc: GC
AU-50
AU-41
SME

Chapter 17 Revision History as of 02/26/2024:

- Updated Organization tiles, order citations, added responsibilities for the Alternate HSO and HSO Representatives, added attachment template for HSO Organizational Appendix, and included information provided by [Spotlights](#).
- Added the requirement for HSO Representatives to have successfully completed the PIV process and have an HSPD-12 badge prior to their appointment as a representative.
- Updated the new NTC HSO training course: PMC-100DE, *S&S Core Competencies*, which replaces SAS-101DE, *Introduction to Safeguards & Security*.
- Updated duties for HSO's to have completed PIV process and if initiating national security positions into e-QIP, HSO must have favorable Tier 5 SSBI or hold a DOE security clearance.
- Changed 12 months to 6 months to complete required HSO training.
- Deleted Course PMC 200DE, *Survey Overview*. Survey fundamentals are now included in PMC 100DE.
- Deleted paragraph allowing HSOs to substitute experience for required HSO training. All HSOs (newly appointed and already serving) are required to complete PMC 100DE and FIC 130DE.
- Added: HSOs must ensure that DOE badges are returned when an employee departs HQ. HSOs must work with the Facility Security Officer (FSO) of the contract to ensure badges are recorded as returned.
- Added: HSOs coordinate with the USAccess sponsor to ensure the record in USAccess is updated to terminate the badge of departing personnel.
- Changed ISC-301: *Conduct of Inquiries* has been replaced with PMC-310, *Incidents of Security Concern Fundamentals*
- Deleted requirement for HSO to maintain printed/hard copy of security training certificates including the ASRB. The HSO need only be able to show proof of completion.
- Added reference material to HSO duties.
- Updated HSO appointment memo sample.

Chapter 17

Headquarters Security Officer Program Duties and Responsibilities

This chapter describes the implementation of the Headquarters Security Officer (HSO) Program and defines the authorities, responsibilities, and requirements for the Program.

The HSO Program applies to all departmental elements at Headquarters (HQ) in accordance with [DOE Order \(O\) 470.4B, Chg. 3, *Safeguards and Security Program*](#), paragraph 5, e.(7).(d) and paragraph 5.e.(7).(e), as well as the HQ Site Security Plan (SSP) which outlines that for HQ, the Director of the Office of Environment, Health, Safety and Security (EHSS), “Directs the development and implementation of a security plan for the protection of the DOE Headquarters, its personnel, and its assets; oversees functions of the DOE cognizant security office for DOE Headquarters facilities and delegates this authority in writing as appropriate.” And EHSS “Oversees implementation of the DOE Headquarters Safeguards and Security (S&S) Program, including the development of S&S implementation procedures and guidance for programs described in this Order and its appendices and attachments, to include the approval of Headquarters equivalencies and exemptions; provides oversight and technical direction for all DOE offices located in Headquarters facilities.” The Administrator of the National Nuclear Security Administration (NNSA) will ensure NNSA employees and contractors comply with their respective responsibilities under this Plan/Program.

Requirements

The HSO program complements and supports the SSP by providing for security points of contact within each HQ element for implementation of security requirements in support the SSP and by authority of the Officially Designated Federal Security Authority (ODFSA).

Each element head must appoint a primary HSO and at least 1 alternate HSO for all HQ elements with more than 30 employees. HQ elements with fewer than 30 employees must appoint an HSO only; however, it is recommended the element also appoint an alternate HSO to act in the absence of the primary HSO. Contractor employees may be appointed to the position of HSO Representative to support their HSO and Alternate HSOs. At a minimum, anyone appointed as primary HSO, alternate, or representative must have successfully completed the personal identity verification (PIV) process. They cannot be appointed HSO duties without first having completed this process. The following requirements apply:

1. HSO appointments must be communicated via memo to the Director, Office of HQ Industrial Security Operations, Office of Environment, Health, Safety and Security (EHSS-42)
2. HSO appointment memos must follow the sample memo in this Chapter.
3. HSOs and Alternate HSOs must be Federal employees.

