U.S. Department of Energy
Washington, DC

ORDER

DOE O 472.2A

Approved: 6-10-2022
Chg 1 (LtdChg): 10-28-2024

SUBJECT: PERSONNEL SECURITY

---

1. PURPOSE. To establish requirements for the Department of Energy (DOE) to operate a successful, efficient, and cost-effective personnel security program to provide accurate, timely and equitable determinations of an individual's eligibility for access to classified information and/or Special Nuclear Material (SNM).

   a. This DOE Order sets forth requirements for personnel security program management and work practices that support accomplishment of DOE missions in a secure environment by individuals in whom both the Department and the American people place their complete trust and confidence.

   b. In all matters related to its internal personnel security activities, DOE retains absolute authority. The procedures in this Order, the requirements of Title 10, Code of Federal Regulations, part 710 (10 CFR 710), and the terms of Executive Order 12968, including investigative and adjudicative standards issued pursuant to its authority, are not subject to collective bargaining.

2. CANCELS/SUPERSEDES. This Order cancels or supersedes the following:

   a. DOE O 472.2 Chg 2 (PgChg), *Personnel Security*, dated 7-9-14

   b. Secretarial Action Memorandum, *Implementation of Security Executive Agent Directive 3, Reporting Requirements for Personnel With Access to Classified Information or Who Hold a Sensitive Position*, dated 9-10-17

   c. Secretarial Memorandum, *Implementation of Security Executive Agent Directive 8, Temporary Eligibility*, dated 6-14-21

   d. Deputy Secretarial Memorandum, *Approval of Reform Recommendation on Implementing SEAD 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position*, dated 1-25-2019

   e. Deputy Secretarial Memorandum, *Implementation of Security Executive Agent Directive 7, Reciprocity of Background Investigations and National Security Adjudications*, dated 6-10-19

   f. Deputy Secretarial Memorandum, *Review of Processes and Standards for Security Clearance Application Processing*, dated 9-12-2018

   g. Deputy Secretarial Memorandum, *Revision of DOE Policy Regarding Application of the Bond Amendment*, dated 4-23-21

h. Associate Under Secretary for Environment, Health, Safety and Security Memorandum, *Complex-wide Cessation of Personnel Security Interviews*, dated 10-2-2018

i. Associate Under Secretary for Environment, Health, Safety and Security Memorandum, *Counterintelligence Risk Assessment Procedures*, dated 11-20-2018

j. Associate Under Secretary for Environment, Health, Safety and Security Memorandum, *Guidance on Processing Security Clearance Applications for Federal and Contractor Personnel*, dated 10-24-2018

k. Associate Under Secretary for Environment, Health, Safety and Security Memorandum*, Security Executive Agent Directive 3, Unofficial Foreign Travel*, dated 6-27-2019

Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive. Contractor Requirements Documents (CRDs) that have been incorporated into a contract remain in effect throughout the term of the contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

a. Departmental Applicability. This Order applies to all Departmental elements, offices and sites engaged at any level in the processing of national security determination and security clearances, as set forth in this Order.

(1) The Administrator of the National Nuclear Security Administration (NNSA) must assure that NNSA employees comply with their responsibilities under this directive. Nothing in this directive will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.

(2) The Administrator of the Bonneville Power Administration (BPA) will ensure that BPA employees and contractors comply with their respective responsibilities under this Order and its CRD, consistent with BPA's procurement, self-financing and statutory authorities.

b. DOE Contractors. Except for the equivalency in paragraph 3.c., the CRD (Attachment 1) sets forth requirements of this Order that apply to contracts that include the CRD. All site/facility management contracts involving classified information or SNM must include this CRD and DOE Acquisition Regulation (DEAR) clause 952.204-2, *Security Requirements*.

c. Equivalencies/Exemptions for DOE O 472.2A.

(1) Exemption or Equivalency Requests. Requests for an Exemption or Equivalency to this Order must be in accordance with DOE O 251.1, *Departmental Directives Program*, current version, and must be sent in memorandum form to the Director, Office of Security for advice.

(a) The memorandum must briefly justify the reason(s) for the exemption or equivalency.

(b) The memorandum must reference the offices, or localities, and requirements for which the exemption or equivalency is sought.

(2) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at Title 50 United States Code (U.S.C.) sections 2406 and 2511, and to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program (NNPP), the Deputy Administrator for Naval Reactors will implement and oversee requirements and practices contained in this Order for activities related to personnel security under the NNPP.

4. REQUIREMENTS.

a. General.

(1) A security clearance is an administrative determination that an individual is eligible for access to classified information and/or access to particular types or categories of classified information or SNM.

(2) Unless otherwise specifically noted, the provisions of this Order apply only to DOE (to include NNSA) Federal, contractor and subcontractor employees, applicants for employment, political appointees, Other Government Agency (OGA) personnel, and consultants.

(3) No individual will be provided access to classified information or SNM unless that individual possesses a need-to-know, has been granted the appropriate security clearance and has signed a SF-312, *Classified Nondisclosure Agreement*, or other nondisclosure agreement approved by the Director of National Intelligence. Access to, knowledge of, or possession of classified information or SNM will not be afforded to any individual solely by virtue of the individual's office, position, or security clearance. Adjudicative personnel are prohibited from making security clearance determinations until they have completed the National Training Center's (NTC) Adjudication Fundamentals Course or other nationally approved training and/or have received adequate initial on-the-job training as determined by the Cognizant Personnel Security Office (CPSO). See Attachment 6 for additional information.

(4) With the few exceptions noted in this Order and provided for in Executive Order (EO) 12968, section 3.3; EO 13526, *Classified National Security Information*, section 4.4; and Security Executive Agent Directive (SEAD) 8, *Temporary Eligibility*, or successor directive, individuals must not be afforded access to classified information or SNM until they have been granted a security clearance.

(5) Security clearances must not be processed merely to achieve the following:

(a) Avoid the use of access controls or physical barriers to distinguish perimeters among security areas or between security and open areas or to alleviate responsibilities for escorting individuals without security clearances within a controlled area. Federal Site Managers may require such individuals under their cognizance to have a security clearance if, in their judgment, operational necessities or cost considerations require it and inadvertent access to classified information by these individuals cannot otherwise be reasonably prevented.

(b) Alleviate individual or management responsibilities for properly protecting classified information or SNM or for controlling dissemination of classified information or SNM on a need-to-know basis.

(c) Establish a pool of employees with pre-existing security clearances.

(d) Accommodate an individual's personal convenience, expedience, gain, or advantage.

(e) Anticipate unspecified classified work.

(f) Determine suitability for Federal employment or fitness for contractor employment. Background investigations requested for national security eligibility will be shared with Human Capital (HC), or the appropriate suitability adjudications office for suitability or employment purposes.

(6) Only individuals who are United States (U.S). citizens who are at least 18 years of age are processed for or granted a security clearance.

(7) Except for circumstances described elsewhere in this Order, an individual's security clearance is based on the review of investigative reports provided to DOE by an authorized investigative service provider (ISP).

(8) All individuals processed for security clearances must be treated equally, in accordance with the requirements set forth in this Order, to preclude the appearance, inference or practice of partiality or favoritism. Anyone who uses personnel security activities to coerce, restrain, threaten, intimidate, or retaliate against individuals for exercising their rights under the Constitution or under any statute, regulation or DOE directive are subject to appropriate disciplinary action.

(9) Contractor applicants and employees must be processed for security clearances in the same manner as Federal applicants and employees except for such additional requirements or considerations which are imposed by DOE O 470.4, *Safeguards and Security Program*, current version, and by 32 CFR 117, *National Industrial Security Program Operating Manual* (NISPOM). For additional information, see Attachment 1.

b. Continuous Vetting. The CPSOs must implement Trusted Workforce requirements consistent with the guidance in EO 13467, as amended, and the Directors of National Intelligence (DNI) and the Office of Personnel Management (OPM) Memorandum Transforming Federal Personnel Vetting: Continuous Vetting and Other Measures to Expedite Reform and Transition to Trusted Workforce 2.0, dated 01-15-2021, and the Federal Personnel Vetting Core Doctrine. The DNI serves as the Security Executive Agent and the Director of OPM serves as the Suitability and Credentialing Executive Agent. Requirements for suitability determinations can be found in DOE O 3731.1, Suitability, Position Sensitivity, Designations, and Related Personnel Matters, current version. Requirements for credentialing determinations can be found in Appendix G.

c. Security Clearance and Access Authorization Types. Security clearances and access authorizations denote an individual's eligibility for access to a particular type of classified information or material, such as National Security Information (NSI), Restricted Data (RD), Formerly Restricted Data (FRD), Transclassified Foreign Nuclear Information (TFNI), or SNM. This section describes those security clearances and access authorizations that are processed by DOE. Other access determinations made by DOE are described in Attachment 2.

(1) Security Clearances.

(a) Top Secret. A Top Secret (TS) security clearance is required for access to NSI, as defined by Executive Order 13526, classified at the Top Secret level, FRD and TFNI (as defined by the Atomic Energy Act of 1954, as amended [AEA]) at the Top Secret level. A Top Secret security clearance also permits access to NSI, FRD, and TFNI classified at the Secret and Confidential levels.

(b) Secret. A Secret (S) security clearance is required for access to NSI and FRD classified at the Secret level. A Secret security clearance also permits access to NSI, FRD, and TFNI classified at the Confidential level.

(c) Confidential. A Confidential (C) security clearance is required for access to NSI, FRD, and TFNI classified at the Confidential level.

(d) The granting of a TS or S security clearance does not give the recipient approval for a Q or L access authorization as defined in 4.c.(2) below. An appropriate need-to-know determination for the recipient is also required.

(2) Access Authorizations.

(a) Q. A Q access authorization is required for and allows access to:

1 RD (as defined by the AEA), FRD and TFNI.

2 SNM, as defined by the AEA, designated as Category I and other categories with credible roll-up to Category I.

3 Information and material described below for L access authorizations.

4 Information listed under TS, S, and C security clearance, in 4.c.(1) above.

(b) L. An L access authorization is required for and allows access to:

1 RD classified at the C level and/or SNM designated as Categories II and III, unless special circumstances determined by a site vulnerability assessment and documented in associated site security plans mandate otherwise.

2 Information listed under S and C security clearance, in 4.c.(1)(b)-(c) above.

(c) Background investigative requirements for all security clearances are mandated by national standards.

d. Central Personnel Clearance Index (CPCI). All applicable DOE personnel security clearance actions (e.g., grants/upgrades/downgrades) will be recorded in CPCI, the DOE system of record. Unless otherwise indicated, all security clearance applicable actions will be automatically imported from the Clearance Action Tracking System (CATS) (see paragraph e. below) into CPCI within 48 hours of receiving the information. Additional information and specific requirements for use of CPCI are set forth in the WebCPCI User's Guide that is available to all individuals authorized access to the system.

e. Clearance Action Tracking System. DOE personnel security staff must use CATS, the case management tracking system of record for recording all security

clearance adjudicative activities. The CATS populates clearance decisions in CPCI upon completion of adjudicative activities.

f. Reciprocity. Reciprocity is the acknowledgement and acceptance of an existing background investigation conducted by an authorized investigative agency; the acceptance of a national security eligibility adjudication determination by an authorized adjudicative agency; and the acceptance of an active national security eligibility determination granted by an executive branch agency. This includes those individuals who are enrolled in a continuous evaluation (CE) program and have a deferred periodic reinvestigation. To apply the guidance in SEAD 7, *Reciprocity of Background Investigation and National Security Adjudications,* or successor directive for individuals requiring a security clearance at DOE who are determined to be currently eligible for access to classified information at another Federal agency, CPSOs must follow the requirements in Appendix E.

g. Reapprovals. Individuals who no longer possess a security clearance must have a security clearance reapproved when a valid justification for access to classified information or SNM has been received by the CPSO and the previously held security clearance was held less than 24 months ago and was removed for administrative, non-prejudicial reasons.

(1) The individual certifies on a Standard Form 86 (SF-86), *Questionnaire for National Security Positions*, and the CPSO verifies there is no change to derogatory information the individual provided at the time of their last background investigation.

(2) The CPSO reviews the completed SF-86 and determines it to be free of any issues of security concern.

(3) The CPSO receives the negative results of a drug test dated no more than 90 days from the date of the request for reapproval.

(4) The CPSO checks the national level personnel security databases (i.e., the Clearance Verification System, etc.) and no issues of a security concern are revealed.

(5) The CPSO is not aware of information about the individual which casts doubt on their eligibility to hold a security clearance.

(6) The required supporting background investigation is less than seven years from the date completed by the ISP, regardless of the level of the currently required security clearance. If the information received is favorable, the requested security clearance must be reapproved after the reinvestigation has been initiated if required. When the background investigation is more than seven years old, all information and items required for processing a security clearance request (see paragraph 4.m. of this Order and Attachment 2, paragraphs 1 and 2) must be obtained by the CPSO.

(7) If at any time during this process the CPSO comes into possession of derogatory information, such information must be resolved favorably by means set forth at section 4.o.(10) before the CPSO may proceed further in considering whether to reapprove access.

(8) Individuals who fall outside the parameters of this section because of the age of their last background investigation or break in service greater than 24 months (e.g., retired DOE Federal or contractor employees) must be processed in accordance with the procedures set forth elsewhere in this Order for issuing security clearances to applicants. However, where the exigencies of a particular case will not permit the timely completion of normal processing procedures and where delay in granting the requested security clearance will result in adverse mission impact, the CPSO may process the individual for temporary access as outlined in SEAD 8.

h. Other Government Agency Clearances. OGA employees who require access to RD for official government purposes must obtain access through the options outlined in Appendix D. For the purposes of the OGA clearances, the parent agency maintains authority and jurisdiction for the requirements of the baseline clearance (TS/S), to include reinvestigation, CE/continuous vetting adjudication, and reporting requirements.

i. Access by Persons Outside the Executive Branch.

(1) Attorneys and other individuals taking part in legal or administrative review proceedings under the jurisdiction of DOE who will require access to classified information must be processed for a One-Time Access to classified information as required by SEAD 8. Certification is required by the Office of the General Counsel (GC), the appropriate CPSO's Chief Counsel's Office, or the Office of Inspector General (OIG)’s Office of Counsel if applicable, that access to specified classified information is needed on the part of the individual to adequately represent his or her client.

