Chapter 3 Revision History:

July 12, 2023 – Entire chapter was updated.

Chapter 3
Personnel Security

This chapter covers the security procedures for Department of Energy (DOE) Headquarters (HQ) that implement the Personnel Security Program in accordance with applicable Federal and DOE requirements:

- 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*
- U.S. Office of Personnel Management memorandum, dated December 15, 2020, entitled, *Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirement for Suspension or Revocation of Eligibility for Personal Identity Verification Credentials*
- 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 472.2A, *Personnel Security*
- DOE Order 475.1, *Counterintelligence Program*

The DOE HQ Personnel Security Program is designed to ensure DOE HQ 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 only personnel who meet defined Federal standards for honesty, reliability, and trustworthiness are allowed such access.

There is a total of 7 Cognizant Personnel Security Offices (CPSO) across the DOE complex handling security clearance related matters: (1) Headquarters, (2) Idaho, (3) Naval Reactors, (4) National Nuclear Security Administration (NNSA) Albuquerque Complex, (5) Richland, (6) Savannah River, and (7) Science Consolidated Service Center. The CPSO for HQ is the Office of Environmental, Health, Safety, and Security in the Office of Headquarters Personnel Security Operations (EHSS-43). The information in this Chapter applies only to security clearance requests processed and granted by EHSS-43 as well as HSPD-12 requests processed and granted by EHSS-74. 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 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 302.
- Section 302 covers the procedures for acquiring new security clearances.
- Section 303 covers other actions that affect security clearances such as transfers, extensions, upgrades, downgrades, and cancellations.
- Section 304 covers the requirements for reporting information that may affect the retention of a security clearance.
- Section 305 covers the procedures for accessing the electronic questionnaire and completing the process required for those seeking a security clearance and an HSPD-12 security badge.
- Section 306 covers the annual process that Headquarters Security Officer (HSO) 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 307 covers procedures for passing security clearance information to organizations hosting classified meetings.

Please visit our Customer SharePoint Site to stay abreast of all Personnel Security information!

Section 301
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)." 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 is required to go through the HSPD-12 process?

Personnel supporting DOE for 6 months or more, whether a Federal or a contractor employee, who do not require a security clearance (access authorization) but do require physical and/or 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.

Uncleared Federal Employees PIV requests are submitted to the Office of Operations and Support, EHSS-74, send email to HQ Federal PIV.

Uncleared Contract Employees PIV requests are submitted to the Office of Headquarters Personnel of Security Operations, EHSS-43, send email to Personnel Security.

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 302 for instructions on the security clearance process.

NOTE: EHSS-43 is authorized to refrain from processing HSPD-12 requests involving persons on parole or probation for a felony offense until they have completed their period of parole or probation.

Requirements for HSPD-12 process:

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 into the USAccess system.

2. Enrollment – After the sponsor enters the required information into *USAccess Program*, the system will automatically contact the employee via e-mail with instructions for scheduling an appointment to enroll at a USAccess Credentialing Center for fingerprints and a photograph. 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 request is submitted.

   a. If the employee's fingerprints are deemed invalid in USAccess, the Sponsor will be notified to cancel the Reprint and initiate a Reissuance, which will prompt the employee to be fingerprinted again.

      NOTE: For assistance with Reissuance please contact the DOE USAccess Helpdesk.

   b. If the employee's fingerprints are returned from Defense Counterintelligence and Security Agency (DCSA) as unclassifiable, the Sponsor will be notified that a second set of prints is required. The HSO will initiate a re-enrollment utilizing the Card Action Wizard in the USAccess Sponsor Utility Portal.

      NOTE: It is the responsibility of the Sponsor and the employee to notify EHSS-43 or EHSS-74 when the employee has been re-fingerprinted. USAccess does not have an automatic notification system.

3. HSPD-12 Badge for Non-U.S. citizens: If subject is a non-U.S. citizen, please refer to DOE O 142.3B, Part 4 – *Unclassified Foreign National Access Program* for additional steps that must be completed before requesting a HSPD-12 badge.

   Submission of HSPD-12 Badge Documentation – The following documents are required:

   Uncleared Federal Employees PIV requests are submitted to the Office of Operations and Support, EHSS-74, send email to HQ Federal PIV:.

   a. **Federal Employees – (Responsibility: Element's Human Capitol (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
      - Optional Form 8 (OF 8) – Signatures required.
      - Position Designation Record (PDR)
      - Position Description (PD) – Signature required

Uncleared Contract Employees PIV requests are submitted to the Office of Headquarters Personnel of Security Operations, EHSS-43, send email to Personnel Security.

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 –Designator's name and title required, no signature required.

Note: The employee must record their 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 Federal Credentialing Services.

HSPD-12 Process:

1. Request received – PIV request will be reviewed for completion and accuracy. The request will be returned to the requestor 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 request has all required documents.

2. Questionnaires Processing – See Section 305 of the Headquarters Facilities Master Security Plan (HQFMSP) for more information.