4. HSO primaries, alternates, and representatives must have the same level of clearance as those holding a clearance in their organization. For example, if someone in their program office holds a Q clearance the HSOs must have a Q clearance.

When no HSO is appointed the Alternate HSO will assume all responsibilities of the HSO listed below.

5. All HSOs, Alternate HSOs, and HSO Representatives, must complete the following training courses, based on availability, within six (6) months of appointment. HSOs, Alternates, and Representatives must maintain proof of completion of the following courses:
 - a. PMC-100DE, *S&S Core Competencies*, computer-based training, available on Learning Nucleus (LN).
 - b. FIC-100DE, *Foreign Visits and Assignments Host Training Overview*, computer-based training, available on LN.
 - c. Headquarters Visitor Management System (VMS) Training, provided by Office of Physical Protection, Office of Environment, Health, Safety and Security (EHSS-41).
6. HSOs, Alternate HSOs, and HSO Representatives ***whose organization possesses, handles, processes, and/or stores classified matter*** are required to complete the following training courses within one year of appointment, if available, HSOs must maintain proof of completion for these courses:
 - a. HQ Classified Matter Protection and Control (CMPC) Overview Briefing is available from the HQ CMPC Program Manager. This is an instructor-led DOE HQ briefing and is specific to HQ personnel. The course is offered throughout the year and HSO staff are notified of the class schedule prior to each start date.
 - b. HQ Classified Document Control Station Course, available from the HQ CMPC Program Manager. This is an instructor-led DOE HQ briefing and is specific to HQ personnel. The course is offered throughout the year and HSO staff are notified of the class schedule prior to each start date.
 - c. HQ Classified Matter Hand Carry Authorization Briefing. This is an instructor-led DOE HQ briefing for personnel who are designated to hand-carry or courier classified material outside of the DOE HQ facilities.
 - d. HSOs, Alternate HSOs, and HSO Representatives are required to complete the following additional training courses, based on availability, within two (2) years of appointment:
 - PSC-100DE, *Personnel Security Overview*, computer-based training, available on LN.
 - PMC-200DE, *Survey Overview*, computer-based training, available on LN.

7. Either the HSO or at least one Alternate HSO representing an organization that handles, processes, and/or stores classified information is required to complete the following additional training courses, based on availability, within two (2) years of appointment.
 - a. PMC-300DE, *Legal Aspects Overview*, is computer-based, training and available on LN. This is prerequisite for the instructor-led National Training Center (NTC) *Conduct of Inquiries* course.
 - b. PMC-310, *Incidents of Security Concern Fundamentals*, instructor-led course taught by the NTC.

NOTE: If a course is unavailable on Learning Nucleus due to revision, the requirement is temporarily waived until the course becomes available. In such cases, the individual will have 90 days from the time the course becomes available to complete it. Additionally, the HSO Program Manager may waive the training requirements based on training history and experience of the HSO, Alternate, or Representative.

Responsibilities

Heads of HQ Elements

1. Designate HSOs. This authority may be delegated in writing to another senior official within the element. HSO appointments are made using a memo signed by the head of element or their designee. See the [Sample Appointment Memorandum](#).
2. Ensure the designation of HSOs is communicated to the Director, Office of HQ Industrial Security Operations, Office of Environment, Health, Safety and Security.
3. Ensure HSOs complete requisite training and attend HSO quarterly meetings and training sessions.
4. Ensure the Facility Data and Approval Record (FDAR) remains current by updating the facility security officer (FSO) in the FDAR if changes to the HSO changes the FSO.
5. Designate in writing a responsible official (e.g., the HSO) within the element to approve employees to hand-carry classified matter out of a facility in accordance with [Chapter 5 section 511 of the HQFMSP](#).

Director, Office of Headquarters Industrial Security Operations, Office of Environment, Health, Safety and Security

1. Provides management oversight and direction to the HSO Program.
2. Appoints an HSO Program Manager and assistants as needed.
3. Ensures sections of the Headquarters Facilities Master Security Plan (HQFMSP) are current and describe the procedures and actions required to implement the HQ security program.