(2) Members of the U.S. House of Representatives and the U.S. Senate, members of the U.S. Supreme Court and the Federal Judiciary are eligible for access to all levels and categories of classified information and SNM, without the need for a background investigation, from the date they assume their office until the date they leave their office. Specific instances of access to classified information and SNM will be subject to need-to-know considerations. To facilitate complex-wide access by these individuals, they will be recorded in CPCI and CATS as possessing QB or LB access authorizations. Such CPCI and CATS entries will be created when the first need for actual access arises and will be coordinated between the Office of Headquarters Personnel Security Operations (for the processing and management of QB and LB access authorizations throughout the complex) and the appropriate CPSO. Such access

authorizations will not be included in any database other than CPCI and CATS.

(3) State governors (including the Mayor of the District of Columbia and the Governors of Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, and the Northern Mariana Islands) will be afforded access to classified information and SNM in the same manner as those listed in (2) above, except that:

(a) They must execute the same nondisclosure agreement applicable to all DOE Federal and contractor employees, and

(b) The Department must not be in possession of information suggesting that such access is not in the best interests of national security. If the Department is in possession of such information, the Director, Office of Departmental Personnel Security (Director) will be consulted prior to the issuance of a QB or LB access authorization.

(4) If required, employees or contractors of the legislative or judicial branches of the Federal Government, or of the governments of any state or territory or leadership officials of any Federally recognized tribal entity, to include staff members and assistants to any of the individuals listed in paragraphs (2) and (3) above, must be processed for the appropriate access authorization in accordance with the procedures set forth in this Order.

j. Access by Former Presidential Appointees. In accordance with EO 13526, *Classified National Security Information, Section 4.4, Access by Historical Researchers and Certain Former Government Personnel*, the need-to-know requirement for access to classified information may be waived for individuals who have previously occupied senior policy-making positions to which they were appointed or designated by the President or Vice President, or who have served as President or Vice President. A waiver of the need-to-know requirement may be approved for those positions as defined in the OPM's *Presidential Transition Guide to Federal Human Resources Management Matters,* dated December 2020, or successor guide, that are designated as Presidential Appointees Requiring Senate Confirmation (PAS). Positions designated as PAS positions may retain their access authorization with the DOE, when approval for continued access has been granted by the Under Secretary for Nuclear Security or the Director, Office of Environment, Health, Safety and Security (EHSS), or their successors, in accordance with Appendix F.

k. Limited Access Authorizations for Non-U.S. Citizens.

(1) Only U.S. citizens are eligible for security clearances. Every effort will be made to ensure that only U.S. citizens are employed in duties that require access to classified information. However, compelling reasons may exist to grant limited access to classified information to a non-U.S. citizen. Such

individuals may be granted a Limited Access Authorization (LAA) in those rare circumstances where the non-U.S. citizens possess unique or unusual skills or expertise that are urgently needed to support a specific Departmental mission involving access to classified information and a qualified U.S. citizen eligible for such access is not available. Non-U.S. citizens are not eligible for access to any greater level of classified information or material than the U.S. Government (USG) has determined may be releasable to the country of which the individual is currently a citizen. The Director must consult with GC for this assessment. Such limited access may be approved only if a background investigation of the level required by EO 12968, or successor national standards, for a TS security clearance is conducted.

(2) A request to process a non-U.S. citizen for an LAA must be approved by the Program Secretarial Officer with jurisdiction over the office in which the individual will be employed. Specific requirements, processes and prohibitions related to the issuance of LAAs are set forth in Attachment 3.

l. Temporary Eligibility. When urgent operational or contractual exigencies or exceptional circumstances exist, CPSOs may grant temporary security clearance eligibility in accordance with Attachment 4. All temporary accesses must be recorded in the National-level databases except for One-Time access, which must only be recorded locally in CATS. The CPSO must follow the requirements in Attachment 4 when granting the following temporary accesses:

(1) Temporary access to classified information;

(2) Temporary access to a higher level of classified information; and

(3) One-time access to classified information.

m. Processing Security Clearances.

(1) CPSOs must have written procedures for submission and acceptance of security clearance requests. Requests for security clearances must be justified and submitted to the appropriate CPSO in accordance with established local procedures.

(2) Security clearances will only be processed after the CPSO has received an appropriate written or electronic request. Security clearance cases must include completion of a SF-86, utilizing the appropriate ISP investigations processing system. Submissions must be reviewed by the CPSO to ensure complete reporting of information for required time frames, answers to all applicable questions, and explanations of answers where required. In addition to a completed Electronic Questionnaire for Investigation Processing (e-QIP) submission, other documents must accompany the request for a security clearance. Refer to Attachment 2 for a complete list of required documents.

(3) A Federal employee must approve e-QIP submissions to the ISP.

(4) When processing security clearances, Personally Identifiable Information (PII) must be protected and handled in accordance with DOE O 206.1, *Department of Energy Privacy Program*, current version, and the Privacy Act of 1974, as amended.

n. Cancellation of Investigative Requests. A CPSO must immediately request the ISP discontinue an ongoing investigation if the CPSO receives information indicating the individual no longer requires a security clearance. If a security clearance request is no longer required for access to classified information at one CPSO because the individual is transferring to a location under the cognizance of another CPSO and the individual requires a security clearance at the gaining CPSO, the losing CPSO must not discontinue the investigation. The CPSOs must work together to ensure that the completed investigative report goes to the gaining CPSO.

o. Processing Investigative Results and Issuing Security Clearance Determinations.

(1) When an investigative report is received, the CPSO must review it to ensure that the required national Federal Investigative Standards have been met as appropriate for the level of security clearance being considered. The CPSO must return any investigative reports that do not meet national standards to the investigative agency for corrective action if necessary.

(2) Investigative reports must be processed so that they will be adjudicated in a timely manner as defined by national level mandates.

(3) Only DOE Federal employees who have been designated in writing as having been properly trained may render formal determinations that affect an individual's security clearance status.

(4) A program of quality oversight, training and testing has been established for this purpose. Refer to Attachment 6 for more information on this program. Employees may begin assisting in determinations once their training regimen has begun.

(5) Any secondary actions where governmental resources are expended must be approved by a Federal employee.

(6) Rendering final security clearance determinations is an inherently governmental function. Contractor support staff may not make a final determination on any adjudicative clearance action which results in granting a clearance or continuing of a security clearance. Security clearance downgrades are exempt from this requirement.

(7) All individuals' initial and continued eligibility for security clearances will be adjudicated using SEAD 4 or successor guidelines.

(8) Where the CPSO has no information related to any of the areas of concern identified in SEAD 4 or successor guidelines, either from the report of investigation or from other sources, a favorable determination must be made.

(9) Where the CPSO has information related to any areas of concern identified in SEAD 4 or successor guidelines, either from the report of investigation or from other sources, such information will be regarded as derogatory and create a question as to the individual's security clearance eligibility.

(10) If questions as to the individual's security clearance eligibility can be favorably resolved in accordance with the processes and considerations set forth in SEAD 4 or successor guidelines, the appropriate security clearance must be granted or continued.

(11) In all cases, each issue of adjudicative significance, to include applicable disqualifying and mitigating factors, will be documented in the Personnel Security File (PSF) or electronic Personnel Security File (ePSF).

(12) When an additional investigation is required to expand, resolve, or corroborate information prior to making a determination, the CPSO may submit a request for such investigation to the appropriate investigative agency, or elect to pursue other options including, but not limited to the following:

(a) Send a letter of interrogatory (LOI) to the individual. LOIs must include a deadline for the individual to provide the response and must inform the individual that requested documentation must be provided as appropriate.

(b) Conduct a personnel security consultation when there is a valid justification for such action. Approval to conduct a personnel security consultation requires CPSO management concurrence and the cognizant Chief Security Officer approval. Only individuals appropriately trained in DOE personnel security consultation techniques and cognizant of all the questions or items of information to be explored are authorized to conduct consultations. DOE F 5631.5, *The Conduct of Personnel Security Interviews under DOE Security Regulation*, or successor form, and DOE F 5631.7, *Privacy Act Statement for Personnel Security Interviews and Related Release Forms*, or successor form, must be properly executed for all personnel security consultations. Personnel security consultations must be recorded, summarized on a CES and

retained in the PSF/ePSF. Transcripts may be prepared as necessary and if so, must be retained in the PSF/ePSF. The information from a personnel security consultation may be used to support additional adjudication actions (mental health evaluation, due process under administrative review, etc.).

(c) Authorize a DOE-sponsored mental health evaluation (requires the individual to complete DOE F 472.2, *Consent to Undergo a Mental Evaluation to be Conducted by a Psychiatrist or Licensed Clinical Psychologist*, or any successor form).

(d) Request the assistance of other CPSOs in different geographical locations to conduct a personnel security consultation or to obtain additional information. Assisting CPSOs must manage such requests in as timely a manner as possible.

(e) Consult with the cognizant counterintelligence office where questions as to the individual's loyalty, allegiance, foreign connections, or unexplained affluence arise. Dual citizen applicants should be identified as such, although being a dual citizen alone is not a counterintelligence indicator. Utilize coordinating procedures and suitable counterintelligence risk assessment standards/principles for security clearance adjudicative decisions. A thorough counterintelligence assessment, along with other available information, is a tool to assist with determining eligibility for access to classified information, specifically, evaluation of information with a foreign nexus.

(f) Obtain a personal financial statement.

(g) Obtain a credit report.

(13) If, in the opinion of the CPSO, the additional investigative and/or follow-up activities have favorably resolved the pertinent questions as to the individual's security clearance eligibility the security clearance must be granted or continued.

(14) When the additional actions fail to favorably resolve the pertinent questions, the CPSO will initiate the Administrative Review procedures set forth at 10 CFR 710.

p. Continuous Evaluation. CPSOs must follow the guidance in SEAD 6, *Continuous Evaluation* (CE), and its implementing guidance to identify derogatory information in assessing the continued eligibility of a covered individual at any time during the period of eligibility:

(1) Automated records checks must be conducted to identify derogatory information to assist in assessing the continued eligibility of a covered

individual at any time during the period of eligibility. The automated records checks must include checks of commercial databases, USG databases, and other information lawfully available to security officials at any time during the period of eligibility.

(2) DOE's implementation of CE must be conducted only on covered individuals to protect the privacy, civil liberties, and PII of covered individuals and any other individual whose information is inadvertently collected as part of the CE process.

(3) Absent a national security concern, criminal reporting requirement, or other legal requirement, information pertaining to individuals other than the covered individual will not be retained unless that information is relevant to a security determination of the covered individual.

(4) Information gathered by CE will go to the sponsoring CPSO for analysis of adjudicative relevance and a determination if the information meets thresholds for further investigation and/or adjudication.

(5) CPSOs must utilize authorized ISPs, making reasonably exhaustive efforts to verify that any information collected that is discrepant or potentially disqualifying pertains to the covered individual. CPSOs must use standard personnel security processes to resolve information of a security concern received on a covered individual. Any potentially disqualifying issue(s) will be adjudicated using SEAD 4 or successor guidelines.

(6) CPSOs must not make an unfavorable personnel security action solely on uncorroborated or unverified discrepant information collected pursuant to SEAD 6. When an adjudicative determination is made to deny or suspend national security eligibility, the covered individual must be afforded Administrative Review in accordance with 10 CFR 710.

(7) CPSOs must update applicable national personnel security databases unless authorized by the Security Executive Agent (SecEA)to withhold information from the databases for national security purposes, to inform on a covered individual's national security eligibility for reciprocity purposes.

(8) CPSOs must make sure covered individuals are aware of CE as an element of the personnel security program and their continuing security and counterintelligence reporting obligations. CE must be included in initial and annual security awareness training.

(9) CPSOs must act upon and share relevant information of a security, counterintelligence, or law enforcement concern with appropriate security, counterintelligence, insider threat, or law enforcement officials.

(10) CPSOs must share relevant information that results in an adverse determination of the covered individual's continued national security eligibility with security officials of other agencies that have a direct interest in the covered individual, (i.e., joint duty, detail or otherwise working for the other agency); or the other agency has granted access or additional access to the individual.

(11) CPSOs must not conduct CE on individuals who no longer meet the definition of a covered individual (e.g., termination of employment, or no longer affiliated with DOE).

(12) A targeted investigation may be requested from the ISP at any time if the CPSO learns of information related to any areas of concern set forth in the SEAD 4 or successor guidelines. Such information may be resolved by the CPSO internally through a LOI, a personnel security consultation, a mental health evaluation, or other actions. Alternatively, an investigation for cause through the ISP may be conducted. The precise scope of such an investigation will depend upon the issues involved.

q. Reinvestigations.

(1) CPSOs must continue to collect a newly completed SF-86 every five years until the Department has implemented Trusted Workforce 2.0 and as required by national standards.

(2) Consistent with the guidance in EO 13467, as amended, CPSOs must conduct reinvestigations on an as-needed basis once periodic deferrals of reinvestigations are implemented in the Department as indicated in 4.b. above.

r. Intra-Agency Security Clearance Actions.

(1) A security clearance issued by any CPSO is a Departmental security clearance and will be recognized universally throughout DOE. Individuals in possession of a current DOE security clearance and with a need-to-know are eligible for access to classified information and SNM at the appropriate level throughout DOE. Access to classified information and SNM at all DOE sites must be predicated upon a valid need-to-know and positive confirmation (as indicated in CATS or CPCI) of the appropriate security clearance.

(2) Shared access occurs where one CPSO receives a valid request for a security clearance for an individual already in possession of an equal or higher security clearance issued by another CPSO. In such a case, the new CPSO will annotate CATS to indicate the shared personnel security interest in the individual. Thereafter, should either office come into possession of information of a security concern regarding the individual or need to take adverse action regarding the individual's security clearance,

the information concerning shared access which has been recorded in CATS and CPCI will be used to ensure that all CPSOs with an interest in the individual are notified.

(a) Where shared access occurs, responsibility for maintenance of the PSF/ePSF and for all other related matters will reside with the CPSO that granted the security clearance.

(b) Except as outlined in (c) below, if the security clearance is administratively withdrawn by that CPSO for any reason and continued need for the security clearance persists with one or more CPSOs exercising shared access, these responsibilities will shift to:

1 The CPSO holding the highest level of shared access or

2 The CPSO with the oldest interest, when all remaining CPSOs hold the same level of shared access.

(c) If a security clearance is administratively terminated under 10 CFR 710.6 or 10 CFR 710.32, the CPSO must immediately notify any CPSO with shared access that the clearance was terminated. Any shared access will terminate with the administrative termination.