3. Background Investigation – Once the Questionnaires process is completed, the applicant's information is automatically forwarded to DCSA.

4. Preliminary Approval – The respective EHSS office will Preliminary Approve an employee if both the fingerprints and the Questionnaires (SF85 or SF85P) 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 the employee cannot be Preliminary Approved, they will continue to use the Local Site Specific Only (LSSO) badge unless otherwise directed. An email will be sent to the 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 – The respective EHSS office will adjudicate and make a final determination on the background investigation received from DCSA. No additional information should be required from the HSO 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.

Information on the issuance and determination process for HSPD-12 credentialing can be found in the December 15, 2020, Office of Personnel Management (OPM) Memorandum entitled, *Credentialing Standards Procedures for Issuing Personal Identity Verification*

Cards under HSPD-12 and New Requirement for Suspension or Revocation of Eligibility for Personal Identity Verification Credentials and also in DOE O 206.2, Identity, Credential, and Access Management.

PIV Transfer

1. Transfer – An individual is transferring from one HQ program office to another HQ program office. The HSO of the losing organization must out process the individual; have the individual complete a BAO Termination Report. If the losing organization is aware the individual will be supporting another HQ program office, the BAO Termination report should annotate "This individual is transferring to (Name of Element)." The BAO Termination Report must be emailed to Personnel Security.

Contractor PIV Transfer

The gaining HQ element is required to submit a complete PIV request to EHSS-43 and ensure the individual's USAccess record is updated to reflect the new sponsorship change. The following documents required are for contractor transfer:

- DOE F 206.4, *The Information Sheet for Sponsorship of HSPD-12 Credential*
- OF-306, *Declaration for Federal Employment*
- PDR, *Position Designation Record*
- DOE F 473.2, *Security Badge Request Card*

Other documentation may be requested by Personnel Security, EHSS-43

Federal PIV Transfer

If additional information is required to determine which type of transfer is being completed, please contact: Office of HR Operations and Compensation (OHROC).

PIV Termination

If any individual who possesses a DOE issued badge is separating from DOE the HSO must out process the individual; have the individual complete a BAO Termination Report and send to the respective security element, EHSS-43 (contract employees) and EHSS-74 (Federal employees) and update the USAccess database.

Please visit our Customer SharePoint Site to stay abreast of all Personnel Security information!

Points of Contact:

Office of Headquarters Personnel Security (EHSS-43) (301) 903-4175, or email Personnel Security

Office of Operations and Support (EHSS-74) (240)-220-4115, or email HQ Federal PIV

Section 302
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, 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:

- Q clearance
- L clearance
- TS clearance
- S clearance
- C clearance

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

In addition, 3 categories of classified matter are identified:

- Restricted Data (RD)
- Formerly Restricted Data (FRD)
- National Security Information (NSI)

The employee must have a security level clearance consistent with their assignment. Common combinations are reflected in the table, shown on the next page.

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 EHSS-43 to ensure 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.
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.

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*.

Responsibilities:

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

1. Contractor Employees – HQ contractor employees requiring security clearances must work with their Facility Security Officer (FSO). The FSO coordinates with the element's HSO to submit the security clearance request package.
2. Federal Employees – Each HQ element has established its own procedure for assisting Federal employees requiring a security clearance.
3. Intergovernmental Personnel Act (IPA) Employees – IPA employees are processed the same as contractor employees, with the exception that 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.
4. Other Government Agency Detailees – Federal employees employed by another agency 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.
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 who do not access classified information may be excluded (exclusion resolution). For more information regarding the processing of the Foreign Ownership, Control or Influence organizations and their Key Management Personnel, refer to Chapter 4, *Foreign Ownership, Control or Influence; Facility Clearance; and Classified Contract Registration*, Section 401-2.
6. All Others – Other categories of people who might require a DOE security clearance. These include Federal or local law enforcement agency personnel participating in joint task forces, members of Presidential or Congressional commissions, U.S. Congressmen and Congresswomen representing districts with DOE facilities, governors and 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 EHSS-43 to determine the required documentation and who will sponsor the security clearance.

Requesting a Security Clearance:

Because security clearance forms contain Personally Identifiable Information (PII), the forms must be protected in accordance with the Privacy Act of 1974. Refer to Chapter 13, *Controlled Unclassified Information*, for specific guidance on the transmission and destruction of PII.

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.

2. Sponsorship in USAccess:

   a. **Federal and IPA Employees**: The HC specialist sponsors and enrolls the applicant in USAccess. See Chapter 3, Section 301, *HSPD-12 Credential for Personal Identity Verification (PIV)* for *Requesting a HSPD-12 Credential*, items 1 and 2 for more information.

   b. **Contractor Employees**: The HSO coordinates with the designated person in their element to sponsor and enroll the contractor into USAccess. See Chapter 3, Section 301, *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 EHSS-43. For information on how to locate a USAccess Credentialing Center, how to schedule an appointment, and the required documents for enrollment, go to USAccess Program on the web.

