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 (AU-41) and the Office of HQ Personnel Security Operations (AU-43). All documents related to requests for security badges must first be submitted to AU-43 and that office, in turn, will forward the documentation to AU-41 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 AU-43 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 AU-41. 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 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 AU-41 positions identified in this chapter, call (202) 586-8075 or (301) 903-0145.

For the names and contact information for those occupying the AU-43 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)

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, AU, 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 AU-41, signs the "Security Official Concurrence" portion of Section N and forwards the DOE F 473.2 to AU-43 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 AU-43. 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 AU-43 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 (AU-40) 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. AU-43 adjudicates the report for Federal and contractor security clearance candidates to determine whether the applicant qualifies for a clearance and an HSPD-12 badge. AU-43 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 AU-41 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) 903-7189 or (301) 903-2644.

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 AU-41 for information and dissemination.

Other Exceptions:

Other exceptions to the policy on Prohibited Articles may be requested via memorandum to the Director, AU-41. 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, AU-41 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 XXXXXXXXX

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.

AU-41 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.
- All personnel who have badges which are encoded to grant access through the turnstiles are subject to random inspection at all HQ facilities.
- DOE Federal and contractor employees issued a temporary badge through the Passage Point system are required to be inspected and 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 vehicle 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 AU-41 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 (301) 903-7189 or (301) 903-2644.

Section 105
Access Control

This section describes methods for controlling access to HQ facilities and detecting unauthorized intrusions into secure areas. AU-426441 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. C-CURE – 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 (LAs) 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 AU-41.

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 an LA, 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 LAs, VTRs, and TLAs; 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 LAs 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, be issued a temporary badge through the Passage Point system, and submit to inspection prior to entry.

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, AU-40 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, AU-40 waived this requirement, provided that the worker logs in each day on initial entry and final departure.

Accessing LAs and VTRs:

Authorized individuals entering an LA 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 an LA or VTR is first established (see Section 201, Establishing, Maintaining, and Deactivating LAs, VTRs, and TLAs) 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 AU-41, 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, AU-41. 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, AU-40. 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, AU-43 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 AU-41; 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. AU-41 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 AU-41 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, AU-41 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 (301) 903-7189 or (301) 903-2644.

C-CURE 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, AU-41
"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. *Use a separate memo for each room access list.* Do not cross reference other access lists.
Effective date:	Select a date several days in the future to allow AU-41 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, AU-41
"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. *Use a separate memo for each room access list*. Do not cross reference other access lists.
Effective date:	Select a date several days in the future to allow AU-41 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, AU-43

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, AU-41
"From":	Must be from the element's HSO, Alternate HSO, a senior Federal official within the program element, or the Director, AU-40
"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, AU-43 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, AU-40 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.

AU-41 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 an LA, 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 must enroll their badges at the self-service kiosk before gaining turnstile access. Those who cannot use the kiosk must proceed to the reception desk to receive a temporary Passage Point paper badge and submit to inspection prior to entry. 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 those who cannot use the kiosk must proceed to the reception desk to receive a temporary Passage Point paper badge. 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 Passage Point visitor badge indicating the visitor's security clearance level. Individuals receiving such a Passage Point visitor badge must submit to inspection prior to entry.

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.

Common Access Card (CAC):

Visitors in possession of a CAC must process through the automated kiosk in the Forrestal or Germantown main lobby or those who cannot use the kiosk must proceed to the reception desk to receive a temporary Passage Point paper badge and submit to inspection prior to entry.

Pre-Announcements:

When an HQ employee expects a visitor, the employee can pre-announce the visit to AU-41 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 AU-41 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 an LA 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.

Exemptions:

All Honor/Color Guard personnel entering a HQ facility for the official performance of duty who possess a CAC will be exempted from receiving a Passage Point badge and undergoing inspection. Use of the automated kiosk in the Forrestal and Germantown Main Lobby is encouraged but not mandatory.

All armed credentialed Law Enforcement Officers (Uniformed or Plain Clothes) on official business will not be subjected to inspection once they have presented their credentials and been processed through the automated Passage Point system.

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.

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
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 and 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 AU-41 a current and complete electronic list of Property Pass Signers. AU-41 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 AU-41 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, AU-40 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.

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.