HSO Program Manager

1. Provides assistance to HSOs and conducts regular informational sessions to foster understanding and compliance with HQ security procedures.
2. Conducts quarterly HSO meetings to discuss upcoming HQ security initiatives, HSO concerns, and related matters.
3. Coordinates updates to the HQFMSP from security program managers and subject matter experts (SME).
4. Publishes the HSO Spotlight to inform HSOs of security-related matters.
5. Assists in determining what training must be completed by assigned HSOs, Alternates, and Representatives and provides recurring training as needed. May provide waivers to required training based on training history and experience as an HSO, Alternate, or Representative.
 - a. Former HSO, Alternate, or Representatives who have been out of active status for less than 12 months may return to active status. HSO, Alternate, and Representatives who have been out of active status for 12 months or more must complete all initial training requirements.
 - b. Appointment memos must reflect the request for a training waiver and document their experience as an HSO, Alternate, or Representative if requesting a waiver in training.
 - c. The Incidents of Security Concern (IOSC) training requirements cannot be addressed with other training or experience and must be current.
6. Assists EHSS Security Program Managers in obtaining HSO participation in efforts to improve HQ security operations.

Headquarters Security Officers

1. Serves as their element's point of contact for all security-related matters.
2. Performs the following duties on behalf of their element and in accordance with the procedures set forth in the HQFMSP.
 - a. Assists heads of HQ elements in the appointment of personnel to the position of Operations Security (OPSEC) Representative as outlined in [Chapter 8, OPSEC of the HQFMSP](#), and acts as the OPSEC Representative if one is not appointed.
 - b. Obtains, assembles, approves, and/or submits the documentation required to obtain a security badge for entering HQ facilities. The requirements and the process for preparing and submitting these documents can be found in [Chapter 3, Personnel Security of the HQFMSP](#).
 - c. Obtains, assembles, approves and/or submits the documentation required to obtain a security clearance in accordance with [Chapter 3, Personnel Security of the HQFMSP](#).

- d. Annually reviews the need for retaining personnel security clearances.
- e. Ensures that personnel complete the documentation required for security clearance reinvestigations. See [Chapter 3, Personnel Security of the HQFMSP](#), for specific details on this process.
- f. Works with supervisors and managers to ensure that clearance holders notify the Office of HQ Security Vetting of reportable events and absences of 90 days or more. For a complete list of reporting requirements reference [Chapter 3, Personnel Security of the HQFMSP](#).
- g. Assists in the transfer of security clearance and access information to other DOE and Federal organizations so organizational personnel may attend classified meetings in accordance with [Chapter 3, Personnel Security of the HQFMSP](#).
- h. If not appointed as the FSO, works with the FSO of the contract to ensure badges are returned and accounted for. The security of DOE identification media and badges are considered items of national security interest; hence, it is imperative that all such media be controlled and accounted for. To ensure contract employees badges are returned, the HSO will work with the FSO of the contract to ensure badges are returned and accounted for. The FSO and HSO will coordinate with the USAccess sponsor to ensure the record in USAccess is updated to terminate the badge.
- i. If not the USAccess sponsor, coordinates with the USAccess sponsor to ensure the record in USAccess is updated to terminate the badge of departing personnel.
- j. Assists contracting officer representatives (CORs) and contractor (FSOs) in understanding and submitting the documentation required for entering facility clearance and classified contract information into the Safeguards and Security Information Management System (SSIMS). [Chapter 4, Foreign Ownership, Control, or Influence \(FOCI\) & Facility Clearance \(FCL\); and Classified Contract Registration of the HQFMSP](#) explains the process in more detail.
- k. Initiates requests for the establishment and termination of Security Areas, ensure these areas are configured to perform classified work, and maintain current access lists, visitor logs, and signage for these areas.
- l. Assists in establishing and maintaining the integrity of Limited Areas (LA) and Vault-Type Rooms (VTR) in accordance with [Chapter 2, LAs & VTRs of the HQFMSP](#).
- m. Nominates personnel for security training and maintain records of CMPC and other security related training in the Appendix to the HQFMSP (see (3) below).
- n. Serves as points of contact on CMPC matters, including providing advice and assistance in the receipt, marking, storage, handling, discussion, transmission, and destruction of classified matter.