3. Documentation Needed for Clearance Requests:

   a. **Federal Employees**: The following documents are required:

      - DOE F 5631.18, *Security Acknowledgement*
      - A copy of the applicant's current resume
      - Position Description (PD)
      - OF-8
      - Position Designation Record (PDR) – Must be signed.
      - Template 5633.33, *Personnel Security Clearance Action Request*

   b. **Contractor Employees**: The contractor's Facility Security Officer (FSO) must obtain and prepare the required application documentation, including:

      - DOE F 5631.18, *Security Acknowledgement*
      - DOE F 473.2, *Security Badge Request* (if applicable)
      - PDR – Does not have to be signed at this time.
      - Template 5633.33, *Personnel Security Clearance Action Request*

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 the Department of Energy Acquisition Regulation (DEAR), Part 952.204.2 *Security Requirements* and 10 CFR 707, *Workplace Substance Abuse Programs at the DOE Sites*.

   The pre-employment screening must include:

   - Verifying the applicant's educational background, including a high school diploma obtained within the past five (5) years, and degrees or diplomas granted by an institution of higher learning.
   - Contacting the applicant's employer(s) of the past three (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 Sample Letter Reporting Results of Contractor Pre-employment Checks and Drug Testing) to EHSS-43 stating:

   - A pre-employment review was conducted.
   - The date(s) the review was conducted.
   - The identity of each entity providing information about the applicant.
   - Certification 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 90 calendar days of the date the applicant certifies their SF-86.

   Drug test results must have a Medical Review Officer's (MRO) name in accordance with 10 CFR 707.13, *Medical review of results of tests for illegal drug use*.

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**: Contracting company must establish their own drug testing programs, as required by 10 CFR 707, *Workplace Substance Abuse Programs at DOE Sites*. The company 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.

A copy of the laboratory report showing the results of the drug test must be included in the applicant's security clearance request package. The report must contain the Medical Review Officer's name in accordance with 10 CFR 707.13, *Medical review of results of tests for illegal drug use*.

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

NOTE: Security clearance requests with positive drug test results will not be processed.

6. 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 their duties" is inadequate and will not be accepted by EHSS-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."

7. 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 EHSS-43 via eCAR. Access to eCAR is attained by individuals who hold a security clearance or has an equivalent background investigation that has been favorably adjudicated and is within scope completing PERSEC F 5630.27, *Clearance Action Tracking System.* A copy of the form can be obtained by emailing Personnel Security or CATS Support Team. Completed forms must be signed and returned to the Personnel Security mailbox for EHSS-43 approval and forwarding to the CATS Support Team for processing. When the account is created, the requestor will

receive an email with instructions for logging into eCAR from the CATS Support team.

8. Submitting a Request for a Security Clearance – Once all of the requirements in the paragraphs above have been met, the HSO creates an eCAR request and uploads the following forms as attachments in the Clearance Action Tracking Systems (CATS):

   Federal Employees:
   DOE F 5631.18, *Security Acknowledgement*
   PD
   OF-8
   PDR
   Drug Test Results
   Current resume
   Template 5633.33, *Personnel Security Clearance Action Request*

   Contractor Employee:
   DOE F 5631.18, *Security Acknowledgement*
   PDR
   Drug Test Results
   Pre-employment letter
   DOE F 473.2, *Security Badge Request* (if applicable)
   Template 5633.33, *Personnel Security Clearance Action Request*

9. EHSS-43 Review of Documentation Submitted – EHSS-43 reviews documents to verify completeness, eCAR submittals found to be inaccurate or incomplete will be rejected and an email will be sent explaining the corrections needed. When the corrections are made, the eCAR is resubmitted to EHSS-43.

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

10. Questionnaire Processing – See Chapter 3, Section 305, *Questionnaires for National Security, Non-Sensitive, or Public Trust Positions* of the HQFMSP for more information.

11. Preliminary Approval – EHSS-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 EHSS-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 the HSO, and the Badge Office informing them of the Preliminary Approval or extension of the LSSO badge. Please refer to Chapter 1, *Physical Security*, for additional information on badges. Please note Federal employees requiring a clearance for their

position will not be preliminary approved unless a waiver of the pre-appointment investigative requirement is approved by HC.

12. Background Investigation – Once the electronic questionnaire process is completed, the applicant's information is automatically forwarded to DCSA. DCSA provides the results of the background investigation to EHSS-43 for review.

NOTE: 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 is made concerning the clearance request. This system will only track the status of an investigation that is requested by DOE. It will not show a status for an investigation requested by any other Federal agency. Applicants may access this site once their electronic questionnaire has been scheduled for the investigation.

Please visit our Customer SharePoint Site to stay abreast of all Personnel Security information!

Points of Contact:

Office of Headquarters Personnel Security (EHSS-43) (301) 903-4175, or email Personnel Security.

Office of Departmental Personnel Security (EHSS-53) (202) 586-3249.