1 If an appeal is filed less than one year from the initial administrative termination in accordance with 10 CFR 710.32(a), the CPSO initiating the termination is responsible for the clearance adjudication. If there is a valid offer of employment and a clearance is required, the CPSO that initiated the termination is responsible for adjudication. Individuals may not be processed for a clearance at another CPSO unless a minimum of one year has elapsed from the administrative termination.

2 If the Director finds that the individual may be processed for a security clearance after appeal, the CPSO initiating the administrative termination must be notified of the decision. The CPSO must take necessary actions to determine the eligibility of the individual, as outlined elsewhere in this Order. Notification of the appeal will be sent to all CPSOs with shared access.

3 If the CPSO grants the security clearance, the CPSOs which held shared access must be notified. Gaining CPSOs where appropriate, may then process for shared access.

(d) The CPSO responsible for maintaining the PSF/ePSF is also responsible for processing the case for Administrative Review, under 10 CFR 710.

(e) If a CPSO with shared access requires a higher level of security clearance, possession of the PSF/ePSF will be transferred to the office where the higher level is required. The losing CPSO will annotate the shared access as outlined in (2) above. The gaining CPSO must request the appropriate investigation and process an upgrade as outlined elsewhere in this Order.

(3) In the event an individual in possession of a security clearance transfers from the cognizance of one CPSO to another, one of the following procedures must be followed:

(a) If the individual requires access at the same security clearance level in the new position, their PSF/ePSF will be forwarded to the gaining CPSO.

(b) If the individual will no longer require access at the losing CPSO, the losing CPSO must execute a DOE F 5631.29, *Security Termination Statement*.

(c) The gaining CPSO is responsible for completing all new and pending actions after the transfer takes effect.

(4) In all cases, the gaining and losing CPSOs must communicate with each other and work together to ensure that the requirements of this section are met.

s. Administrative Withdrawal of Security Clearances.

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

(2) Within three (3) working days of one of the conditions in paragraph 4.s.(1) above being met, the sponsoring office must provide the CPSO a completed DOE F 5631.29, *Security Termination Statement*, or written notice. In cases in which it is not possible to obtain the individual's signature, an unsigned DOE F 5631.29 may be accepted, along with a concise written explanation of the circumstances surrounding the administrative withdrawal and the reasons why a signature could not be obtained.

(3) Within three (3) working days of receipt of a DOE F 5631.29 or written notice of one of the conditions in paragraph 4.s.(1) above being met, the CPSO must administratively withdraw the individual's security clearance and note the date the clearance was withdrawn in the individual's PSF/ePSF in CATS and CPCI. The CPSO must also notify any other

CPSOs with shared access interests. Possession of the DOE F 5631.29 by the CPSO is not needed to affect an administrative withdrawal action.

(4) In all cases, administrative withdrawals are non-prejudicial, and do not entitle the individual to any of the Administrative Review procedures of 10 CFR 710. When a security clearance is administratively withdrawn and where there is unresolved derogatory information and/or adverse security clearance action (s) are pending against the individual, this fact must be recorded in CATS and CPCI.

t. Suspensions of Security Clearances/Administrative Review. The processes and procedures governing the suspension of active security clearances and the processing of security clearance denial and revocation actions are set forth in 10 CFR 710.

u. Actions by the Secretary. Nothing in this Order will be construed to limit the Secretary's authorities and responsibilities under EO 12968, EO 10865, DOE implementing regulations at 10 CFR 710, or the AEA to grant, continue, deny, or terminate a security clearance in the interest of national security.

v. Personnel Security Files.

(1) PSFs/ePSFs contain information that is identified as PII and controlled under the Privacy Act of 1974, as amended. Within DOE, PII must be identified and protected as Controlled Unclassified Information (CUI) or successor classification marking as required by DOE Order 471.7, *Controlled Unclassified Information,* or successor Order (to include requirements for marking, transmission, storing and destruction).

(2) PSFs/ePSFs may contain information that requires a classification review in accordance with DOE O 475.2, *Identifying Classified Information*, current version. Documents that contain classified information must be protected as required by DOE O 471.6, *Information Security*, current version, to include requirements for marking, transmission, storing, and destruction.

(3) A compromise in the information involving a PSF/ePSF must be reported in accordance with DOE O 206.1, current version. A compromise of information which may be classified must be reported in accordance with DOE O 470.4, *Safeguards and Security Program*, current version.

(4) PSFs/ePSFs must not be released to representatives of DOE contractors (except those contractor employees engaged in support of the DOE personnel security program, or as otherwise permitted in this Order). Detailed information concerning the organization of DOE PSFs/ePSFs and restrictions on their dissemination appear in Appendix B.

(5) PSFs/ePSFs are identified as a system of records under DOE control and are subject to 10 CFR 1008, *Records Maintained on Individuals* (Privacy Act), regarding their release. 10 CFR 1008 establishes the procedures for individuals who request to review or obtain a copy of the contents of their PSFs/ePSFs. Specific instructions for submitting a Privacy Act request are at 10 CFR 1008.6, *Procedures for Privacy Act Requests*. Further information on how to submit a request for access can be obtained by contacting the cognizant Privacy Officer. Under no circumstances will individuals be given access to investigative reports from their PSF/ePSF without prior written approval of the originating agency. Absent such approval, individuals requesting access to these reports must be referred to the originating agency.

(6) PSFs/ePSFs and the associated information in CATS, CPCI or any other DOE database must be retained in accordance with National Archives and Records Administration (NARA)/DOE Records Schedule. Reports of investigation provided by other agencies will be retained as part of the PSF/ePSF in accordance with these guidelines unless the originating agency provides a shorter retention schedule. In that event, the originating agency's schedule will supersede DOE retention policy and such reports must be purged from PSFs/ePSFs, CATS and CPCI accordingly.

(7) PSFs/ePSFs that no longer need to be retained pursuant to this Order must be destroyed in accordance with NARA/DOE Record Schedules. Destruction of files containing classified or CUI must be accomplished in accordance with the current version of DOE O 471.6 or DOE O 471.7, respectively.

w. Reporting Requirements.

(1) All individuals applying for or in possession of a DOE security clearance must truthfully provide all information requested for personnel security purposes. All individuals have a specific obligation to report personnel security-related matters as they occur, whether related to themselves or to other individuals applying for or in possession of a DOE security clearance.

(2) All cleared individuals (including individuals with a suspended clearance) and applicants must follow the guidance in SEAD 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position*, and DOE O 475.1, *Counterintelligence Program,* current version. Cleared individuals incur a special and continuing security obligation to be aware of the risks associated with foreign intelligence operations and/or possible terrorist activities directed against them in the U.S. and abroad. Cleared individuals also have a responsibility to recognize and avoid personal behaviors and activities that may adversely impact their continued national security eligibility.

(3) Cleared individuals and applicants must report to their CPSO any planned or actual involvement in any of the activities in accordance with the timelines indicated in Attachment 5, using the appropriate reporting form prior to participation in such activities or otherwise as soon as possible following the start of their involvement.

(4) Failure to comply with reporting requirements may result in administrative action that includes, but is not limited to, revocation of the individual's security clearance.

(5) Reportable Information (see Attachment 5) must be reported verbally or in writing directly to the CPSO immediately upon the individual becoming aware of the situation or incident. If the information is verbally reported by the individual, a written confirmation must be submitted to the CPSO within three (3) working days after the situation or incident.

(6) Federal management officials must notify the CPSO of conditions affecting the status of an applicant's or employee's security clearance (e.g., death, employment termination (regardless of reasons), change in need for access to classified information or SNM) within three (3) working days, followed by written confirmation within the next ten (10) working days of the occurrence.

(7) CPSOs are responsible for ensuring that security clearance applicants and holders under their cognizance are aware of their reporting responsibilities (e.g., signed DOE Form 5631.18, *Security Acknowledgment*).

(8) Individuals with active security clearances will be briefed initially and annually regarding their personnel security responsibilities as required by DOE O 470.4, *Safeguards and Security Program*, current version.

x. Suitability Determinations for Federal Employees and Referrals to Servicing Personnel Offices.

(1) Derogatory or discrepant information developed as part of the personnel security process may be relevant to an individual's suitability for Federal employment. Therefore, each CPSO must establish procedures for the referral of such information to the servicing personnel offices for the DOE employees under their cognizance. The servicing personnel office must take appropriate action regarding the individual's employment status.

(2) In situations where adverse employment suitability information arises concerning an employee of another Federal agency, the information will be provided to the DOE processing personnel office for referral to the other Federal agency.

y. Pre-Appointment Waivers.

(1) Candidates who have accepted offers of employment to a position designated as sensitive under 5 CFR Part 1400, *Designation of National Security Positions*, may have the pre-appointment investigative requirement waived, allowing the hiring manager and/or program office to bring the candidate onboard prior to the completion of a favorably adjudicated background investigation. This waiver must be requested in writing and include a justification which reflects that the position involves duties that fulfill an immediate need to the Department's national security mission and a delay in filling that position would adversely affect the Department's ability to carry out its national security mission.

(2) The CPSO will review the SF-86 once it has been submitted to the ISP with a request for expedited service, as well as the minimum initial checks in accordance with SEAD 8. If no security concerns are identified, the CPSO will forward the results of these checks, along with the SF-86, to the Office of the Chief Human Capital Officer (HC) for a decision.

(3) Once the CPSO certifies that no security concern exists and the pre-appointment wavier is approved by the HC, hiring managers and/or program offices will implement controls to restrict access to classified information and prevent the individual from performing the duties that make the position sensitive until a favorable full-field background investigation and adjudication is completed and the security clearance is granted.

5. RESPONSIBILITIES.

a. Program Secretarial Officers. Approve requests to process non-U.S. citizens for LAAs and One-Time access in accordance with SEAD 8. These responsibilities may be delegated to the CPSOs.

b. Federal Heads of Departmental Elements.

(1) Ensure that the requirements associated with determining the level of security clearance required and the means to request a security clearance are communicated and implemented by the appropriate offices, individuals, and contracting/procurement officials under their cognizance.

(2) Determine whether and when temporary access is warranted for an individual under their cognizance.

(3) Direct contracting/procurement officials under their cognizance to incorporate this Order's CRD into affected contracts.

c. Federal Site Managers.

(1) Ensure that the requirements of this Order are communicated to and implemented by the appropriate offices, individuals, and contracting/procurement officials under their cognizance.

(2) Determine whether and when to request security clearances for employees under their cognizance who, though they do not require access to classified information or SNM, are situated such that inadvertent exposure to such information or material cannot otherwise be reasonably prevented.

(3) Determine whether and when to approve requests for temporary access to a higher level of classified information or SNM.

(4) Communicate to all cleared DOE personnel under their cognizance their personal responsibilities regarding holding a DOE security clearance. Such individuals are thereafter responsible for adhering to these responsibilities.

d. Contracting and Procurement Officials. Ensure that the CRD (Attachment 1) of this Order is incorporated into affected contracts via the Laws, Regulations, and DOE Directives clause of the contracts. Incorporation must occur as soon as possible, but in no event more than 180 days following the issuance of the CRD.

e. Director, Office of Departmental Personnel Security. Provides necessary oversight, guidance, direction, clarification, and assistance for the requirements of this Order to be implemented correctly and consistently by:

(1) Representing DOE at government-wide meetings to address and resolve personnel security policy issues, investigation scope and timeliness matters, and adjudicative procedures.

(2) Chairing the DOE Personnel Security Quality Panel (PSQP). The primary goal of the PSQP is to enhance policies and procedures pertaining to the Department's Personnel Security Program. The panel is responsible for:

(a) Identifying and discussing challenges and process improvements;

(b) Sharing best practices;

(c) Providing status of pending initiatives;

(d) Coordinating contemplated changes to policies and procedures; and

(e) Coordinating presentations from subject matter experts.

(3) Granting Bond Amendment Waivers.

(4) Managing the Personnel Security Assistance Visit Program (PSAVP). The PSAVP provides the Office of Departmental Personnel Security a flexible means for meeting with the programs one-on-one (annually or as needed) to address concerns, provide recommendations for improvement, and gain a continued understanding of how implementation of national level and Departmental initiatives are affecting operations. The assistance visits are informal collaborative meetings and are not a replacement for or affiliated with:

(a) Formal inspections of the DOE Personnel Security Program conducted by the Office of Enterprise Assessments, or

(b) Audits, inspections, or investigations conducted by the Office of Inspector General.

f. Cognizant Personnel Security Offices. Implement the requirements in accordance with direction provided in this Order and by the Office of Departmental Personnel Security.

g. Office of the General Counsel Offices of Chief Counsel.

(1) Provide notification to the CPSO when access to classified information is required by outside attorneys in proceedings involving the Department.

(2) Consult in determining what level of classified information is releasable by the USG to specified foreign countries in support of LAAs.

(3) Provide legal sufficiency reviews as requested by the CPSOs and the Director.

h. Office of Enterprise Assessments and Office of Inspector General. Assess the personnel security processes within the Department to ensure their compliance with national and Departmental policy.

i. Office of Intelligence and Counterintelligence. Conduct counterintelligence assessments and assist with the personnel security process as needed in accordance with paragraph 4.o.(12)(e).

6. INVOKED STANDARDS. This Order does not invoke any DOE technical standards or industry standards as required methods. Any technical standard or industry standard that is mentioned in or referenced by this Order is not invoked by this Order. Note: DOE O 251.1D, Appendix J provides a definition for "invoked technical standard."

7. REFERENCES. See Attachment 7.

8. DEFINITIONS. See Attachment 8.

9. CONTACT. Questions concerning this Order should be addressed to the Office of Environment, Health, Safety and Security, Office of Departmental Personnel Security, at 202-586-3249.

