

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

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

Chapter 3

Personnel Security

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

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

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

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

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

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

Section 301

Acquiring New Security Clearances

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

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

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

Security classification is cast into three levels:

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

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

Employee Accesses Authorized Based on DOE-Issued Security Clearances

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

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

HQ Implementation Procedures

Preliminary Considerations:

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

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

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

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

Who Does What?

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

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

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

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

Requesting a Security Clearance:

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

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

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

3. Obtaining Documentation from the Applicant

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

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

The pre-employment screening must include:

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

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

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

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

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

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

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

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

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

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

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

6. Other Documentation Required

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

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

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

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

Federal Employees:

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

Current resume

Contractor Employee:

DOE F 5631.18, *Security Acknowledgement*

PDR

Drug Test Results

Pre-employment checks/letter

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

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

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

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

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

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

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

Reciprocity:

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

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

Interim Access Authorization (IAA):

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

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

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

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

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

Administrative Review (AR) Processing:

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

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

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

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

Protection of Personnel Security Information:

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

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

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

Applicant Tracking System (ATS):

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

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

Points of Contact

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

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

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

Forms/Samples/Graphics

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

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

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

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

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

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

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

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

Helpful Website

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

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

Date

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

Dear Sir/Madam:

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

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

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

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

Sincerely,

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

Enclosure (drug testing laboratory report)

ATTACHMENT 301-2

PERSEC F 5630.27
05/01/2019

Submit Completed Request
Attach to Email
Reset Form
Save Form

CLEARANCE ACTION TRACKING SYSTEM

Unclassified Account Access Request

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

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

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

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

Role(s): Adjudicator I Adjudicator II Supervisor/Assigner Processor Vault Worker
Select All That Apply Administrative Review Administrator CI Officer eCAR Only Read Only

Adjudication

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

Processing

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

Other

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

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

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

CPSO Approver:	<input type="text"/>	Approval Date:	<input type="text"/>
----------------	----------------------	----------------	----------------------

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

CATS Approving Official:	<input type="text"/>	Approval Date:	<input type="text"/>
--------------------------	----------------------	----------------	----------------------

CATS Administrator:	<input type="text"/>	Completion Date:	<input type="text"/>
---------------------	----------------------	------------------	----------------------

CLEARANCE ACTION TRACKING SYSTEM

User Code of Conduct

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

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

CATS User Acknowledgement

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

Employee Signature:

Date:

ATTACHMENT 301-3

TEMPLATE 5633.33 (June 2020)		PERSONNEL SECURITY CLEARANCE ACTION REQUEST			
SUBJECT INFORMATION					
Subject Type: Please select		Routing Symbol:	DOB:	SSN:	
Name (Last Suffix, First Middle):			Job Title:		
Place of Birth (City, State/Country):		Foreign National <input type="checkbox"/> Yes <input type="checkbox"/> No	Multiple Citizenship <input type="checkbox"/> Yes <input type="checkbox"/> No	Citizenship Country:	
Physical Home Address (Street Address, City, State, Country, Zip Code):					
Mailing Address (Street Address, City, State, Country, Zip Code):					
Personal Email Address:			Personal Phone #:		
Work Email Address:			Work Phone #:		
Submitter Name:		Submitter Email Address:		Submitter Phone #:	
SUBJECT WORK LOCATION / BILLING					
Owning CPSO: HEADQUARTERS	Work Site: Please Select		SOI: DN11	SON: Please Select	
EMPLOYER INFORMATION					
Employer (Legal Name):					
Employer Code: NOT NEEDED	Facility Code:	Facility Classification Level: NOT NEEDED		Facility Primary Interest Site: NOT NEEDED	
Contract Number:			Primary Contract Number:		
Contract Clearance Access Level: Please Select		Contract Classification Level: Please Select			
ACTION REQUESTED					
Clearance Action Requested: Please select	Clearance Access Level: Select		Classification Level: Please select	Frequency of Access: Please select	
Special Request		Justification for Clearance Request:			
Special Access Program <input type="checkbox"/> Yes <input type="checkbox"/> No					
Interim PIV <input type="checkbox"/> Yes <input type="checkbox"/> No					
Prior Security Clearance? <input type="checkbox"/> Yes <input type="checkbox"/> No					