- o. Advises and assists the heads of HQ elements in establishing, manning, and operating Classified Document Control Stations (CDCS) and appointment of CDCS personnel in accordance with [Chapter 5, CMPC of the HQFMSP](#).
- p. Provide the names of the Express Mail Document Control (EMDC) designees as well as the Classified Mailing Address (CMA) designees to the CMPC Program manager and provide updates or revisions as required in accordance with [Chapter 5, CMPC of the HQFMSP](#).
- q. Provide and maintain copies of the element's signed "Hand-Carry Briefing" and "Contingency Plan" for the designated Hand-Carry personnel or Courier in accordance with [Chapter 5, CMPC of the HQFMSP](#). Provide list of designated Hand Carry/Courier personnel within element to CMPC Program manager for issuance of official credentials. Revisions and updates to the list must also be provided when required. Serves as points of contact on matters related to the receipt, marking, storage, handling, discussion, transmission, and destruction of Controlled Unclassified Information (CUI). See [Chapter 5, CMPC](#) and [Chapter 13, CUI of the HQFMSP](#) for more information.
- r. Assists personnel in understanding and complying with visitor access control procedures in place at HQ facilities as outlined in [Chapter 1, Physical Security of the HQFMSP](#).
- s. Assists personnel in understanding and complying with procedures for controlling Unclassified Foreign Visits and Assignments and Classified Foreign Visits. Has access to Foreign Access Central Tracking System (FACTS) to ensure the required information is entered into the system. Assists in the preparation of required security plans, ensuring hosts and escorts understand their responsibilities, to include the requirements necessary for sharing classified information with foreign nationals; and ensuring the heads of HQ elements approve these visits and/or assignments. [Chapter 6, Foreign Interaction of the HQFMSP](#) goes into more detail on these requirements.
- t. Assists the HQ Survey Team in conducting self-assessments and initial, periodic, special, and termination surveys as referenced in [Chapter 7, DOE S&S Survey Program of the HQFMSP](#).
- u. Assists in the development, submission, and verification of corrective action plans (CAPs) to remedy security discrepancies identified in self-assessments and surveys. Reference [Chapter 7, DOE S&S Survey Program of the HQFMSP](#).
- v. Receives and reports incidents of security concern to the HQ IOSC Program Manager, and if appointed as an Inquiry Officer, conduct required security inquiries or assist the appointed inquiry officer in conducting the inquiry. Assist supervisors in issuing security infractions. Reference [Chapter 11, Incidents of Security Concern of the HQFMSP](#) for more on this subject.
- w. Assists personnel in acquiring security equipment, such as security containers, secure communications devices, copy machines approved for

classified processing and shredders that are approved for destruction of classified material. Reminds users of recurring requirements such as inspecting shredders every six months, and re-keying (to include sending out notices of emergency re-key requirements) and testing. Although the classified container's custodian is responsible for the container, the HSO assists with combination changes for classified storage containers within the organization. The HSO will also complete necessary documentation to ensure the safe is empty and ready to transfer or excess.

- x. Prepares requests concerning security operations for Equivalencies and Exemptions from DOE Orders in accordance with [Chapter 16, Equivalencies and Exemptions of the HQFMSP](#).
 - y. Assists in monitoring and facilitating the completion of security awareness briefings, including the Annual Security Refresher Briefing (ASRB).
3. Develops and maintains an organizational [HSO Organizational Appendix Template Instructions](#). The HSO Program Manager can aid with setting up an Appendix. The Appendix should reflect the security posture of the program office and should be updated, as necessary.
 4. Attends quarterly HSO meetings and training sessions and other activities recommended by the HSO Program Manager.
 5. Complies with Hand carry and Authorization Program Standard Operating Procedure that is found in [Chapter 5, CMPC of the HQFMSP](#).