BY ORDER OF THE SECRETARY OF ENERGY:

DAVID M. TURK
Deputy Secretary

TABLE OF CONTENTS

APPENDIX A:
POSITIONS REQUIRING BACKGROUND INVESTIGATION BY THE FEDERAL BUREAU OF INVESTIGATION

Per section 145e. of the Atomic Energy Act (AEA), individuals occupying or under consideration for positions requiring access to information in a Special Access Program (SAP) must have their required background investigation (and reinvestigations) conducted by the Federal Bureau of Investigation (FBI). Background investigations (and reinvestigations) for individuals requiring access to Sensitive Compartmented Information (SCI) are not included in this population and will be submitted, per the processes set forth in this Order, to the Defense Counterintelligence and Security Agency (DCSA).

Additionally, per section 145f. of the AEA, the DOE has the authority to identify other positions which, either by virtue of the program in which they reside or other reasons, are of a high degree of importance or sensitivity that, upon certification, also require investigation (and reinvestigation) by the FBI. Under this authority, positions requiring confirmation by the United States Senate will be subject to background investigations and reinvestigations by the FBI.

APPENDIX B:
PERSONNEL SECURITY FILES

1. Safeguarding.

a. Personnel Security Files (PSFs) and electronic Personnel Security Files (ePSFs) contain many different types of information that require protection, ranging from Controlled Unclassified Information (CUI) [to include Personally Identifiable Information (PII)] to classified information (see section 4.v. of this Order). The Privacy Act of 1974, as amended sets forth strict safeguarding requirements for Federal records relating to individuals, to include training, rules of conduct and other requirements for individuals whose duties involve maintaining such records. It also establishes penalties for violations of these requirements. Because of the privileged and sensitive nature of the information contained in PSF/ePSFs, these files must only be released within DOE to individuals (including contractor support staff) who have been the subject of a favorably adjudicated, current background investigation of the level required for a Top Secret security clearance, have a valid need to know, and who are authorized to:

(1) Adjudicate or otherwise process security clearances;

(2) Determine suitability or fitness for Federal employment;

(3) Certify individuals in the Human Reliability Program (HRP);

(4) Conduct official investigations into violations of criminal or civil law;

(5) Conduct counterintelligence and/or counterterrorism investigations and assessments;

(6) Evaluate individuals in support of the Department's Insider Threat Program;

(7) Ensure compliance with DOE requirements;

(8) Conduct medical and/or mental health evaluations in support of personnel security or HRP determinations; or

(9) Determine eligibility and access to a Department’s SAP.

b. Disclosure to individuals within DOE under circumstances not covered by this appendix must be made in consultation with, and with the approval of local counsel [or, for Headquarters, General Counsel (GC). Other types of disclosures may be permitted consistent with the Privacy Act and in consultation with local counsel (or, for Headquarters, the GC).

c. Reports of investigations of individuals who have been processed for security clearances may be shown to representatives of other Federal agencies conducting

background investigations for personnel security or suitability purposes or to the DOE-affiliated individuals identified above. Such individuals must show (or in the case of the Office of the Inspector General, state) that they have an official purpose for reviewing the investigation. With the exception noted below in paragraph 1.d., such individuals must not be given copies of an investigation conducted by another Federal agency, except that copies of these investigations must be given to representatives of the OIG, upon request. If copies are needed, they will be advised that the reports may be requested directly from the agency that conducted the investigation. Such individuals may be provided copies of DOE-generated documents from the PSF/ePSF.

d. Representatives from the Office of Intelligence and Counterintelligence (IN) may be provided copies of investigative reports as necessary for the performance of official duties.

e. Representatives from Program Offices who are responsible for determining eligibility and access to DOE SAPs may be provided copies of investigative reports, as necessary.

f. Pursuant to the Privacy Act of 1974, as amended, DOE-generated information may be released upon written request to a Federal, state, or local law enforcement agency in support of a criminal or civil investigation. Such a request must specify the portion of the PSF/ePSF that is desired, and the justification for seeking such information.

g. DOE-generated information may also be permitted to other government agencies to support suitability/security clearance purposes. Such permissions must be made in consultation with, and with the approval of all offices which provided source information for such document generation.

h. A record of each disclosure in accordance with 1.c.-g. above, must be recorded in the PSF/ePSF, to include:

(1) The name and position title of the individual to whom the disclosure is made;

(2) The individual's agency affiliation and address;

(3) The date of the disclosure;

(4) The nature and purpose of the disclosure; and

(5) The name and position of the person releasing the information.

i. In all instances, before releasing classified information from a PSF/ePSF to any party, the DOE representative responsible for releasing the information must verify that the intended recipient possesses the appropriate level of security clearance and has an official need-to-know.

j. Safe Files are PSFs designated as protected under a higher form of security from disclosure to those individuals identified in paragraphs 1.a.-f. above. These files include members of DOE senior leadership, members of Congress, Senators, current and former Presidents and Vice Presidents, and those individuals whose primary role within the Department of Energy is to make security clearance determinations. Individuals who have regular and/or routine access to personnel security files must obtain authorization from the Director of the Cognizant Personnel Security Office (CPSO) or designee prior to accessing safe files.

k. Maintenance, storage, and control of PSF/ePSF (both active and terminated files) is the responsibility of CPSOs and may not be delegated or otherwise assigned to local or contractor security offices.

2. Contents and Arrangement of Data in Personnel Security Files.

a. A PSF must be maintained in paper or electronic form for everyone processed for a security clearance. The CPSO initially processing an individual for a security clearance must assign a unique PSF case number to each file. The unique PSF case number assigned by the original CPSO will always be used to identify that individual's file, regardless of the current location of the PSF.

b. The PSF of any individual who is being or has been processed for a security clearance, whether active or terminated, must contain the original or a copy of any document related to a personnel security action, which may include the most recent investigative report prepared by a Federal investigative agency, and any documents, correspondence, or forms involving the initial and any subsequent security clearance action(s).

c. Paper PSFs must be arranged so that administrative material is on the left side and adjudicative and investigative material is on the right side. Material on each side of the folder must be arranged chronologically with the oldest on the bottom progressing to the newest on the top.

(1) Administrative materials include, but are not limited to, memoranda and other correspondence relating to administration of the case, including: requests for security clearances; prescreening forms; notes to the file (except notes containing investigative or adjudicative data); requests to other offices for consultations; security advisory letters; suspension correspondence, notification letters, and responses; correspondence relating to special security clearances and access authorizations; security badge and briefing forms; and similar data. A DOE F 5631.16, *File Summary Sheet*, must be placed on top of the left side of the PSF.

(2) Adjudicative and investigative materials include, but are not limited to, investigative reports used to support security clearance determinations, including: the questionnaire completed by the individual, fingerprint cards, release forms, security acknowledgment; reports of investigation from any

Federal agency or local law enforcement activity, the Office of Inspector General, or contractor security personnel; reciprocity and related material; documentation regarding security infractions; letters, memoranda, or notes to the file containing investigative data; summaries of investigations; incident reports, reports of treatment for a mental illness, drug abuse, or alcohol abuse; consultation summaries; letters of interrogatory to the individual and responses to those interrogatories from the individual; correspondence and reports relating to psychiatric and/or psychological evaluations; case evaluations; and any other material relating to the adjudication of the individual's eligibility for a security clearance.

d. The PSF/ePSF must not be used as a storage location for other documents, including, but not limited to the Classified Information Nondisclosure Agreement (SF-312). Specific storage requirements for the SF-312 are available in DOE O 470.4, *Safeguards and Security Program*, current version.

(1) Information that must be included in all PSFs/ePSFs:

(a) *File Summary Sheet* (DOE F 5631.16) or equivalent record approved by the Office of Departmental Personnel Security

(b) Clearance Access Request

(c) *Security Acknowledgement* (DOE F 5631.18)

(d) Drug Test Results, where applicable

(e) Case Evaluation Sheet, where applicable

(f) *Security Termination Statement* (DOE F 5631.29), where applicable

(2) Information that may be included in PSFs/ePSF as necessary and applicable:

(a) SF-86, *Questionnaire for National Security Positions*, or successor form

(b) Copy of Birth Certificate

(c) Education Documentation

(d) Credit Reports

(e) DCSA/FBI Investigative Results

(f) Fingerprint cards

(g) Other Government Agency Reports

(h) Special Access Documentation (e.g., SAP, SCI, HRP)

(i) Clearance Verification Forms (Reciprocity)

(j) Letters of Interrogatory and Responses

(k) SEAD 3 Reporting Form

(l) Foreign Travel Requests

(m) Controlled correspondence receipts (e.g., PS form 3811, *Domestic Return Receipt*)

(n) Request for Personnel Security Consultation

(o) Results of Personnel Security Consultation

(p) *The Conduct of Personnel Security* Interview *Under DOE Security Regulations* (DOE F 5631.5) or successor form

(q) *Privacy Act Statement for Personnel Security Interviews and Related Release Forms* (DOE F 5631.7), or successor form

(r) Waiver (*Consent to Undergo a Mental Evaluation to be Conducted by a Psychiatrist or Licensed Clinical Psychologist*) (DOE F 472.2)

(s) Psychiatric, psychological, or other mental health evaluations or reports

(t) Medical Documents

(u) Notification of Clearance Determination

(v) Clearance Extension Documentation

(w) Polygraph Examination Report

(x) Name/marital status change

(y) *Data Report on Spouse/Cohabitant* (DOE F 5631.34)

(z) Security Incident/Infraction /Issue Report Documentation

(aa) Foreign Travel Request

(bb) Counterintelligence Correspondence

(cc) Privacy Act Release

(dd) Correspondence Request for Reinvestigation

(ee) Statement of Charges/Summary of Security Concerns

(ff) Administrative Review Documentation and Appeal Documentation

(gg) *File Transfer Record* (DOE F 5631.25)

(hh) CI Assessments conducted in accordance with section 4.o.(12)(e) of this Order, and related materials

(ii) Notes to File

(jj) Other miscellaneous documents that directly relate to the adjudicative process.

APPENDIX C:
ADJUDICATIVE CONSIDERATIONS RELATED TO STATUTORY REQUIREMENTS AND DEPARTMENTAL REQUIREMENTS

1. Section 1072 of the National Defense Authorization Act for Fiscal Year 2008, 50 U.S.C. § 3343, commonly referred to as the Bond Amendment, identifies additional factors to be considered when granting or renewing a security clearance for any person covered by that statute. In any case in which the Bond Amendment applies, as detailed below, all correspondence (notification letters, referral letters, etc.) must expressly indicate this fact.

2. Illegal Use of Controlled Substances. For purposes of applying the Bond Amendment prohibition on granting or renewing a security clearance to an unlawful user of a controlled substance or an addict, the following definitions apply:

   a. An unlawful user of a controlled substance is any person who uses a controlled substance and has lost the power of self-control with reference to the use of the controlled substance or who is a current user of the controlled substance in a manner other than as prescribed by a licensed physician. Such use is not limited to the use of drugs on a particular day, or within a matter of days or weeks before, but rather that the unlawful use occurred recently enough to indicate the individual is actively engaged in such conduct.

   b. An addict of a controlled substance is as defined in 21 U.S.C. § 802(1), which is any individual who habitually uses any narcotic drug so as to endanger the public morals, health, safety, or welfare; or is so far addicted to the use of narcotic drugs as to have lost the power of self-control with reference to his or her addiction.

   c. Cleared incumbents and applicants who are determined to be an unlawful user or addict are subject to the Bond Amendment, and the Department will process those individuals for Administrative Review (AR) and may suspend, deny or revoke eligibility for access to classified information in accordance with 10 CFR Part 710 and this Order, as applicable.

3. Disqualifiers.

   a. The Bond Amendment disqualifies individuals from holding a Q or L access authorization (and Sensitive Compartmented Information (SCI) and Special Access Program (SAP) access) who have been:

      (1) convicted in any U.S. court of a crime, sentenced to imprisonment for that crime and, as a result incarcerated for not less than one (1) year;

      (2) discharged or dismissed from any of the Military Departments under dishonorable conditions; or

      (3) determined to be mentally incompetent by an adjudicating authority, based on an evaluation by a duly qualified mental health professional employed

by, or acceptable to and approved by, the U.S. Government (USG) and in accordance with established procedures and standards.

b. In cases falling under subparagraphs 3.a.(1)-(3), the individual's access authorization will be adjudicated in accordance with Security Executive Agent Directive (SEAD) 4 and with the procedures set forth in this Order. If a denial or revocation is warranted, the Bond Amendment will be noted as a factor as indicated in paragraph 1. above and the clearance will be processed for AR under 10 CFR Part 710.

c. If the application of SEAD 4 (or successor guidelines) and the procedures set forth in this Order indicate a favorable adjudication of the Bond issue is warranted, the CPSO may use this as the basis to request a meritorious waiver of the applicable Bond Amendment disqualifiers(s). If a waiver is sought, the CPSO will forward the case file to the Director with a recommendation that a Bond Amendment waiver be granted.

d. If the Director concurs, the file will be returned to the CPSO with direction that the waiver has been granted and that the CPSO may proceed with making its adjudicative determination. The Director will retain a list of all such waivers for periodic reporting purposes.

e. If the Director does not concur, the Director will notify the CPSO to process the Bond issue for AR under 10 CFR Part 710.

APPENDIX D:
OTHER GOVERNMENT AGENCY CLEARANCES

1. Classified Visits. The Classified Visits process must be utilized for any other government agency (OGA) personnel requiring access to Restricted Data (RD) at a DOE site.

   DOE may approve access to RD for a classified visit to DOE sites when an OGA individual has the appropriate clearance, access authorization, and a need-to-know. When utilizing the classified visit process, Cognizant Personnel Security Offices (CPSOs) are not required to grant OGA individuals a Q or L access authorization. Refer to DOE O 470.4, *Safeguards and Security Program*, current version, for guidance on processing OGA individuals for classified visits.

2. Reciprocity. OGA employees requiring access to RD for the purposes of a joint duty, detail, task force or similar type assignment at DOE, or where the OGA individual needs to access RD at their agency location, require an access authorization granted via reciprocity. The OGA is responsible for initiating and processing the investigation, and adjudication of the OGA individual's security clearance to the appropriate level to obtain an L or Q access authorization. If the OGA has granted the appropriate clearance, the CPSO may process the OGA individual based on clearance eligibility and the access will be identified in DOE databases as OGA access.

   a. Approvals for access must be based on the following:

      (1) Sponsorship by a DOE program office. All requests for an OGA individual to obtain access to RD must contain a DOE program office sponsor.

      (2) Verification that the background investigation used for the OGA individual’s eligibility meets the requirements for the level of clearance required at DOE.