Forms/Samples/Graphics:

DOE F 206.4, Information Sheet for Sponsorship of HSPD-12 Credential

DOE F 473.2, *Security Badge Request*

DOE F 5631.18, *Security Acknowledgement*

Sample Letter Reporting Results of Contractor Pre-employment Checks and Drug Testing

Section 303
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 their security clearance.

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

eCAR Actions:

EHSS-43 reviews all investigative reports and provides unbiased adjudication in accordance with SEAD 4, *National Security Adjudicative Guidelines*. If the background investigation is favorable, EHSS-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 new credential is required, USAccess will be updated by the Sponsor with the appropriate clearance level and a new HSPD-12 badge will be printed. Please refer to Chapter 1, *Physical Security*, for additional information.

1. **Applicant** – An individual who has never held national security access authorization eligibility, or whose national security access authorization eligibility does not meet the requirements of reapproval or reciprocity. The sponsoring HSO of the element must submit an Applicant eCAR request at the risk level and sensitivity commensurate with the responsibilities and duties reflected on the PD and/or PDR. For a list of required forms, please see Chapter 3, Section 302-3, *Requesting A Security Clearance.*

2. **Transfer –** An individual is transferring from one HQ program office to another HQ program office. The losing element must terminate the individual's security clearance because they are no longer performing duties requiring such a clearance. The HSO of the losing organization should out process the individual (refer to Chapter 15, *Out-processing*); have the individual complete a DOE F 5631.29, *Security Termination*; and annotate "This individual is transferring to (Name of Element)" on the DOE F 5631.29. If the HSO is aware the individual will be performing classified work in their 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 Personnel Security.

If the gaining HQ element requires the individual to perform classified work, the HSO of the gaining element must create and submit a Transfer eCAR. The documents required for the eCAR are Template 5633.33, Personnel Security Clearance Action Request, the DOE F 5631.29, *Security Termination* 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 EHSS-43 before the transfer paperwork is received.

If the gaining HQ element does not require the individual to perform classified work, please refer to the section below entitled, "Other Actions, section # 1 Termination."

3. **Reapproval** – An individual had a clearance that was terminated and now needs to be reapproved. A security clearance can be reapproved if the clearance was administratively withdrawn within the last 24 months and the most recent background investigation is within the last 7 years. The sponsoring HSO of the element should submit a Reapproval eCAR request consisting of Template 5633.33, Personnel Security Clearance Action Request, the DOE F 5631.18, *Security Acknowledgement*, the PDR, the PD if a Federal employee, and negative drug test results dated within 90 days of the reapproval eCAR. For contractor employees only, the HSO must also complete a new DOE F 473.2, *Security Badge Request*, and add it to the eCAR request.

4. **Upgrade** – An individual has a DOE L, S, or C clearance but requires a Q or TS clearance. 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. The documents required are Template 5633.33, Personnel Security Clearance Action Request, the PDR, and the PD 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.

5. **Downgrade** – 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 consisting of Template 5633.33, Personnel Security Clearance Action Request, the PDR, and the PD if the individual is a Federal employee. For contractor employees, the HSO must also complete a new DOE F 473.2 and add it to the eCAR request.

6. **Extension** – An individual with a security clearance needs to support an additional DOE element. The HSO of the element requiring the individual's new services must submit a request for Extension in eCAR. 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 their sponsoring element.

    a. Internal Extensions – an individual will be supporting an additional HQ program office.

b. External Extensions – an individual holds a clearance at another CPSO and will be supporting a HQ program office. The clearance needs to be extended to HQ.

c. Required documents for both types of extensions are:

- Template 5633.33 Personnel Security Clearance Action Request
- PDR
- PD (Feds only)
- Badge Request Card (contractors only).

7. **Reciprocity** – The acknowledgement and acceptance of an existing background investigation conducted by an authorized investigative agency, acceptance of a national security eligibility adjudication by an authorized adjudicative agency, and the acceptance of an active national security eligibility determination granted by an executive branch agency. This includes those individuals who are enrolled in a Continuous Evaluation (CE) program and have a deferred periodic reinvestigation. The applicant for reciprocal clearance at DOE 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 EHSS-43 is in possession of derogatory information that has not been mitigated by the applicant's most recent background investigation.

   A reciprocity eCAR includes the Template 5633.33, Personnel Security Clearance Action Request, DOE F 5631.18, Security Acknowledgement, the PDR, the PD if a Federal employee, and negative results of a drug test dated within 90 days of the eCAR request. For contractor employees, the HSO must also complete a new DOE F 473.2, *Security Badge Request*, and add it to the eCAR request.

8. **Temporary Eligibility (Interim Security Clearance)** – Individuals needing temporary access to classified information. Only under exceptional circumstances and when such action is clearly consistent with Departmental and national interests, will a contractor applicant or employee, pending completion of the appropriate investigation, be permitted to have temporary access to classified information. Non-U.S. citizens are not eligible for interim access to classified information or SNM. The Federal Head of Element must prepare a memorandum request to the Director of EHSS-40, that includes a detailed justification explaining why:

   - A serious delay of, or interference in, an operation or project essential to a DOE program will occur unless the processed 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 EHSS-43. Requests submitted with justifications that do not meet the requirements as specified above will be returned with no action taken by EHSS-43. It is important to note that the submission of a request for an interim clearance does not guarantee the applicant will be granted an interim clearance. Both the applicant and Federal Head of Element will be notified in writing of the final decision.