Alternate Headquarters Security Officers

1. Supports the HSO as a point of contact for their element for security-related matters.
2. Assists the HSO in performing the following duties in accordance with procedures set forth in the HQFMSP.
 - a. Assists in obtaining, assembling, approving, and/or submitting the documentation required to obtain a security badge for entering HQ facilities. The requirements and the process for preparing and submitting these documents can be found in [Chapter 3, Personnel Security of the HQFMSP](#).
 - b. Assists in obtaining, assembling, approving and/or submitting the documentation required to obtain a security clearance in accordance with [Chapter 3, Personnel Security of the HQFMSP](#).
 - c. Annually reviews the need for retaining personnel security clearances.
 - d. Assists in ensuring personnel complete the documentation required for security clearance reinvestigations. See [Chapter 3, Personnel Security of the HQFMSP](#), for specific details on this process.
 - e. Works with supervisors and managers to ensure clearance holders notify the Office of HQ Personnel Security Operations of reportable events and

Absences of 90 days or more. For a complete list of reporting requirements reference [Chapter 3, Personnel Security of the HQFMSP](#).

- f. Assists in the transfer of security clearance and access information to other DOE and Federal organizations so organizational personnel may attend classified meetings in accordance with [Chapter 3, Personnel Security of the HQFMSP](#).
- g. Coordinates with the USAccess sponsor to ensure the record in USAccess is updated to terminate the badge of departing personnel.
- h. Assists contracting officer representatives (CORs) and contractor (FSOs) in understanding and submitting the documentation required for entering facility clearance and classified contract information into the Safeguards and Security Information Management System (SSIMS). [Chapter 4, FOCI & FCL of the HQFMSP](#) explains the process in more detail.
- i. Assists with the establishment and termination of Security Areas, ensure these areas are configured to perform classified work, and maintain current access lists, visitor logs, and signage for these areas.
- j. Assists in establishing and maintaining the integrity of Limited Areas (LA) and Vault-Type Rooms (VTR) in accordance with [Chapter 2, LAs & VTRs of the HQFMSP](#).
- k. Nominates personnel for security training and maintain records of CMPC and other security related training in the Appendix to the HQFMSP as described in the [HSO Organizational Appendix Template Instructions](#).
- l. Serves as points of contact on CMPC matters, including providing advice and assistance in the receipt, marking, storage, handling, discussion, transmission, and destruction of classified matter.
- m. Advises and assist the heads of HQ elements in establishing, manning, and operating Classified Document Control Stations (CDCS) and appointment of CDCS personnel in accordance with [Chapter 5, CMPC of the HQFMSP](#).
- n. Serves as points of contact on matters related to the receipt, marking, storage, handling, discussion, transmission, and destruction of CUI. See [Chapter 5, CMPC of the HQFMSP](#) and [Chapter 13, CUI of the HQFMSP](#) for more information.
- o. Assists personnel in understanding and complying with visitor access control procedures in place at HQ facilities as outlined in [Chapter 1, Physical Security of the HQFMSP](#).
- p. Assists personnel in understanding and complying with procedures for controlling Unclassified Foreign Visits and Assignments and Classified Foreign Visits. Has access to Foreign Access Central Tracking System (FACTS) to ensure the required information is entered into the system. Assisting in the preparation of required security plans, ensuring hosts and escorts understand their responsibilities, to include the requirements necessary for sharing classified information with foreign nationals; and

ensuring the heads of HQ elements approve these visits and/or assignments. [Chapter 6, Foreign Interaction of the HQFMSP](#) goes into more detail on these requirements.