      (3) Verification of favorable adjudication of a background investigation at the appropriate level and/or enrollment in Continuous Evaluation (CE) or Continuous Vetting (CV).

   b. DOE program office sponsors must ensure that the OGA individuals understand their requirement to report security concerns (as required by SEAD 3) to their home agency and to the DOE CPSO.

   c. CPSOs must ensure that any reported security concerns are forwarded to the individual's home agency for action. If information of a security concern exists, CPSOs may terminate an OGA individual’s DOE access without recourse by the agency or the agency’s employee. The employee will not be afforded due process in relation to the DOE access.

d. A CPSO may return a request for OGA individual's access when:

(1) The background investigation conducted does not meet the requirements for the level of clearance requested; or

(2) The investigation was not favorably adjudicated for a security clearance in accordance with applicable national standards; or

(3) The CPSO has information which would indicate that the individual poses an unacceptable risk to national security or DOE assets; or

(4) A DOE program office is not willing to sponsor the clearance.

e. If a request for OGA access is denied, the decision is considered final and not subject to any due process with DOE. Furthermore, the access request will not be processed by any other means in accordance with this Order without the submission of a new complete request.

3. One-Time Access.

a. DOE may approve one-time access to classified information for OGA individuals who are U.S. citizens, and whose expertise offers specialized and important benefit and value to the USG or to individuals limited to the period needed to accomplish the national security requirement whose access is needed to accomplish the national security mission. One-time access must not exceed one year. If access is required for more than one year, the individual must be processed for a security clearance by their home organization. One-time access will not be active for multiple national security requirements unless specifically authorized by the Program Secretarial Officer. The CPSO may consider granting additional access after the request for investigation is submitted to the Investigative Service Provider.

b. The need for one-time access must originate with the DOE sponsoring organization and be approved by the CPSO. All requests for one-time access must be provided to the CPSO and include a detailed justification with all the following criteria identified:

(1) The unique qualifications of the individual and/or the unique circumstances that require divulging access to classified information;

(2) The expected benefit to the USG and national security;

(3) The expected nature, extent, and level of access to classified information; and

(4) Dates for which access is required.

c. Personally Identifiable Information (PII), as required by SEAD 8, *Temporary Eligibility*, or any successor document, must be obtained from the individual and corroborated as required in the Federal Investigative Standards (FIS) prior to granting an access authorization.

(1) For Top Secret and Q Access, information relating to an individuals' foreign contacts must also be obtained.

(2) All applicable records checks must be conducted and favorably adjudicated prior to approving access.

(3) Records documenting the approval of one-time access and the dates for which one-time access was granted must be maintained within DOE systems only and are not to be reported into national databases to include, but not limited to, the Central Verification System (CVS), Defense Information System for Security (DISS), Scattered Castles, etc.

(4) Individuals approved for one-time access must receive a comprehensive security briefing and be required to sign an approved non-disclosure agreement (i.e., SF-312 or successor) prior to receiving classified information. Individuals must be debriefed immediately when access is no longer required.

(5) One-time access may be terminated at any time with no appeal. CPSOs may accept one-time access approvals from other agencies based on their own risk assessment.

(6) One-time access must not serve as the basis for subsequent final security clearance and must not be authorized for convenience or to fill positions that would otherwise require a security clearance.

4. Revalidation. DOE sponsoring offices must revalidate the OGA personnel access authorizations every 12 months or request the CPSO remove an access authorization when the requirement no longer exists. CPSOs may remove access authorizations where a sponsoring office has failed to revalidate OGA personnel access authorizations.

APPENDIX E:
RECIPROCITY OF BACKGROUND INVESTIGATIONS

1. When determining reciprocity, CPSOs must use national personnel security databases and/or repositories to determine if any prior or current background investigations or national security eligibility adjudications exist on a covered individual.

2. CPSOs must accept background investigations completed by an authorized investigative service provider (ISP) that meet all or part of the investigative requirements for a national security background investigation, except as identified in paragraphs 2.a. and b. below. When a prior background investigation meets part of the investigative requirements, the CPSO must review the investigative record and conduct the necessary investigative checks through an authorized ISP to bring the investigation up to the current standard for the type of security clearance required.

   a. CPSOs may request the covered individual to identify any changes since the last Standard Form 86, *Questionnaire for National Security Positions* (SF-86), or successor form. CPSOs may conduct an appropriate personnel security inquiry pertaining to any changes.

   b. CPSOs must accept national security eligibility adjudications for clearances at the same or higher level conducted by an authorized adjudicative agency, except as identified in the paragraphs below:

      (1) New information of national security adjudicative relevance has been reported, developed, or made known to agency officials since the last investigation that indicates the individual no longer satisfies eligibility requirements.

      (2) The most recent national security eligibility adjudication was recorded with an exception, as defined in SEAD 4, *National Security Adjudicative Guidelines*, or successor guidelines. CPSOs may accept national security eligibility adjudications recorded with an exception based on their own risk assessment.

      (3) A Bond Amendment disqualifier applies as identified in SEAD 4 and the covered individual requires access to Sensitive Compartmented Information, Special Access Programs, or Restricted Data.

      (4) The covered individual's national security eligibility was granted on a temporary (interim), limited, or one-time basis.

      (5) The covered individual's national security eligibility is currently denied, revoked, or suspended. Absent the presence of mitigating factors or other reasons, covered individuals found to be ineligible for access to classified information or to hold a sensitive position must remain ineligible for national security duty for a minimum of one year from the date of a denial or revocation.

3. Where exceptions exist in paragraph 2.b. above, reciprocity is not applicable until the following conditions are met:

   a. If the most recent background investigation is less than seven years old, the CPSO must obtain the most recent SF-86 and background investigation. The SF-86 must be free of any derogatory information. If the SF-86 is free of derogatory information, the CPSO must adjudicate the background investigation and grant reciprocity.

   b. If the most recent background investigation is more than seven years old, reciprocity is not applicable unless the individual is enrolled in an approved continuous evaluation program and their periodic reinvestigation was deferred because of that enrollment. The CPSO must obtain a new background investigation and adjudicate the clearance request based on the new investigation until the Department has implemented periodic reinvestigation deferrals. When accepting reciprocity, the CPSOs must ensure immediate enrollment of the individual into CE.

   c. If a Bond Amendment disqualifier applies as identified in SEAD 4 or successor guidelines, the CPSO must adjudicate and obtain a waiver if appropriate, before granting reciprocity. Such requests must be processed in accordance with Appendix C.

4. CPSOs must initiate additional security processing if any of the following circumstances apply:

   a. When a background investigation has not been adjudicated or does not meet the standard for the type of security clearance requested, the agency must review the investigative record and conduct the necessary investigative checks through an authorized ISP to bring the investigation up to date and to the standard for the type of security clearance requested. The CPSO must not duplicate investigative elements that, in their determination, are unlikely to change.

   b. If the CPSO requests updated security information from the individual since the last SF-86 submission and the individual indicates there has been a change in the information provided for the last background investigation, the CPSO must review the investigative record and conduct the necessary investigative checks for the changed information.

5. Reciprocity determinations for national security background investigations and adjudications must be made within five (5) working days of receipt by the CPSO for security processing. Processing for employment, suitability, or fitness requirements is considered outside the scope of national security reciprocity determinations and will not be counted or reported as part of the security processing.

6. When additional investigative checks are authorized, the additional processing time for completion and adjudication of the investigative checks must not be counted or reported as part of the security processing to make a reciprocity determination.

7. When review of the investigative record is authorized by this Order, the time required to obtain the investigative record will not be counted or reported as part of the security processing to make a reciprocity determination.

APPENDIX F:
ACCESS BY FORMER POLITICAL APPOINTEES

1. "Access" as used in this Appendix is defined as being only to the information that the political appointee originated, reviewed, signed, or received while serving as an appointee.

2. The Program Office sponsoring the former political appointee for continued access is responsible to ensure that unauthorized disclosure does not occur.

3. Approval by the Under Secretary for Nuclear Security (NA-1) or the Director, Office of Environment, Health, Safety, and Security (EHSS-1) must be in memorandum format and include a detailed justification explaining why:

   a. A continuation of access would be in the interest of national security;

   b. How continued access would further the DOE mission and specifically by what means disapproval would cause a disruption or delay in operations; and

   c. The services of another cleared individual with the same expertise and knowledge are not available.

4. The process for obtaining authorization for continued access will proceed as follows:

   a. The Program Office submits a justification memorandum to NA-1/EHSS-1 as outlined above requesting continued access for the individual.

   b. NA-1/EHSS-1 returns its approval or disapproval to the requesting Program Office.

   c. The Program Office submits an approval action via eClearance Access Request (eCAR) to the Office of Personnel and Facility Clearances and Classification (NA-74) or the Office of Headquarters Personnel Security Operations (EHSS-43) for processing.

5. Any positions outside of Presidential Appointees Requiring Senate Confirmation (PAS) designation for which continued access is requested under EO 13526 will require coordination through the Office of the General Counsel (GC) prior to submission to EHSS-43 or NA-74. In these cases, GC will review requests for applicability under this Order, and if relevant, requests will be forwarded to NA-1/EHSS-1 for approval.

6. The process for obtaining authorization for positions outside of PAS designation will proceed as follows:

   a. The Program Office submits a justification memorandum to NA-1/EHSS-1 as outlined above requesting continued access for the individual.

b. NA-1/EHSS-1 routes the request to GC for interpretation and review of applicability under EO 13526, and GC provides their response to NA-1/EHSS-1.

c. NA-1/EHSS-1 provides their approval or disapproval to the requesting Program Office.

d. If approved, the Program Office submits the approval action via eCAR to NA-74 or EHSS-43 for processing.

7. When access is granted under this Appendix, the individual will be notified in writing by NA-74 or EHSS-43 of the approval and the limitations of their access. For purposes of access management, the clearance eligibility information will be documented in DOE clearance tracking systems only, and will not be transferable to any other agency via national databases. Specifically, this access is not used for reciprocity purposes. Authorization must not exceed a period of one year from the date of approval.

8. For political appointee positions that are not covered or approved under EO 13526, appointees may maintain their access with DOE via DOE O 321.1, *Employment of Experts and Consultants*, current version, or with other executive branch agencies via SEAD 7, *Reciprocity of Background Investigations and National Security Adjudications*, or successor directive.

APPENDIX G: PERSONAL IDENTITY VERIFICATION (PIV)

This Appendix provides the credentialing standards and procedures to promote defined goals in DOE eligibility determinations to issue HSPD-12 PIV credentials for access to federally controlled facilities and information systems:[1] the protection of the life, safety, property, or health of employees, contractors, vendors or visitors to Federal facilities; the protection of the Government's physical assets, information systems, records, including privileged, proprietary, financial or medical records; and the privacy of the individuals whose data the Government holds in its systems.

1. DEFERRED PROCESSING. If an HSPD-12 Credential applicant is currently awaiting a criminal hearing or trial; is awaiting or serving a form of pre-prosecution probation, suspended or deferred sentencing, probation, or parole in conjunction with an arrest or criminal charges for a crime that is punishable by imprisonment of 6 months or longer, or has an outstanding warrant, the adjudicator may suspend further processing and notify the sponsor of the cause. When the hearing, trial, criminal prosecution, suspended sentencing, deferred sentencing, probation, or parole has been completed, the applicant may be resubmitted to the identity proofing process to determine eligibility for an HSPD-12 Credential.

2. HSPD-12 ELIGIBILITY ADJUDICATION.

   a. The credentialing standards (adjudicative guidelines) provided in the 2008 *Final Credentialing Standards* and the 2016 PAC Memorandum, as clarified by the 2020 *Credentialing Standards Procedures*, and any future iterations of such standards, must be applied to determine eligibility for an *HSPD-12* PIV credential for physical or logical access to federally controlled facilities and/or information systems.

   b. The following six standards must be applied when adjudicating an individual's eligibility for an HSPD-12 PIV credential which provides logical and/or unescorted physical access. The six standards may also be used when determining an individual's suitability for other credentials, e.g., LSSO, which provides logical and/or unescorted physical access. A PIV card will not be issued to a person if:

      (1) The individual is known to be, or reasonably suspected of being, a terrorist;

[1] The term "federally controlled", as it relates to facilities and information systems is defined in 48 Code of Federal Regulations §2.101.

(2) The individual's claimed identity cannot be verified;

(3) There is a reasonable basis to believe[2] that the individual has provided fraudulent information concerning his or her identity;

(4) There is a reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information;

(5) There is a reasonable basis to believe the individual will use a PIV card outside the workplace or inappropriately; or

(6) There is a reasonable basis to believe the individual will use federally controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems, or engage in inappropriate uses of such systems.

c. Additionally, the following supplemental standards must be applied to the adjudication of eligibility for individuals who do not require a suitability determination or security clearance. DOE may consider denying or revoking a PIV card to an individual based on one of these supplemental credentialing standards.

(1) There is a reasonable basis to believe based on the individual's misconduct or negligence in employment, that issuance of a PIV card poses an unacceptable risk;[3]

(2) There is a reasonable basis to believe based on the individual's criminal or dishonest conduct, that issuance of a PIV card poses an unacceptable risk;

(3) There is a reasonable basis to believe based on the individual's material, intentional false statement, deception, or fraud in connection with contract employment, that issuance of a PIV card poses an unacceptable risk;

[2] A "reasonable basis to believe" occurs when a disinterested observer, with knowledge of the same facts and circumstances, would reasonably reach the same conclusion.

[3] An "unacceptable risk" refers to a threat to the life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; to records, including classified, privileged, proprietary, financial, or medical records; or to the privacy of data subjects, which will not be tolerated by the Government.

(4) There is a reasonable basis to believe based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;

(5) There is a reasonable basis to believe based on the nature or duration of the individual's illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;

(6) There is a statutory or regulatory bar that prevents the individual's contract employment; or would prevent federal employment under circumstances that furnish a reasonable basis to believe that issuance of a PIV card poses an unacceptable risk; or

(7) The individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

d. A new credentialing determination will be required if there has been a break in service (or in a contractor's association with Government contract work) exceeding 24 months following the favorable adjudication of the previously conducted investigation.

e. In the adjudication process, the adjudicator shall have the authority to obtain additional information as may be deemed necessary to resolve possible issues of concern pertaining to the applicant.

f. An Individual who has received an unfavorable national security eligibility determination under E.O. 12968, *Access to Classified Information*, may undergo an HSPD-12 eligibility determination if the individual's employment is not terminated due to the unfavorable information.[4] The unfavorable national security adjudication determination may be sufficient basis for non-issuance or revocation of a PIV credential.