9. **Reinvestigations** – A newly completed SF-86 must be collected every 5 years for Q and TS, and every 10 years for L and S until Trusted Workforce 2.0 is implemented. Trusted Workforce 2.0 was established to reshape background investigations and overhaul the personnel vetting process by creating a single government-wide system that allows for reciprocity across all Federal organizations. This includes shifting from periodic reinvestigations every 5 to 10 years, towards a Continuous Vetting program, which protects and monitors our trusted workforce in real time.

   Another aspect of the reinvestigation process allows EHSS-43 to conduct reinvestigations on an as-needed basis. EHSS-43 has autonomy to move the reinvestigation onto the Investigative Service Provider or defer the reinvestigation process based on review of the SF-86.

Once a DOE security clearance is granted, the applicant is entered into the CE Program. However, individual must still undergo a background reinvestigation (see Chapter 3, Section 306, Security Clearance Reinvestigations and Verifications).

CE is a real-time review of an individual's background at any time to determine if they continue to meet the requirements to access classified information.

Other Actions:

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

1. **Termination** – An individual with a security clearance is departing DOE or no longer needs a security clearance – The individual's security clearance must be terminated. The HSO out-processes the individual (see Chapter 15, *Out-processing*) and has the individual complete DOE F 5631.29, *Security Termination*. The completed form must be emailed to Personnel Security.

2. **Downgrade** – (Cleared to Uncleared) 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. These forms should be emailed to Personnel Security. A complete PIV request must be submitted if the individual still requires access to a HQ facility. Please

refer to Chapter 3, Section 301, HSPD-12 Credential for Personal Identity Verification (PIV) for the required paperwork and do the following:

- Federal Employees: Email complete paperwork to HQ Federal PIV.
- Contractor Employees: Email complete paperwork to Personnel Security.

A downgrade to BAO action cannot be processed until the losing program office submits a DOE F 5631.29, *Security Termination Statement.* If the downgrade is for a contractor employee, the HSO must also complete and submit a new DOE F 473.2 via email to Personnel Security. EHSS-43 will contact the HSO if any additional paperwork is needed.

3. **Cancellation** – An individual no longer requires a security clearance after the request was submitted to EHSS-43 – The servicing HSO of an individual who is being processed for a security clearance (hasn't been granted yet) but no longer needs it must submit Template 5633.33, *Personnel Security Clearance Action Request* 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 Personnel Security. EHSS-43 will accept an email in lieu of the form as long as an explanation for cancellation is provided.

Administrative Review (AR) Processing:

EHSS-43 cannot approve applicants for security clearance 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 Code of Federal Regulations, Part 710 (10 CFR 710).

The procedures delineated in 10 CFR 710 establish methods for the conduct of the administrative review of questions concerning an individual's eligibility for a security clearance when it is determined that such questions cannot be favorably resolved and outline the notice to the individual, initial decision process, commencement of hearings, hearing officer's decision, the final appeal process, and reconsideration of access.

Please visit our Customer SharePoint Site to stay abreast of all Personnel Security information!

Points of Contact:

Office of Headquarters Personnel Security (EHSS-43) (301) 903-4175 or email Personnel Security.

Section 304
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 EHSS-43.

HQ Implementation Procedures:

Reportable Information: Per DOE Order 472.2A, Personnel Security, Attachment 4 – Reporting Requirement

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 in possession of a DOE security clearance.

Such matters, listed below, must be reported verbally or in writing directly to EHSS-43 immediately upon the individual becoming aware of the situation or incident. If the information is verbally reported, a written confirmation must be provided by the individual to EHSS-43 within 3 working days after the situation or incident.

> *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 their access restricted or withdrawn.*

Reportable information includes, but is not limited to:

1. Unofficial Foreign Travel:

    a. Covered individuals must report all unofficial (i.e., personal) foreign travel plans to the appropriate CPSO before the start of travel. If reporting does not occur before planned travel, the covered individuals must report travel to the CPSO as soon as possible after the travel occurs, and no longer than 5 working days. Reports of planned unofficial foreign travel must include, at a minimum, the following information as available and applicable:

        (1) Full itinerary;
        (2) Dates of travel;
        (3) Mode(s) of transport, including identity of carriers;
        (4) Passport number;

(5) Emergency point of contact;
(6) Names and association of foreign national traveling companions, and
(7) Planned interactions with foreign governments, companies or citizens during travel and reasons for contact (routine travel/tourism-related contacts excepted).

b. When the need for emergency unofficial foreign travel precludes full compliance with the above requirements, the covered individual must, at a minimum, verbally notify their supervisor/management chain concerning the nature of the emergency. Full reporting must be accomplished within 5 working days of return.