- q. Assists the HQ Survey Team in conducting self-assessments and initial, periodic, special, and termination surveys as referenced in [Chapter 7, DOE S&S Survey Program of the HQFMSP](#).
 - r. Assists in the development, submission, and verification of corrective action plans (CAPs) to remedy security discrepancies identified in self-assessments and surveys. Reference [Chapter 7, DOE S&S Survey Program of the HQFMSP](#).
 - s. Receives and reports incidents of security concern to the HQ IOSC Program Manager, and if appointed as an Inquiry Officer, conduct required security inquiries or assist the appointed inquiry officer in conducting the inquiry. Assists supervisors in issuing security infractions. Reference [Chapter 11, Incidents of Security Concern of the HQFMSP](#) for more on this subject.
 - t. Assists personnel in acquiring security equipment, such as security containers, secure communications devices, copy machines approved for classified processing and shredders that are approved for destruction of classified material. Reminds users of recurring requirements such as re-keying (to include sending out notices of emergency re-key requirements) and testing. Although the classified container's custodian is responsible for the container, the HSO assists with combination changes for classified storage containers within the organization.
 - u. Prepares requests concerning security operations for Equivalencies and Exemptions from DOE Orders in accordance with [Chapter 16, Equivalencies and Exemptions of the HQFMSP](#).
 - v. Assists in monitoring and facilitating the completion of security awareness briefings, including the Annual Security Refresher Briefing (ASRB).
 - w. Develops and maintains an organizational Appendix to the HQFMSP as described in the [HSO Organizational Appendix Template Instructions](#).
- 3. The HSO Program Manager can aid with setting up an Appendix. The Appendix should reflect the security posture of the program office and should be updated, as necessary.
 - 4. Attends quarterly HSO meetings and training sessions and other activities recommended by the HSO Program Manager.
 - 5. Complies with Hand carry and Courier Program Standard Operating Procedure.

HSO Representative

- 1. Assists the HSO and Alternate HSO in performing the following duties in accordance with procedures set forth in the HQFMSP.

- a. Assists in obtaining, assembling, and/or submitting the documentation required to obtain a security badge for entering HQ facilities. The requirements and the process for preparing and submitting these documents can be found in [Chapter 3, Personnel Security of the HQFMSP](#).
- b. Assists in obtaining, assembling, and/or submitting the documentation required to obtain a security clearance in accordance with [Chapter 3, Personnel Security of the HQFMSP](#).
- c. Annually reviews the need for retaining personnel security clearances.
- d. Assists in ensuring that personnel complete the documentation required for security clearance reinvestigations. See [Chapter 3, Personnel Security of the HQFMSP](#), for specific details on this process.
- e. Works with supervisors and managers to ensure that clearance holders notify the Office of HQ Security Vetting of reportable events and absences of 90 days or more. For a complete list of reporting requirements reference [Chapter 3, Personnel Security of the HQFMSP](#).
- f. Assists in the transfer of security clearance and access information to other DOE and Federal organizations so organizational personnel may attend classified meetings in accordance with [Chapter 3, Personnel Security of the HQFMSP](#).
- g. Coordinates with the USAccess sponsor to ensure the record in USAccess is updated to terminate the badge of departing personnel.
- h. Assists contracting officer representatives (CORs) and contractor (FSOs) in understanding and submitting the documentation required for entering facility clearance and classified contract information into the Safeguards and Security Information Management System (SSIMS). [Chapter 4, FOCI & FCL of the HQFMSP](#) explains the process in more detail.
- i. Assists in establishing and maintaining the integrity of Limited Areas (LA) and Vault-Type Rooms (VTR) in accordance with [Chapter 2, LAs & VTRs of the HQFMSP](#).
- j. Nominates personnel for security training and maintains records of CMPC and other security related training in the Appendix to the HQFMSP as described in the [HSO Organizational Appendix Template Instructions](#).
- k. [Serves as point of contact on CMPC matters, including providing advice in the receipt, marking, storage, handling, discussion, transmission, and destruction of classified matter.](#)
- l. Advises and assists the heads of HQ elements in establishing, manning, and operating Classified Document Control Stations (CDCS) and appointment of CDCS personnel in accordance with [Chapter 5, CMPC of the HQFMSP](#).
- m. Serves as point of contact on matters related to the receipt, marking, storage, handling, discussion, transmission, and destruction of Controlled

Unclassified Information (CUI). See [Chapter 5, CMPC of the HQFMSP](#) and [Chapter 13, CUI of the HQFMSP](#) for more information.