3. NON-UNITED STATES NATIONALS CREDENTIALING: The following credentialing standards must be applied to non-U.S. nationals[5] who work as employees or contractors for Federal departments or agencies or others who require long-term logical or physical access to Federal government facilities.

a. In circumstances where investigative standards cannot be met, a PIV must not be issued.

---

[4] If an individual who otherwise meets these standards is found: 1) unsuitable for the competitive civil service under 5 CFR part 731, 2) ineligible for access to classified information under E.O. 12968, 3) disqualified from appointment in the excepted service or from working on a contract, or 4) ineligible to hold a national security sensitive position, the unfavorable decision may be a sufficient basis for non-issuance or revocation of a PIV card.

[5] The term "United States national" includes both U.S. citizens and U.S. non-citizen nationals (i.e., American Samoans).

b. Reciprocity rules do not apply to alternative identity credentials, e.g., alternative credentials issued by another Federal agency when a PIV cannot be issued.

c. Non-U.S. national credentials must indicate the specific site to which the individual is granted access. The site name must be printed on the credential; for the GSA USAccess credential, the site name must be placed in the Agency Specific Data field.

d. Due to limitations that apply to the employment of non-U.S. nationals and the ability to collect background investigation information in locations outside the United States, special considerations apply when a PIV credential is needed for a non-U.S. national.

(1) The employment verification requirements for Non-U.S. national federal employees or contractors are:

(a) Verify employment eligibility through E-Verify for non-U.S. nationals living in the U.S.

(b) Verify immigration status through the United States Customs and Immigration Service's (USCIS) Systemic Alien Verification for Entitlements (SAVE)[6] system for non-U.S. nationals living in U.S. territories (other than American Samoa).[7]

(2) The background investigation requirements for non-U.S. national federal employees or contractors are dependent on the residency status and length of time in the U.S. of the non-U.S. national.

(a) Non-U.S. nationals living in the U.S. or a U.S. Territory for three or more years continuously and immediately preceding the start of the Federal affiliation require a Tier 1 investigation or equivalent after employment authorization or immigration status is verified.

(b) Non-U.S. nationals living in the U.S. or a U.S. Territory for less than three continuous years preceding the start of the Federal affiliation cannot be processed for a Tier 1 investigation. At the Head of Departmental Element's discretion, based on a risk determination, an LSSO badge, may be issued until the employee or contractor in question has resided for three years in the U.S. or

[6] https://www.uscis.gov/save

[7] The U.S. territory of American Samoa is not included in the "United States" as defined by the Immigration and Nationality Act, and therefore the DHS E-Verify and SAVE verification programs are unable to verify work authorization or immigration status of individuals in American Samoa. Departmental elements should conduct such background investigation as may be possible and appropriate under the circumstances in this territory.

U.S. Territory. If an LSSO is issued; the following checks[8] must be completed:

1 Federal Bureau of Investigation (FBI) fingerprint based National Criminal History Check (NCHC) must be completed before an LSSO badge is issued;

2 FBI Investigations Files name check;

3 Terrorist Screening database name check;

4 USCIS check against SAVE system; and

5 Any additional checks deemed necessary by the Department or Head of Departmental Element.

4. UNFAVORABLE PIV DETERMINATIONS.

a. For cases where the adjudicative process results in an unfavorable credentialing determination, the adjudicating office must do the following:

(1) Within two working days of the determination, furnish the individual a comprehensive written explanation of the basis for the denial or revocation of PIV eligibility to the degree that the national security interests of the United States and other applicable law permits;

(2) Afford the individual a response opportunity (written) and 30 days to provide information or documentation that may refute or alleviate the concerns; and

(3) Evaluate the individual's response, and, if the concerns are not eliminated or adequately addressed, notify the individual in writing of the final unfavorable determination and apprise the individual of the appeals process available to the individual as detailed below, including contact information.

b. Report unfavorable PIV eligibility determinations to the contract entity that employs or seeks to employ the covered individual. While it is appropriate to advise the contractor that an unfavorable PIV eligibility determination has been made, it may not be appropriate to disclose additional information about the basis for the determination.

5. PIV APPEAL PROCESS.

[8] The listed checks will provide limited results, does not constitute a Tier 1investigation, and will not be documented as a Tier 1 investigation.

a. The identity verification appeal process does not interfere with DOE's discretion to make suitability or access authorization (security clearance) determinations either before or after a person has entered on duty.

b. Upon receipt of the adjudicator's denial or revocation of HSPD-12 Credential notice, an individual has ten working days to inform the adjudicator in writing, or by electronic means (e.g., email), of the intent to file an appeal. The individual may be represented and advised by counsel or a representative of the individual's choosing in the appeal process, at the individual's expense.

c. The individual must file the actual written appeal with the adjudicator within 30 working days after notifying the adjudicator of intent to file. The appeal must be submitted in writing and provide a response to the information that formed the basis of the denial or revocation of the HSPD-12 Credential.

d. Upon receiving the individual's notification of intent to file an appeal, the adjudicator will notify the contract entity that employs or seeks to employ the covered individual.

e. Upon receiving the individual's notification of intent to file an appeal, the adjudicator will identify and notify members of the appeal panel. The appeals panel cannot include the individual who made the initial decision to deny or revoke the PIV eligibility. The appeal panel will consist of three members, who must be DOE employees who have been investigated to a level commensurate with the person filing the appeal, as follows:

(1) A representative of the Departmental or Field Element having cognizance over the site, appointed by the head of that element;

(2) A DOE attorney designated by the General Counsel; and

(3) A representative of the security office for the hiring site, appointed by the head of the relevant Departmental or Field Element.

f. Upon receipt of the written appeal, the adjudicator prepares an appeal package for each panel member consisting of a copy of all identity proofing documentation, the background investigation, the notification of denial or revocation of the HSPD-12 Credential providing the adjudicator's rationale for denial or revocation, and the written appeal of the individual.

g. Each panel member will review the package and within 30 working days respond to the adjudicator in writing indicating either concurrence or nonconcurrence with the denial or revocation of the HSPD-12 Credential decision. For any nonconcurrence, the panel member will provide a brief rationale.

h. The decision of the appeal panel will be determined by simple majority of concurrence or nonconcurrence. This decision is final. The adjudicator will

inform the appellant and sponsor of the appeal decision and, in those instances where there is majority nonconcurrence with denial or revocation of the HSPD-12 Credential, the HSPD-12 Credential will be issued in accordance with the PCI Operations plan.

6. TRANFERS FROM OTHER GOVERNMENT AGENCIES. DOE will accept PIV card credentialing determinations made by other Federal agencies under the following conditions:

   a. The PIV eligibility determination was a favorably adjudicated final (not interim) determination at the appropriate tier for the new position based on a completed Tier 1 or equivalent or higher level of investigation;

   b. There has been no break in service (or in a contractor's association with Government contract work) exceeding 24 months following the favorable adjudication of the previously conducted investigation; and

   c. DOE is not in possession of any new information that calls into question the person's eligibility for a PIV credential."

7. SUSPENSION OF PIV ELIGIBILITY.

   a. An individual’s PIV may be suspended (suspending an Active PIV credential and associated access privileges granted by the credential) when DOE is in possession of credible adverse information that a person may pose an unacceptable risk (to the life, safety, property, or health of employees, contractors, vendors, or visitors to a Federal facility; to the Government’s physical assets or information systems; to records, including privileged, proprietary, financial, or medical records; or to the privacy of the individuals whose data the Government holds in its systems), and the nature of the risk must be assessed in accordance with the respective organizations’ implementation guidance.

   b. Credible adverse information must be referred for other action as necessary and appropriate and in a timely manner, including referral to the Office of Inspector General, as appropriate, pursuant to DOE O 221.1, *Reporting Fraud, Waste and Abuse to the Office of Inspector General*, current version. Appropriate referrals could be to local law enforcement, a Local Insider Threat Working Group, a physical security office, a counterintelligence office, or the FBI, depending on the circumstances.

   c. When information is received that suggests the person presents an imminent risk to facilities or information systems or a danger to the occupants and visitors to a facility or to the public, immediate action must be taken to retrieve the PIV credential from the credential holder if the nature of the risk permits. Additionally, the technical features of the credential that enable access to facilities

and information systems must be revoked and the individual denied access to facilities and information systems until resolution of the issue.

d. The following examples describing information about a covered individual derived from self-reporting or third-party reporting may warrant immediate suspension of credentials. They are provided for illustrative purposes and are not intended to be exhaustive. They do not replace the measured judgment and consideration of all circumstances surrounding the issue.

(1) Known or reasonable suspicion of terrorist activities or involvement.

(2) Known or reasonable suspicion of activities demonstrating that the individual has used or intends to use his or her PIV credential or credential tokens to permit access to a Government facility or information system to do harm or permit others to do harm to the facility, its occupants, or its systems.

(3) Known activities, or reasonable suspicion or threat of activities, designed to corrupt, destroy, or otherwise affect the operating status and availability of critical Government information systems.

(4) Gaining, attempting to gain, or assisting others in their efforts to gain unauthorized access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information with intent to compromise the information, commit identity fraud, or to otherwise use the information in a malicious or harmful way.

(5) Violent actions or the threat of violent actions at a Federal workplace.

(6) Bringing, or attempting to bring, an unauthorized weapon into a Federal workplace.

(7) The covered individual's expression of his or her intent to harm or kill him or herself or others.

(8) The covered individual's behavior or statements that allow a reasonable inference that he or she intends to harm him or herself or others.

e. When the risk is not deemed to be imminent, but there is a reasonable basis to believe there may be an unacceptable risk due to issues that potentially impact the individual's eligibility for a PIV credential, discretion exists to determine if the PIV credential and all associated technical features enabling access to facilities and information systems should be suspended or if the individual should retain access until the matter is fully resolved.

f. Derogatory information that results in the suspension of PIV eligibility must also result in the appropriate suspension (or if suspension is not available, the revocation) of the access to physical facilities and information systems.

(1) When possible and advisable, all available information should be reviewed, including, but not limited to the PIV credential holder's explanation, before deciding to suspend (or revoke) the PIV credential. However, there is no requirement to do so if, the delays created by this review would increase risk. The decision maker should err on the side of caution and safety and suspend or revoke the PIV credential if credible information is received that there is an imminent risk or danger.

(2) Site-specific procedures to issue emergency notifications when imminent risk calls for immediate suspension or revocation must be established.

(3) The suspension or revocation steps are particularly important if the credential cannot be safely recovered from the credential holder. Suspension or revocation protocols must be developed for circumstances when a PIV credential eligibility is to be suspended. The protocols must be designed to effectuate an immediate suspension or revocation of the card's functionalities, to include physical, logical, and derived accesses.

g. Regardless of the means used to suspend or revoke the PIV card, the following must be accomplished in a timely manner to mitigate the unauthorized use of the card:

(1) Whenever possible, collect and secure the PIV credential.

(2) Immediately alert all access points at the sponsoring Federal facility (and any other facilities where the individual has been granted access) that the PIV credential and credential tokens have been suspended; provide a physical description or picture of the person when there may be an imminent risk or safety concern, if possible.

(3) Terminate any existing access privileges to IT systems and applications, including remote access.

(4) Report the individual's PIV credential eligibility as "suspended" in USAccess, Central Verification System (CVS),[9] or successor data system, as applicable. The USAccess application is the authoritative source for identifying and executing suspensions and terminations of all PIV credentials.

[9] Joint Federal Investigations Notice and Suitability and Credentialing Executive Agent Notice/NBIB Notice No.18-02 Suit/Cred EA Notice No.18-01 dated April 05, 2018.

(5) As appropriate, notify and coordinate with Local Insider Threat Working Groups and/or Federal and local law enforcement offices through established channels, and notify and coordinate with the Office of Inspector General, as appropriate, pursuant to DOE O 221.1, current version.

(6) The derogatory information that resulted in suspension of the credential is reportable for national security eligibility or counterintelligence reasons as follows:

(a) If the person in question occupies a sensitive position, notify the office which is responsible for determining national security eligibility, as appropriate, as well as the Local Insider Threat Working Group.[10]

(b) If the person in question occupies a non-sensitive position, the underlying derogatory information will dictate whether counterintelligence and/or insider threat authorities should be notified.[11]

(7) When suspending PIV eligibility of contractor employees, the contracting company must be notified of the suspension. While it is appropriate to advise the contractor that a suspension has occurred, it may not be appropriate to disclose additional information about the basis for the determination.

[10] See Security Executive Agent Directive 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position (2017).
11IBID

ATTACHMENT 1:
CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 472.2A, *PERSONNEL SECURITY*

This Contractor Requirements Document (CRD) prescribes requirements and procedures necessary for U.S. Department of Energy (DOE), including the National Nuclear Security Administration (NNSA, hereafter referred to uniformly as DOE, unless otherwise specified), contractors to efficiently and effectively process their employees for DOE security clearances. These requirements incorporate and supplement requirements found in Title 32 Code of Federal Regulations (CFR) Part 117, *National Industrial Security Operating Manual* (NISPOM), and the CRD attached to DOE Order (O) 470.4, *Safeguards and Security Program*, current version.

The contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with this CRD. Unless otherwise specified, all references in this CRD to contractors apply to both prime contractors and subcontractors.

A violation of the provisions of this CRD relating to the safeguarding or security of Restricted Data (RD), Special Nuclear Material (SNM) or other classified information or matter, may result in a civil penalty pursuant to section 234B of the *Atomic Energy Act of 1954* (AEA), as amended (42 U.S.C. 2282b). The procedures for the assessment of civil penalties are in Title 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations* (10 CFR Part 824).

In addition to the requirements set forth in this CRD, contractors are responsible for complying with all Attachments (2-8) to this Order referenced in and made a part of this CRD, and which provide program requirements and/or information applicable to contracts in which this CRD is included.