c. Covered individuals traveling to a sensitive country must receive an appropriate defensive counterintelligence briefing from the local Counterintelligence Office prior to travel. Covered individuals must also receive post-travel debriefings from IN for all unofficial foreign travel if applicable in accordance with paragraph 1.e., below. Deviations from sensitive country travel itineraries must be reported immediately upon return, but in no event greater than 5 working days upon returning to work.

d. Unplanned border crossings to Canada or Mexico must be reported within 5 working days of the occurrence.

e. Upon return from any unofficial foreign travel, the covered individual must report the following information to their CPSO/Counterintelligence:

(1) Unplanned interactions with foreign governments, companies or citizens, and the reasons for the interaction(s) (not including routine travel/tourism-related contacts).
(2) Unusual or suspicious occurrences during travel, including those of a possible security or counterintelligence significance; and
(3) Any foreign legal or customs incidents.

5. Contacts with Foreign Intelligence: Covered individuals must report all unofficial contacts with any known or suspected foreign intelligence entity to Counterintelligence. Reporting must occur immediately upon the covered individual's becoming aware of the contact, and in no event later than 3 working days [upon returning to work]. Counterintelligence will ensure the information is passed to the appropriate CPSO. If this occurs while outside the U.S., reporting must occur immediately upon return to the covered individual's normal duty station, and in no event later than 3 working days upon returning to work.

6. Elicitation: Attempted elicitation (to include by media sources), exploitation, blackmail, coercion, or enticement to obtain classified matter or other information or material specifically prohibited by law from disclosure, regardless of means, must be reported by covered individuals to counterintelligence immediately, and in no event later than 3 working days upon returning to work. Reporting is required regardless of whether the attempt results in a disclosure. Counterintelligence will ensure the information is passed to the appropriate CPSO. If this occurs while outside the U.S., reporting must occur

immediately upon return to the cover individual's normal duty station, and in no event later than 3 working days.

7. Continuing Association with Foreign Nationals: Covered individuals must report to the appropriate CPSO any unofficial continuing association with known foreign nationals that involves bonds of affection, personal obligation, or intimate contact (Note: cohabitation with any foreign national for more than 30 days, regardless of the nature of the relationship, must be reported under this requirement).

   This requirement is based on the nature of the relationship, regardless of how or where the contact was made or how the relationship is maintained (i.e., in person, telephonic, mail, internet, etc.).

   a. After initial reporting, updates must be provided when there is a significant change (e.g., enduring relationship that involves substantial sharing of personal information and/or the formation of emotional bonds; transitioning from cyber, postal, telephonic, etc. contact to face-to-face contact, establishing an intimate and/or monogamous relationship, and marriage proposals) in the nature of the contact.

   b. "Continuing" contact is any contact which recurs, or which might reasonably be expected to recur, but does not include casual contact not based upon affection, obligation, or intimacy.

   c. Covered individuals must report under this section immediately after it becomes apparent that contact is continuing, and in no event later than 3 working days.

8. Foreign Activities: The following foreign activities must be reported by covered individuals to the appropriate CPSO immediately, but in no event later than 3 working days:

   a. Direct involvement in a foreign business;

   b. Opening of a foreign bank account;

   c. Purchase of a foreign property (whether located in a foreign country or not);

   d. Application for or receipt of foreign citizenship;

   e. Application for, possession, or use of a foreign passport or identity card for travel;

   f. Voting in a foreign election;

   g. Adoption of a non-U.S. citizen child.

9. Other Reportable Information: The following occurrences/actions must be reported to the appropriate EHSS-43 immediately, but in no event later than 3 working days after occurrence. This report must be in writing.

   a. Arrests, criminal charges (including charges that are dismissed), citations, tickets, summons, or detentions by Federal, state, or other law enforcement authorities for violations of law within or outside the U.S. Traffic violations for which a fine of less than $300 was imposed need not be reported unless the violation was alcohol or drug related.

   b. Financial anomalies including, but not limited to:

      (1) Bankruptcy;
      (2) Wage garnishment;
      (3) Delinquency more than 120 days on any debt;
      (4) Unusual infusions of assets more than $10,000 or greater, such as inheritance, winnings, or similar financial gain.

   c. Action to legally change one's name;

   d. Change in citizenship;

   e. The use of any Federally illegal drug (to include the abuse or misuse of any legal drug), and any drug or alcohol related treatment.

   f. An immediate family member assuming residence in a sensitive country, and

   g. Hospitalization for mental health reasons.

10. Marriage/Cohabitant(s): All cleared individuals (including individuals with a suspended clearance) and applicants must provide a completed DOE F 5631.34, *Data Report on Spouse/Cohabitant* directly to the CPSO within 45 calendar days of marriage or cohabitation. Note: A cohabitant is a person with whom the covered individual resides and shares bonds of affection, obligation, or other commitment, as opposed to a person with whom the covered individual resides for reasons of convenience (e.g., a roommate). A cohabitant does not include individuals such as a husband, wife, and children.