- n. Assists personnel in understanding and complying with visitor access control procedures in place at HQ facilities as outlined in [Chapter 1, Physical Security of the HQFMSP](#).
 - o. [Assists personnel in understanding and complying with procedures for controlling Unclassified Foreign Visitors and Assignments and Classified Foreign Visits](#). Have access to Foreign Access Central Tracking System (FACTS) to ensure the required information is entered into the system. Assists in the preparation of required security plans, ensuring hosts and escorts understand their responsibilities, to include the requirements necessary for sharing classified information with foreign nationals; and ensuring the heads of HQ elements approve these visits and/or assignments. [Chapter 6, Foreign Interaction of the HQFMSP](#) goes into more detail on these requirements.
 - p. Assists the HQ Survey Team in conducting self-assessments and initial, periodic, special, and termination surveys as referenced in [Chapter 7, DOE S&S Survey Program of the HQFMSP](#).
 - q. Assists personnel in acquiring security equipment, such as security containers, secure communications devices, copy machines approved for classified processing and shredders that are approved for destruction of classified material. Reminds users of recurring requirements such as re-keying (to include sending out notices of emergency re-key requirements) and testing. Although the classified container's custodian is responsible for the container, the HSO assists with combination changes for classified storage containers within the organization.
 - r. Assists in monitoring and facilitating the completion of security awareness briefings, including the Annual Security Refresher Briefing (ASRB).
- 2. Attends quarterly HSO meetings and training sessions and other activities recommended by the HSO Program Manager.
 - 3. Complies with the Hand Carry and Courier Program Standard Operating Procedure.

Points of Contact

For more information on the HSO Program and the duties identified in this chapter, an email can be sent to the [HQ HSO Program](#), or by calling them at, (301) 903-7189 or (301) 903-2644.

Acronyms

A

AAAP	Accelerated Access Authorization Program
ACREM	Accountable Removable Classified Media (outdated term)
APR	Accountable Property Representative
ATS	Applicant Tracking System

B

BAO	Building Access Only

C

C	Confidential
CAS	Central Alarm Station
CCDF	Centralized Classified Destruction Facility
CCEB	Combined Communications Electronic Board
CDC	Child Development Center
CDCS	Classified Document Control Station
CF	Office of the Chief Financial Officer (routing symbol)
CF-30	Office of the Budget
CF-80	Office of Risk Management
C/FGI-MOD	Confidential/Foreign Government Information – Modified Handling Authorized
CFR	Code of Federal Regulations
CI	Counterintelligence (usual meaning)
CI	Critical Information (Chapter 8)
CI	Office of Congressional and Intergovernmental Affairs (routing symbol) (Chapter 5)
CI-1	Director, Office of Congressional and Intergovernmental Affairs (Chapter 5)
CMA	Classified Mailing Address
CMPC	Classified Matter Protection and Control
CNWDI	Critical Nuclear Weapons Design Information
CO	Contracting Officer
COMSEC	Communications Security
COR	Contracting Officer's Representative
CPCI	Central Personnel Clearance Index
CSCS	Contract Security Classification Specification

D

DARTS	Departmental Audit Reports Tracking System
DC	Derivative Classifier
DOE	U.S. Department of Energy
DOS	U.S. Department of State
DS/C/DC	DOS Bureau of Diplomatic Security/Office of Diplomatic Courier Services
DV	Distinguished Visitor

E

EMDC	Express Mail Document Control
e-QIP	Electronic Questionnaires for Investigations Processing

F

F	Form
FAA	Federal Aviation Administration
FACTS	Foreign Access Central Tracking System
FDAR	Facility Data and Approval Record
FGI	Foreign Government Information
FIPS	Federal Information Processing Standard
FOCI	Foreign Ownership, Control, or Influence
FRD	Formerly Restricted Data
FSO	Facility Security Officer