As stated in the DOE Acquisition Regulation (DEAR) found at 48 CFR Part 970.5204-2, titled *Laws, Regulations, and DOE Directives*, regardless of the performer of the work, site/facility contractors with the CRD incorporated into their contracts are responsible for compliance with the CRD. Affected site/facility management contractors are responsible for inserting the requirements of the CRD into subcontracts at any tier to the extent necessary to ensure compliance with the CRD.

In performing actions under this Order, the contractor may encounter personally identifiable information (PII). Loss or compromise of PII must be reported in accordance with the provisions of the CRD attached to DOE O 206.1, *Department of Energy Privacy Program*, current version, as applicable.

The AEA and Executive Order 12968 provide the basis for DOE's personnel security program, which encompasses sets of activities for determining an individual's eligibility for access to classified information or SNM.

1. General Requirements for Security Clearances.

   a. Security clearance requests for Key Management Personnel (KMP) and other contractor employees where there is a pending Facility Clearance (FCL) request must be managed in accordance with DOE O 470.4, *Safeguards and Security Program*, current version, and the NISPOM.

   b. Security clearances must only be requested and maintained at the minimum number necessary to ensure operational efficiency.

   c. The contractor must submit a security clearance request to DOE only after determining the security clearance is essential for the individual to perform tasks or services stipulated in the contract.

   d. The contractor must not request a security clearance to:

      (1) Avoid the use of access controls or physical barriers to distinguish perimeters among security areas or between security and open areas, or to alleviate responsibilities for escorting individuals without security clearances within a controlled area. Federal Site Managers must require such contract employees to have security clearances if, in their judgment, operational necessities or cost considerations require it and inadvertent access to classified information or SNM by these individuals cannot otherwise be reasonably prevented.

      (2) Alleviate individual or management responsibilities for properly protecting classified information or SNM or controlling dissemination of classified information or SNM on a need-to-know basis.

      (3) Determine an individual's fitness for employment with the contractor.

      (4) Establish a pool of contractor employees with pre-existing security clearances.

      (5) Accommodate an individual's personal convenience, expedience, gain or advantage.

      (6) Anticipate unspecified classified work.

   e. A security clearance must be requested only when required to avoid the unnecessary expenditure of DOE resources and the unwarranted invasion of an individual's privacy.

   f. Individual access to classified information or SNM must not be permitted until notification has been received from DOE that a security clearance has been granted. Verbal notification from the CPSO may be accepted, to be followed by written confirmation of the action.

g. Security clearances must be requested only for individuals who are United States (U.S.) citizens and are at least 18 years of age.

h. Only authorized DOE Federal employees can render a formal security clearance determination; however, contractors are authorized to take actions that affect an individual's access, such as restricting access to classified information or SNM when a security clearance is terminated or administratively withdrawn, or obtaining a DOE F 5631.29, *Security Termination Statement*, prior to the individual's departure.

i. Contractor personnel must provide logistical assistance (see paragraph 4.e. below) to DOE and Federal investigative agencies for conducting initial investigations, reinvestigations (if applicable), and additional investigations when authorized by DOE.

j. DOE retains authority in all matters related to DOE personnel security activities. Personnel security activities are not subject to collective bargaining between contractor management and labor.

k. The contractor must not use an individual's security clearance status as a determining factor for hiring, entering into a consultant agreement, or awarding a subcontract.

l. Contractor management officials or other employees must not use DOE personnel security requirements to coerce, restrain, threaten, intimidate, or retaliate against individuals for exercising their rights under the Constitution or under any statute, regulation, or DOE directive.

m. Unless otherwise stipulated, the contractor will not be required to reimburse DOE for costs associated with processing the contractor's applicants or employees for investigative or other types of actions related to security clearances.

2. Security Clearance and Access Authorization Types.

a. Security clearances and access authorizations denote an individual's eligibility for access to a particular type of classified information or material, such as National Security Information (NSI), RD, SNM or Sensitive Compartmented Information (SCI). Unless otherwise specified, access authorizations and security clearances are commonly referred to as security clearances throughout this CRD.

b. This section describes those security clearances and access authorizations for which DOE cognizant personnel security offices (CPSO) are responsible. Other access authorizations issued by DOE appear in Attachment 2.

c. Security Clearances.

(1) Top Secret. A Top Secret (TS) security clearance is required for access to NSI, as defined by EO 13526, classified at the TS level and Formerly

Restricted Data (FRD), as defined by the AEA at the TS level. A TS security clearance also permits access to NSI and FRD classified at the Secret and Confidential levels.

(2) Secret. A Secret (S) security clearance is required for access to NSI and FRD classified at the S level. A Secret security clearance also permits access to NSI and FRD classified at the Confidential (C) level.

(3) Confidential. A Confidential (C) security clearance is required for access to NSI and FRD classified at the C level.

Granting a TS or S security clearance does not give the recipient approval for a Q or L access authorization without the appropriate need-to-know by the recipient.

d. Access Authorizations.

(1) Q. A Q access authorization is required for access to:

(a) RD, as defined by the AEA, classified at the TS or S level;

(b) SNM, as defined by the AEA, designated as Category I and other categories with credible roll-up to Category I;

(c) A Q access authorization permits access to information and material described below for L access authorizations;

(d) A Q access authorization also allows access to information listed under TS, S, and C security clearances above.

(2) L. An L access authorization is required for access to:

(a) RD classified at the C level and/or SNM designated as Categories II and III, unless special circumstances determined by a site vulnerability assessment and documented in associated site security plans mandate otherwise;

(b) An L also allows access to information listed under S and C security clearances above.

3. Pre-Employment and Pre-Processing Requirements.

a. The contractor must require applicants and employees selected for positions requiring security clearances to provide evidence of U.S. citizenship and must verify such evidence when requesting that the individuals be processed for security clearances. Acceptable evidence of U.S. citizenship consists of the following:

b. For an individual born in the U.S., a current or expired U.S. passport or passport card or a birth certificate are the primary and preferred means of citizenship verification. Acceptable birth certificates must show that the record was filed shortly after birth and must be certified with the registrar's signature. The birth certificate must bear the raised, impressed, or multi-colored seal of the registrar's office. The only exception is if a state or other jurisdiction does not issue such seals as a matter of policy. Uncertified copies of birth certificates are not acceptable. A delayed birth certificate (one created when a record was filed more than one year after the date of birth) is acceptable if it shows that the report of birth was supported by acceptable secondary evidence of birth. Secondary evidence may include baptismal certificates, hospital birth records or affidavits of individuals having personal knowledge about the facts of the birth. Other documentary evidence can be early census, school, or family records; newspaper files; or insurance papers. All documents submitted as evidence must be original or certified.

c. For an individual claiming citizenship by naturalization, a *Certificate of Naturalization (*Form N-550 or N-570) showing the individual's name is required.

d. For an individual claiming citizenship acquired by birth abroad to a U.S. citizen, one of the following (showing the individual's name) is required:

(1) Certificate of Citizenship (Form N-560 or N-561),

(2) Consular Report of Birth Abroad of a Citizen of the U.S. of America (State Department Form FS 240)

(3) N-600, Application for Certificate of Citizenship

(4) *Certificate of Birth* (Form FS 545 or DS 1350),

(5) A current or expired U.S. passport, or passport card

e. The contractor must not concurrently submit an applicant or employee for a DOE security clearance and a security clearance with another Federal agency. If a security clearance is required to perform work on classified contracts at DOE and one or more other agencies, the contractor will submit the request for the highest security clearance necessary and rely upon reciprocity for lower clearances.

f. The contractor must furnish information pursuant to 48 CFR 952.204- 2(h)(2)(vi) [the DEAR Clause], if required by the CPSO.

4. Processing DOE Security Clearance Requests.

a. Security clearance requests must be forwarded through established channels to the CPSO using the DOE F 473.3, *U.S. Department of Energy Clearance Access Request* (DOE F 473.3), or eClearance Access Request. Requests must include a cover letter or form that requests the security clearance and provides the

justification for processing (additional documentation may be required by the CPSO).

The justification must describe in detail (without revealing classified information) the duties of the position and the levels and types of classified information or SNM to be accessed. The contractor must also indicate whether the individual holds or has held a security clearance issued by DOE or any other Federal agency. General statements such as "A security clearance is required to perform contractual duties" are unacceptable, as are statements that policy requires all applicants or employees to be processed for security clearances. The following represents an example of an acceptable justification:

(1) "Mr./Ms._____is a computer system engineer with ABC, Inc. involved in systems analysis in support of XE-50. The duties of the position will require access to plans and operations concerning the Tritium Recovery Facility for the MHGTR, which are classified as Secret."

(2) Verification of the individual's evidence of U.S. citizenship, as detailed in paragraph 3.a. above.

(3) The DOE contract or subcontract number under which the security clearance is being requested.

(4) Information regarding contractor reviews, pursuant to 48 CFR 952.204- 2(h)(2)(vi) [the DEAR Clause], if required by the CPSO, and

(5) Additional documentation set forth in Attachment 2.

b. The contractor must also:

(1) Designate certain employees to review completed security forms and all related material for adequacy and completeness before they are submitted to DOE.

(2) Advise employees and applicants for employment in writing that their forms will be reviewed only by those designated employees and that such information will not be used for any other purpose within the company.

(3) Elect whether to maintain copies of the individual's security forms in paper or electronic format. If the contractor elects to maintain copies of the individual's security forms, the individual must be informed of the contractor's policy concerning copies of the security forms, the contractor's procedures for protecting the information from unauthorized disclosure, and the procedures by which the individual may obtain access to, or copies of, the security forms maintained by the contractor. The contractor should recommend to the individual that they maintain copies of their completed security forms for personal records.

c. Establish written procedures for the protection of security clearance request information, including procedures for the following:

(1) Designating responsible employees who are trained in the procedures for reviewing completed security forms before their submission to DOE.

(2) Informing all employees with access to completed security forms, pre-employment or pre-processing check information and other security clearance-related information of their responsibility to protect the information from unauthorized disclosure.

(3) Ensuring individuals can complete and submit all forms or other data collections required during the security clearance process in private. Assistance in completion of any forms will be provided by a contractor employee who has been specifically designated by the contractor to review such forms.

d. Deficient security clearance requests will be returned to the contractor by the CPSO with a clear indication of the nature of the deficiency(ies). The contractor must ensure that deficient requests are corrected and returned to the CPSO in a timely manner.

e. The contractor must assist in the timely processing of security clearance actions by:

(1) Ensuring the availability of the contractor applicants and employees for the conduct of personal interviews by the investigative service provider or consultations by DOE personnel security staff, and

(2) Ensuring that other employees are made available, as needed, to provide information during the conduct of all personnel security background investigations.

f. The contractor is responsible for reviewing, approving, and submitting security clearance requests for its subcontractor, consultant, or agent applicants or employees. Such requests must be kept to a minimum in accordance with DOE requirements.

5. Temporary Eligibility.

a. When urgent operational or contractual exigencies or exceptional circumstances exist, CPSOs may grant temporary security clearance eligibility in accordance with Attachment 4.

b. Temporary Access to Classified Information (Interim Security Clearances). Only under exceptional circumstances when such action is clearly consistent with Departmental and national interests will a contractor applicant or employee, pending completion of the appropriate investigation, be permitted to have

temporary access to classified information. Interims are temporary measures pending completion of an expedited investigation, which must be in process. Non-U.S. citizens are not eligible for interim access to classified information or SNM. Contractors may submit a request that a particular applicant or employee be considered for interim access when providing justification for the security clearance request [see paragraph 4.a.(1) above] but determinations regarding whether any individual is afforded such access is solely the purview of Federal CPSO staff. See Attachment 4 for additional information regarding interims.

c. Temporary Access to a Higher Level of Classified (Temporary Security Clearances Upgrade).

(1) Circumstances may arise where an urgent operational or contractual exigency exists requiring a cleared DOE contractor employee to have non-recurring (not to exceed 180 days) access to classified information or SNM at a higher level than is authorized by their existing security clearance. When access is expected to exceed 180 calendar days, the sponsor will request a Temporary Access to Classified information in accordance with paragraph 5.a. above.

(2) In such situations, and only for compelling reasons in furtherance of the DOE mission, the contractor must certify the need in writing and submit it to the appropriate Federal Site Manager. If the Federal Site Manager is satisfied that exigent circumstances exist, the Federal Site Manager must certify the need for the security clearance in writing and submit it to the appropriate CPSO. The CPSO may consider the request and grant or deny the security clearance in accordance with procedures set forth in Attachment 4.

d. One-Time Access to Classified Information.

(1) During exceptional circumstances, DOE contractor employees may be approved for one-time access to classified information when it is determined to be in the national security interest. One-time access will be limited to DOE contractor employees whose expertise offers specialized and important benefit and value to the United States Government (USG), or to individuals to whom access to classified information needs to be provided in the interest of national security.

(2) One-time access must be limited to the period needed to accomplish the national security requirement and must not exceed one year. Where access is expected to be more than one year, the contractor employee is required to be sponsored for a security clearance.

(3) One-time access will only be granted to U.S. citizens with a willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A request by a contractor to process

one-time access to classified information must be approved by the most senior DOE-cleared management official of the company holding the affected contract and the DOE Program Secretarial Officer with jurisdiction over the office where the contractor employee will be employed. Specific requirements and processes related to the issuance one-time access to classified information is set forth in Attachment 4.

6. Limited Access Authorization (Non-U.S. Citizen).

a. Only U.S. citizens are eligible for a security clearance. Contractors must make every effort to ensure that only U.S. citizen employees are assigned to perform duties that may require access to classified information. However, compelling reasons may exist to grant access to classified information to a non-U.S. citizen contractor employee. Where a non-U.S. citizen possesses unique or unusual skills or expertise that is urgently needed to support a specific Departmental mission involving access to classified information, and a qualified U.S. citizen eligible for such access is not available, contractors may submit non-U.S. citizens for a Limited Access Authorization (LAA). LAAs provide limited access to certain types of classified information by non-U.S. citizens, and are subject to strict controls and conditions. Such submissions must include detailed information concerning the steps the contractor took to secure the services of a U.S. citizen.

b. LAAs must not permit access to any greater level of classified information than the USG has determined may be releasable to the country of which an individual is currently a citizen. DOE's Headquarters General Counsel must make this assessment. LAAs must only be approved if a background investigation at the level required by EO 12968, or successor national-level standards, is conducted.

c. A request by a contractor to process a non-U.S. citizen for an LAA must be approved by the most senior DOE-cleared management official of the company holding the affected contract and the DOE Program Secretarial Officer with jurisdiction over the office where the contractor employee will be employed. Specific requirements and processes related to the issuance of LAAs are set forth in Attachment 3.