11. Reportable Actions by Others: Covered individuals must alert the appropriate CPSO to the following reportable activities/actions on the part of other covered individuals:

   a. An unwillingness to comply with rules and/or regulations, or to cooperate with security requirements;

   b. Unexplained affluence or excessive indebtedness;

   c. Alcohol abuse;

d. Illegal use or misuse of drugs or drug activity;

e. Apparent or suspected mental health issues where there is reason to believe it may impact the covered individual's ability to protect classified matter or other materials specifically prohibited by law from disclosure;

f. Criminal conduct;

g. Any activity that raises doubts as to whether another covered individual's continued national security eligibility for access to classified matter or to hold a national security position is clearly consistent with the interests of national security; or

h. Misuse of U.S. government property or information systems.

Administrative Withdrawal of Security Clearance:

Security clearances must be administratively withdrawn when there is termination of employment, a change of official duties, or any other change in circumstance such that the individual no longer requires access to classified information or SNM.

Within 3 working days of one of the above conditions, the sponsoring office must provide EHSS-43 a completed DOE F 5631.29, *Security Termination*, or written notice. In cases in which it is not possible to obtain the individual's signature, an unsigned DOE F 5631.29 may be accepted, along with a concise written explanation of the circumstances surrounding the administrative withdrawal and the reasons why a signature could not be obtained.

The purpose of DOE F 5631.29 is to ensure the individual is aware of the continuing responsibility to protect classified information and SNM after withdrawal of a security clearance.

In all cases, administrative withdrawals are non-prejudicial, and do not entitle the individual to any of the Administrative Review procedures of 10 CFR 710.

Please visit our Customer SharePoint Site to stay abreast of all Personnel Security information!

Points of Contact:

Office of Headquarters Personnel Security (EHSS-43) (301) 903-4175 or email Personnel Security.

Forms/Samples/Graphics

DOE F 5631.34, *Data Report on Spouse/Cohabitant*

Section 305
Questionnaires for National Security, Non-Sensitive, or Public Trust Positions)

This section supplements the procedures described in Section 301, HSPD-12 Credential for PIV, and Section 302, Acquiring New Security Clearances, and the process for data collection for background investigations.

DOE uses the Standard Form-86 (SF-86), Standard Form-85 (SF-85), and Standard Form-85P (SF-85P) questionnaire 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 system which collects this information on each Standard Form on behalf of all Federal agencies, including DOE. The questionnaire must be completed by every DOE Federal or contractor employee applying for an HSPD-12 security badge and/or a security clearance.

Initiating the SF-85, SF-85P, or SF-86:

An applicant needing to complete the SF-85, SF-85P, or SF-86 form will have a request initiated which allows them to access the system where they will be required to complete their applicable Standard Form. The individual will receive a notification email containing important instructions about registration, the link to the website, and a due date for when the form must be completed and transmitted to EHSS-43 or EHSS-74 for review. Applicants will be given no more than 7 days to complete the form.

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

After the Standard Form is completed, the applicant certifies their answers are correct, prints a copy of the form for their records, digitally signs the signature pages, and releases the form to the appropriate Personnel Security Office (EHSS-43 or EHSS-74) for review. The form is reviewed for completeness and accuracy. If corrections are needed, the appropriate Personnel Security Office will return the form directly to the applicant and send an email with a detailed explanation of the corrections/clarifications needed. EHSS-43 and EHSS-74 gives the applicant 3 days to make the corrections, certify the form, digitally sign the signature pages, and release the form for review. The form is reviewed for completeness and accuracy again. If acceptable, the form is released to DCSA to start the background investigation. The designated Personnel Security Office has 14 days from the time the applicant certifies the form to submit to DCSA.

EHSS-43 or EHSS-74 will return forms for corrections or clarifications two times. After the second time, the HSO or HC Specialist will be contacted for assistance.

Notification of Completion:

There is no automatic notification that alerts EHSS-43 or EHSS-74 when a Standard Form is waiting for review. EHSS-43 requires the applicant notify the office by email when the applicant has completed the form and released it for review. If EHSS-43 is not notified the form is ready for review EHSS-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 EHSS-43 that these actions are complete.

Please visit our Customer SharePoint Site to stay abreast of all Personnel Security information!

Points of Contact:

Office of Headquarters Personnel Security (EHSS-43) (301) 903-4175, or email Personnel Security.

Helpful Website:

Refer to Defense Counterintelligence and Security Agency for:

Guides and Resources for filling out your Standard Form:

- e-QIP Applicant Brochure
- First-time User Login Instructions (PDF file) [865.29 KB]
- Click-to-Sign Instructions for Applicants (PDF file) [768.43 KB]
- Guide for the Standard Form (SF) 86 (PDF file) [3.78 MB] (Updated to align with SF 86 version 07/2017)

Section 306
Security Clearance Reinvestigations and Verifications

At the beginning of each month, EHSS-43 will provide the HSO a list of active clearance holders in their respective organization who are due for reinvestigation for that particular month. The list is transmitted via memorandum and contains processing instructions. The majority of the packages are scanned and transmitted via encrypted e-mail.