G

GAO	Government Accountability Office
GSA	General Services Administration

H

HC	Office of Human Capital (routing symbol)
HQ	Headquarters
HQFMSP	Headquarters Facilities Master Security Plan
HS	Office of Health, Safety and Security (routing symbol)
HS-1.2	Office of Corporate Security Strategy, Analysis, and Special Operations
HS-52	Office of Security Assistance
HS-53	Office of Departmental Personnel Security
HS-60	Office of Classification
HS-90	Office of Headquarters Security Operations
HS-91	Office of Physical Protection
HS-92	Office of Information Security
HS-93	Office of Headquarters Personnel Security Operations
HR	Human Resources
HSO	Headquarters Security Officer
HSPD	Homeland Security Presidential Directive
HSPD-12	Homeland Security Presidential Directive 12

I

IAA	Interim Access Authorization
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IN	Office of Intelligence and Counterintelligence (routing symbol)
IN-20	Office of Counterintelligence
IPA	Intergovernmental Personnel Act
IR	Infrared
ISFD	Industrial Security Facilities Database
ISOO	Information Security Oversight Office
ISSO	Information System Security Officer

K

KMP	Key Management Personnel

L

LA	Limited Area
LSSO	Local Site-Specific Only

M

MA	Office of Management (routing symbol)
MA-40	Office of Administration
MA-43	Office of Logistics and Facility Operations
MA-431	Facilities Management Operations
MA-432	Office of Project Integration and Logistics Operations
MA-60	Office of Acquisition and Project Management

N

NA	National Nuclear Security Administration (routing symbol)
NA-3.5	NNSA Office of Congressional, Intergovernmental and Public Affairs
NA-70	Office of the Associate Administrator for Defense Nuclear Security
NA-71	NNSA Security Operations Division
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NNPI	Naval Nuclear Propulsion Information
NNSA	National Nuclear Security Administration
NOCONTRACT	No Dissemination to Contractors
NODIS	No Distribution
NOFORN	No Foreign Dissemination
NP	Non-Possessing
NSA	National Security Agency
NSI	National Security Information
NTC	National Training Center

O

OCIO	Office of the Chief Information Officer
OF	Optional Form
OGA	Other Government Agency
OPM	Office of Personnel Management
ORCON	Originator Controlled Information

P

PACS	Physical Access Control System
PADS	Procurement and Assistance Data System
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PRO	Procurement Request Originator
Property Pass	Property Removal Authorization
PROPIN	Proprietary Information
PTS	Protective Distributions System

R

RD	Restricted Data
RELIDO	Releasable by Information Disclosure Official
REL TO	Authorized for Release to
RF	Radio Frequency

S

S	Secret
S/RD	Secret/Restricted Data
SAACS	Security Alarm and Access Control System
SAP	Special Access Program
SAPOC	Special Access Program Oversight Committee
SC	Office of Science (routing symbol)
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SF	Standard Form
SF-701	Security Area Checklist
SF-85	Questionnaire for Non-Sensitive Positions
SF-86	Questionnaire for Sensitive Positions/Questionnaire for National Security Positions
SF 86C	Standard Form 86 Certification
SNM	Special Nuclear Material
SPECAT	Special Category
S&S	Safeguards and Security
SSA	Statement of Security Assurance
SSAN	Social Security Account Number
SSIMS	Safeguards and Security Information Management System
SSO	Special Security Officer
STE	Secure Terminal Equipment

T

TFNI	Transclassified Foreign Nuclear Information
TLA	Temporary Limited Area
TS	Top Secret
TSA	Transportation Security Administration
TSCM	Technical Surveillance Countermeasures
TSCMO	Technical Surveillance Countermeasures Officer
TSCMOM	Technical Surveillance Countermeasures Operations Manager

U

UK	United Kingdom
UPS	United Parcel Service
USPS	United States Postal Service

V

VIP	Very Important Person
vIPER	vIPER Universal Secure Phone
VTC	Video Teleconferencing
VTR	Vault-Type Room

W

WAP

WNINTEL

Wireless Access Point

Warning Notice: Sensitive Intelligence Methods or Sources Involved

This page intentionally left blank.