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

Instructions for Template
*Required Fields

SUBJECT INFORMATION

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

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

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

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

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

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

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

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

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

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

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

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

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

Personal phone number: Provide number, if known

Work email: Provide work email, if known

Work phone: Provide phone number, if known

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

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

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

SUBJECT WORK LOCATION / BILLING

Owning CPSO: Populated with Headquarters

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

SOI: Populated with DN11

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

EMPLOYER INFORMATION

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

Employer Code: Populated with Not Needed

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

Facility Classification Level: Populated with Not Needed

Facility Primary Interest Site: Populated with Not Needed

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

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

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

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

ACTION REQUESTED

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

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

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

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

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

CERTIFICATION***Certifications:**

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

Documents:

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

ATTACHMENT 301-4

Applicant Tracking System Quick Reference Guide

What is ATS

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

Getting Started

There are three basic steps in using ATS:

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

Step 1: Opening Internet Explorer

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

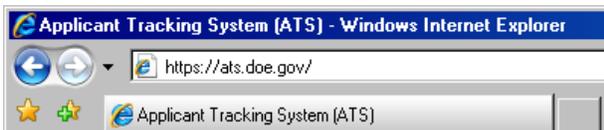


Explorer

Step 2: Creating an ATS Account

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

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



The ATS Log In page opens.



Click on the **New User** button. The logon page changes to the new user registration page.

Fill in the following data on the page:

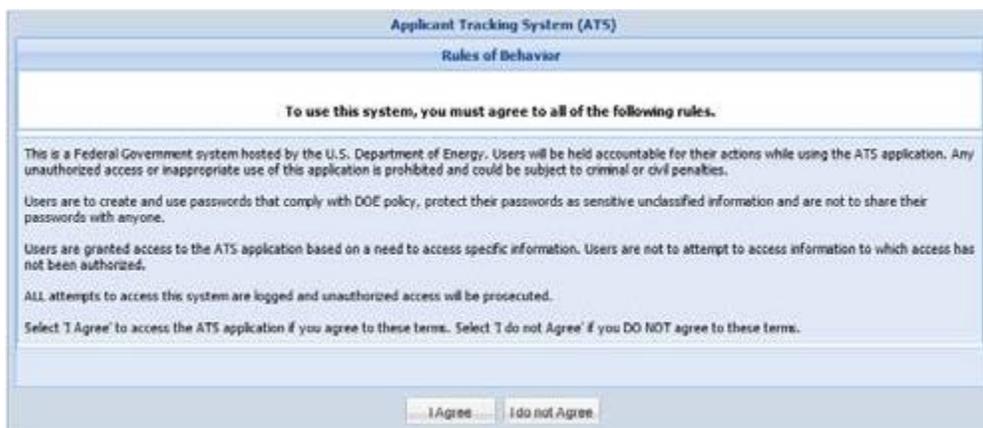
- Your first and last name
- Last 4 digits of your SSN
- Your Email address
- Your user ID – there are no restrictions; you can enter whatever you want
- Your password – the restrictions are listed at the bottom of the page

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

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

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

The **Rules of Behavior** window opens.



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

Step 3: Viewing Investigation Dates



Step 3: Viewing Investigation Dates

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

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

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

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

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

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

Additional Information

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

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

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

Section 302

Other Security Clearance Actions

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

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

HQ Implementation Procedures

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

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

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

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

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

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

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

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

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

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

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

Points of Contact

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

Forms/Samples/Graphics

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

DOE Form 5631.29, *Security Termination Statement* (The following link may only be accessible by use of the Internet Explorer browser)
<http://energy.gov/cio/downloads/security-termination-statement> for a copy of this form

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

This page intentionally left blank.

Section 303

Reporting Requirements for Personnel Holding Security Clearances

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

HQ Implementation Procedures

Reportable Information:

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

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

Other reportable information includes, but is not limited to:

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

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

Reporting 90 Day Absences:

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

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

Points of Contact

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

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

Forms/Samples/Graphics

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

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

ATTACHMENT 303-1

Sample 90-Day Absence Report

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

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

SUBJECT: Reporting 90-Day Absence

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

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

Section 304

Electronic Questionnaires for Investigations Processing

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

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

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

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

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

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

HQ Implementation Procedures

What Must Be Done:

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

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

e-QIP Registration:

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

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

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

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

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

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

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

Notification of Completion:

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

Continuation of HSPD-12 Badge or Security Clearance Processing:

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

Points of Contact

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

Helpful Website

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

This page intentionally left blank.