EHSS-43 also provides the HSO a list of all clearance holders currently sponsored by their element. The list is accompanied by a memorandum from EHSS-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: EHSS-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.*

Reinvestigations:

Once HSO's receive the list of clearance holders due for reinvestigation the following actions are needed:

- Confirm all personnel on the list still require a security clearance.
- Confirm the clearance level for each person on the list is consistent with the person's actual access to classified information.
- Submit the required documents for reinvestigation

When the individual needs to retain their current security clearance, the HSO must submit a reinvestigation eCAR containing the following document:

Federal Employee:

- PD and OF-8
- PDR
- Template 5633.33, *Personnel Security Clearance Action Request*
- 5631.18, *Security Acknowledgement*

Contract Employee:

- PDR
- 5631.18, *Security Acknowledgement*
- Template 5633.33, *Personnel Security Clearance Action Request*

The eCAR will be reviewed by EHSS-43 and if acceptable, the HSO will be notified to initiate an e-QIP request for the employee. See Chapter 3, Section 305 Electronic Questionnaires for Investigations Processing (e-QIP) for information on what actions the employee must take to complete e-QIP processing.

All responses, requisite forms, and/or eCAR requests should be submitted within 30 days from the date the Program Office receives their reinvestigations due list and accompanying memo. Extension deadlines may be granted on a case-by-case basis; however, Program Offices and HSOs are strongly encouraged to make every effort to complete these actions within the 30-day timeframe.

When the individual fails to submit the documentation required for their 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 their security clearance.

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

1. Individual has separated from DOE – Have the individual complete DOE F 5631.29, *Security Termination*. When the employee is unavailable to sign the DOE F 5631.29, the HSO must complete and sign the form. On the second page, the HSO should click the radio button indicating the Subject is not available for debrief and submit it to EHSS-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, *Security Termination*, annotating "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 EHSS-43.

3. Downgrade – (Cleared to Uncleared) 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. These forms should be emailed to Personnel Security.

   A complete PIV request must be submitted if the individual still requires access to an HQ facility. Please refer to Chapter 3, Section 301, HSPD-12 Credential for Personal Identity Verification (PIV) for the required paperwork and do the following:

   - Federal Employees: Email complete paperwork to HQ Federal PIV.
   - Contractor Employees: Email complete paperwork to Personnel Security.

   A downgrade to BAO action cannot be processed until the security clearance has been terminated.

If the downgrade is for a contractor employee, the HSO must also complete and submit a new DOE F 473.2 via email to Personnel Security. EHSS-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 Personnel Security.

Clearance Verification:

EHSS-43 provides a CPCI report identifying all the HQ Federal, contractor employees, consultants and OGA, by HQ element, with active or pending security clearances.

Once HSO's receive the clearance verification list the following actions are needed:

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

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, their security clearance must be terminated. The actions required for each scenario are detailed under Reinvestigations, above.

When the individual has a different office symbol, EHSS-43 must be provided with the new information. A list containing the name of the employee, the DOE file number, and the new office symbol is acceptable. (Note: If the individual transferred to a different position (Federal employees only), EHSS-43 needs a copy of the PD and PDR).

Upon completion of the review, provide the list of corrections to EHSS-43 and confirm all other information is correct. EHSS-43 will update CPCI with the updated information.

Please visit our Customer SharePoint Site to stay abreast of all Personnel Security information!

Points of Contact:

Office of Headquarters Personnel Security (EHSS-43) (301) 903-4175, or email Personnel Security .

Section 307
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.

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 Clearance Holders Attending Classified Meetings at DOE Field Sites:

HQ clearance holders who will be attending a classified meeting at a DOE field site need not pass their security clearance information to that site, unless they are visiting a DOE site supervised by the NNSA and requires the passing of Sigma accesses (see process for passing Sigma accesses below).

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

HQ clearance holders attending a classified meeting at an OGA, or the U.S. Congress must pass their security clearances 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, their 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, email address, and fax number.
- Select the level and category of information to be accessed which is located on the form (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 or 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 (Adobe digital with certs or wet 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 EHSS-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 EHSS-43. The DOE F 5631.20 should be submitted 15 working days prior to the visit. EHSS-43 cannot guarantee the visit request will be completely processed if not received at least 15 working 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:

EHSS-43 does not pass SCI clearances. To have SCI passed to the site contact HQ SSO in the Office of Counterintelligence (IN-20).

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 Sigma Processing. The DOE F 5631.20 is no longer required. Please direct all questions regarding Sigma accesses to Sigma Processing.

Individuals 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.

EHSS-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 EHSS-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 EHSS-43; however, if Sigma 14, 15, or 18 access is requested, the Sigma Access Request Form must be completed and emailed (encrypted) to Sigma Processing.*

Individuals 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.

Please visit our Customer SharePoint Site to stay abreast of all Personnel Security information!

Points of Contact:

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

Office of Headquarters Personnel Security (EHSS-43) (301) 903-4175, or email Personnel Security.