Section 305

Security Clearance Reinvestigations and Verifications

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

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

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

HQ Implementation Procedures

Reinvestigations:

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

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

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

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

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

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

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

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

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

Clearance Verification:

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

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

These actions include:

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

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

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

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

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

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

Points of Contact

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

Forms/Samples/Graphics

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

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

DOE Form 5631.29, *Security Termination Statement* (The following link may only be accessible by use of the Internet Explorer browser)
<http://energy.gov/cio/downloads/security-termination-statement> for a copy of this form

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

Section 306

Passing Clearances for Classified Meetings or Visits

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

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

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

HQ Implementation Procedures

HQ Clearance Holders Attending Classified Meetings at DOE Field Sites:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Visitors Attending Classified Meetings at HQ Facilities:

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

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

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

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

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

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

Visitors Attending SCI Meetings at HQ Facilities:

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

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

Points of Contact

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

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

Forms/Samples/Graphics

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

This page intentionally left blank.

Section 307

HSPD-12 Credential for Personal Identity Verification (PIV)

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

Who Needs a HSPD-12 Credential?

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

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

Requesting a HSPD-12 Credential:

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

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

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

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

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

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

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

HSPD-12 Process:

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

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

Points of Contact

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

Forms/Samples/Graphics

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

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

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

Sample DOE F 206.4 (see Attachment 307-1)

Sample DOE F 473.2 (see Attachment 307-2)

Sample OF-306 (see Attachment 307-3)

Helpful Website

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

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

ATTACHMENT 307-1

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

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

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

Information Sheet for Sponsorship of HSPD-12 Credential

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

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

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

Reviewed by _____ Date: 01/01/20

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

ATTACHMENT 307-2

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

U.S. DEPARTMENT OF ENERGY
SECURITY BADGE REQUEST

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

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

PRIVACY ACT STATEMENT ON REVERSE

DOE F 473.2 INSTRUCTIONS

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

ATTACHMENT 307-3

Declaration for Federal Employment*

Form Approved:
OMB No. 3206-0182

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

GENERAL INFORMATION

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

◆ Raylan Harlan Givens

2. SOCIAL SECURITY NUMBER

◆ 123-45-6789

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

◆ Germantown, MD

3b. ARE YOU A U.S. CITIZEN?

 YES NO (If "NO", provide country of citizenship) ◆

4. DATE OF BIRTH (MM / DD / YYYY)

◆ 01/01/1990

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

◆ Ray Givens

6. PHONE NUMBERS (Include area codes)

Day ◆ 301-555-5555

Night ◆ 301-555-5555

Selective Service Registration

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

- 7a. Are you a male born after December 31, 1959? YES NO (If "NO", proceed to 8.)
- 7b. Have you registered with the Selective Service System? YES (If "YES", proceed to 8.) NO (If "NO", proceed to 7c.)
- 7c. If "NO," describe your reason(s) in item 16.

Military Service

8. Have you ever served in the United States military? YES (If "YES", provide information below) NO

If you answered "YES," list the branch, dates, and type of discharge for all active duty.
If your only active duty was training in the Reserves or National Guard, answer "NO."

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

Background Information

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

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

9. During the last 7 years, have you been convicted, been imprisoned, been on probation, or been on parole? (Includes felonies, firearms or explosives violations, misdemeanors, and all other offenses.) If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved. YES NO
10. Have you been convicted by a military court-martial in the past 7 years? (If no military service, answer "NO.") If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the military authority or court involved. YES NO
11. Are you currently under charges for any violation of law? If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved. YES NO
12. During the last 5 years, have you been fired from any job for any reason, did you quit after being told that you would be fired, did you leave any job by mutual agreement because of specific problems, or were you debarred from Federal employment by the Office of Personnel Management or any other Federal agency? If "YES," use item 16 to provide the date, an explanation of the problem, reason for leaving, and the employer's name and address. YES NO
13. Are you delinquent on any Federal debt? (Includes delinquencies arising from Federal taxes, loans, overpayment of benefits, and other debts to the U.S. Government, plus defaults of Federally guaranteed or insured loans such as student and home mortgage loans.) If "YES," use item 16 to provide the type, length, and amount of the delinquency or default, and steps that you are taking to correct the error or repay the debt. YES NO

U.S. Office of Personnel Management
5 U.S.C. 1302, 3301, 3304, 3328 & 8716

Optional Form 306
Revised October 2011
Previous editions obsolete and unusable