7. Reporting Requirements.

a. All cleared contractor employees (including individuals with a suspended clearance) and applicants must follow the guidance in Attachment 5. Cleared contractor employees incur a special and continuing security obligation to be aware of the risks associated with foreign intelligence operations and/or possible terrorist activities directed against them in the U.S. and abroad.

b. Cleared contractor employees also have a responsibility to recognize and avoid personal behaviors and activities that may adversely impact their continued national security eligibility. Cleared contractor employees must report any

planned or actual involvement in any of the activities as indicated in Attachment 5, or otherwise as soon as possible following the start of their involvement.

c. Failure to comply with reporting requirements may result in administrative action that includes, but is not limited to, revocation of the cleared contractor employee's security clearance.

d. Reportable Information (see Attachment 5) must be reported verbally or in writing directly to the CPSO immediately upon the individual becoming aware of the situation or incident. If the information is verbally reported, a written confirmation must be submitted within three (3) working days after the situation or incident.

e. Contractors must notify the CPSO of any of the following conditions affecting the status of a contractor applicant's or employee's security clearance. All notifications under this paragraph must be made within three (3) working days followed by written confirmation within the next ten (10) working days.

(1) When made aware of any other information of a personnel security interest, as delineated in Attachment 5, concerning a contractor applicant or employee;

(2) When the contractor restricts or withdraws a contractor employee's access to classified information or SNM without DOE direction;

(3) When a cleared employee is terminated under unfavorable circumstances, regardless of the reason for the termination;

(4) When made aware of the death of a contractor applicant or employee; or

(5) When a cleared contractor employee is transferred to another location (minimally, this will apply when a contractor employee's security clearance moves to the jurisdiction of another CPSO).

f. The contractor must inform contractor applicants and employees who are applying for or in possession of a security clearance that they have a specific obligation to truthfully provide all information requested for personnel security purposes to DOE. Contractors and clearance holders must:

(1) Provide full, frank, and truthful answers to relevant and material questions.

(2) Furnish, or authorize others to furnish if necessary, information that DOE deems necessary to the security clearance eligibility process, when requested.

(3) Report any situations or incidents as they occur that may have the tendency to impact the individual's eligibility for a security clearance

verbally and in writing and directly to DOE immediately upon the individual becoming aware of the situation or incident and in no event later than three (3) working days after the event (see Attachment 5).

(4) Notify CPSO whenever they learn of the presence of any such situations or incidents that may have the tendency to impact an individual's eligibility for a security clearance regarding anyone they know to possess a DOE security clearance or to be in the process of obtaining a DOE security clearance immediately upon the individual becoming aware of the situation or incident and in no event later than three (3) working days after the event.

(5) The foregoing responsibilities apply when completing security forms, during all personnel security investigations and at any stage of the security clearance process including, but not limited to letters of interrogatory, personnel security consultations, DOE-sponsored mental health evaluations and other authorized investigative activities.

(6) All DOE contractor employee security clearance holders and applicants who are approached by any individual seeking unauthorized access to classified information or SNM, or who experience any other potentially counterintelligence-related incidents, must report such information in accordance with DOE O 475.1, *Counterintelligence Program*, current version.

g. Failure or refusal to cooperate with any of these activities may prevent DOE from granting or continuing a security clearance. In this event, any current security clearance may be administratively withdrawn or, for contractor applicants, further processing of a security clearance request may be terminated.

h. Contractor employees with active security clearances will be initially briefed and annually briefed regarding their personnel security responsibilities in accordance with the CRD attached to DOE O 470.4, *Safeguards and Security Program*, current version.

8. Administrative Withdrawal of Security Clearances.

a. The contractor must request the CPSO administratively withdraw a contractor employee's security clearance when an individual terminates employment or when official duties no longer require access to classified information or SNM. The contractor must provide the CPSO a DOE F 5631.29, *Security Termination Statement*, completed by the contractor employee, within three (3) working days upon termination of employment or when official duties no longer require access to classified information or SNM.

b. The purpose of DOE F 5631.29 is to ensure that the individual is aware of the continuing responsibility to protect classified information and SNM after withdrawal of a security clearance. In cases where it is not possible to obtain the

individual's signature, the completed but unsigned DOE F 5631.29 must still be submitted. In addition, the contractor must provide an explanation to the CPSO of the circumstances surrounding the withdrawal and why the employee's signature could not be obtained.

9. Security Clearance Pending Reemployment/Reassignment. The CPSO may approve a contractor request for an individual who is terminating employment with the contractor per paragraph 8.a. of this CRD to retain a security clearance when the contractor verifies that the individual will be reemployed or reassigned by the contractor within the next 90 calendar days to a position that will require a security clearance.

10. Security Clearance Reapproval Requests. The contractor must request the CPSO consider reapproving a security clearance for a contractor applicant or employee when the contractor is aware that the individual previously held a security clearance. The CPSO will advise the contractor whether the individual must complete a new set of security forms, update information previously provided, or be subject to additional investigation per the provisions of paragraph 4. of this CRD.

11. Security Clearance Upgrade Requests. The contractor must request that the CPSO upgrade a contractor employee's security clearance in accordance with any new, higher access requirements associated with the duties of the position. The request must be accompanied by appropriate personnel security forms and a revised security clearance justification statement, as directed by the CPSO.

12. Security Clearance Downgrade Requests. The contractor must request that the CPSO downgrade a contractor employee's security clearance in accordance with any new, lower access requirements associated with the duties of the position. The request must be accompanied by a revised security clearance justification statement.

13. Security Clearance Suspension, Revocation, and Denial.

    a. Upon receiving notification from the CPSO of an employee's security clearance suspension or denial of final security clearance, even after previous approval of an interim, the contractor must ensure that the employee is precluded from access to classified information and/or SNM.

    b. Suspension, denial, or revocation of an individual's security clearance does not prevent the contractor from assigning or transferring the individual to duties that do not require a security clearance.

14. Training. All cleared contractor employees and any contractor employees involved in personnel security activities must be fully qualified as necessary relative to their duties and responsibilities, in accordance with national and Departmental requirements and Attachment 6.

15. Records Maintenance.

a. The contractor must maintain current records that reflect, by contract numbers, all contractor employees granted security clearances. The records must include the contractor employee's name, PSF case number, and the date the security clearance was granted.

b. Copies of correspondence to and from DOE that reflect security clearance matters for each contractor applicant and employee must be maintained including: the request for a security clearance, notification that security clearance action was affected, and security clearance termination and administrative withdrawal action. Such copies must be maintained while the individual holds a security clearance at the contractor's request and for a period of two (2) years after the date the individual's security clearance is terminated, at which time they may be destroyed.

c. All records and information pertaining to contractor applicant and employee security clearance matters, including copies of personnel security forms and information collected from the conduct of pre-employment or pre-processing checks, must be protected against unauthorized disclosure in accordance with the *Privacy Act of 1974* (5 U.S.C 552a). Information collected by the contractor for security clearance processing must not be used by the contractor for any purpose other than that for which it is intended and must not be provided to non-contractor employees or any other entity or organization without prior approval from the CPSO.

16. Recertifications and Reinvestigations.

a. The contractor must submit a completed SF-86 on an as-needed basis once periodic deferrals of reinvestigations are implemented in the Department every five years until the Department has implemented Trusted Workforce 2.0 and as required by national standards.

b. The contractor must comply with periodic DOE requests to recertify its employees' security clearance status.

c. The contractor must comply with a request for recertification or for an examination of security clearance or other records that may be requested during the conduct of a DOE security survey or special survey.

d. The contractor must ensure that cleared contractor employees cooperate fully with DOE requirements concerning reinvestigations when applicable.

17. Actions by the Secretary. Nothing in this CRD will be construed to limit the Secretary's authorities and responsibilities under EO 12968 (section 1.2(b), et al), EO 10865 (section 9), or the AEA to grant, continue, deny, or terminate a security clearance in the interest of national security, or to modify or withhold certain AR procedures set forth at 10 CFR 710.

ATTACHMENT 2:
SECURITY CLEARANCE REQUESTS/JUSTIFICATIONS AND ACCESS AUTHORIZATIONS

[This attachment provides information and/or requirements associated with DOE O 472.2A and is applicable to contracts in which the associated CRD (Attachment 1) is included.]

1. In addition to the information set forth elsewhere in the body of this Order and in the CRD, all justifications for security clearances (for both initial and reinvestigation actions) must contain the following:

    a. Full name of the individual.

    b. Individual's Social Security Number.

    c. Date and place of birth.

    d. Individual's status (Federal employee/contractor employee).

    e. Contractor name (if contractor applicant/employee).

    f. Primary program code (e.g., EM - Environmental Management; FE - Fossil Energy and Carbon Management; IG - Inspector General; NE - Nuclear Energy; OE - Office of Enforcement; NNSA - Nuclear Security/Administrator for National Nuclear Security Administration; SC - Office of Science).

    g. Facility code (if contractor employee).

    h. Level of security clearance required, i.e., TS, S, C, Q or L.

    i. A detailed description (without revealing classified information) as to why the individual requires access. The description must include a full explanation of the information to be accessed, how often the access is needed, and for what programs/projects the information is needed.

    j. Full name, title, and telephone number of the requester.

    k. Signature of the requester.

2. All initial security clearance requests (to include first-time clearance requests and reapprovals) must include the justification, as set forth in 1. above, except in cases where reciprocity applies, as indicated by an '*':

    a. Negative results of a drug test dated no more than 90 calendar days prior to the individual's SF-86 signature or, for cases being considered under reciprocity, no more than 90 calendar days prior to the date of the security clearance request (not required for employees of state or local governments).

b. An SF-87, *Fingerprint Chart* (for Federal employees); an FD 258, *Applicant Fingerprint Chart* (for all others); or fingerprints taken electronically via an approved capture method (e.g., at a GSA-provided Homeland Security Presidential Directive-12 enrollment center), when available. Note: Fingerprints are not required if a previous investigation included a classifiable fingerprint search by the Federal Bureau of Investigations.

c. DOE F 5631.18, *Security Acknowledgement*.

3. In addition to TS, S, and C security clearances and L and Q access authorizations, all of which are granted by CPSOs, the DOE issues several other types of access authorizations. These other access authorizations are issued by the DOE office indicated:

a. Sensitive Compartmented Information (SCI). SCI access must be approved by the DOE Senior Intelligence Officer or their designated representative within the Office of Intelligence and Counterintelligence.

b. Cryptographic Information (CRYPTO). CRYPTO access is approved by the Office of Technical Security.

c. Communications Security (COMSEC). COMSEC access is approved by the Office of Technical Security.

d. Nuclear Weapon Data. Requirements and procedures for access to nuclear weapon data (categorized as SIGMA information) is determined and promulgated by the National Nuclear Security Administration (NNSA) using DOE and NNSA directives. For additional information, consult DOE O 452.8, *Control of Nuclear Weapon Data*, current version; DOE O 452.7, *Protection of Use Control Vulnerabilities and Designs*, current version; and DOE O 457.1, *Nuclear Counterterrorism*, current version.

e. Special Access Program (SAP). A SAP is a program created for a specific segment of classified information that imposes safeguards and access requirements that exceed those normally required for information at the same classification level and/or category. Access to any SAP must be granted in accordance with procedures established within DOE O 471.5, *Special Access Programs*, current version.

f. North Atlantic Treaty Organization Information (NATO). NATO access requires NNSA approval from the Office of Security Operations and Performance Assurance.

ATTACHMENT 3:
LIMITED ACCESS FOR NON-U.S. CITIZENS

[This attachment provides information and/or requirements associated with DOE O 472.2A and is applicable to contracts in which the associated CRD (Attachment 1) is included.]

Limited Access Authorizations (LAA) for Non-U.S. Citizens.

1. This section deals solely with non-U.S. citizens who have not been investigated or issued a security clearance by any foreign government. Non-U.S. citizens who have been investigated and granted the equivalent of a security clearance by a foreign government may be granted access to classified information at DOE via the passing of a security assurance by the foreign government to DOE in accordance with DOE Order 470.4, *Safeguards and Security Program*, current version.

2. Where there are compelling reasons in furtherance of a DOE mission, non-U.S. citizens who possess a special expertise may be granted limited access to classified information only for specific programs, projects, or contracts for which there is need for access. Such individuals will not be eligible for access to any greater level of classified information than the U.S. Government (USG) has determined may be releasable to the country of which the individual is currently a citizen. The Director must consult with the DOE Office of the General Counsel to make this assessment. Such limited access may be approved only if an investigation of the level required by Executive Order 12968, *Access to Classified Information*, or successor national standards, for a Top Secret (TS) security clearance can be conducted.

3. A non-U.S. citizen granted an LAA is not eligible for access to SNM or to any of the following types of classified information:

    a. TS, Cryptographic (CRYPTO), Restricted Data, Formerly Restricted Data or Special Access Program information.

    b. Information that has not been determined by a USG Designated Disclosure Authority to be releasable to the country of which the individual is a citizen.

    c. Communication Security (COMSEC) information.

    d. Sensitive Compartmented Information (SCI) or Intelligence information.

    e. North Atlantic Treaty Organization (NATO) Information. However, a national of a NATO member nation may be authorized access to NATO information provided that a NATO Security Clearance Certificate is obtained by DOE from the individual's home country and such access is limited to performance on a specific NATO contract.

        (1) Information for which foreign disclosure has been prohibited in whole or in part (identified as Not Releasable to Foreign National (NOFORN)).

(2) Classified information provided to the USG by a third party government and information furnished in confidence to the USG by a third party government.

4. The Program Secretarial Officer with jurisdiction over the information to be released to the non-U.S. citizen must submit a detailed request and justification for the desired LAA to the appropriate Cognizant Personnel Security Office (CPSO).

5. Upon receipt of the request, the CPSO will conduct a consultation with the non-U.S. citizen. The consultation does not require approval as those consultations in 4.o.(12) of the requirements section. The CPSO must determine:

   a. The nature and extent of the individual's contacts and continuing associations with individuals outside the U.S. (to include family members);

   b. The degree to which the individual exercises his or her foreign citizenship;

   c. Whether the individual or any of the individual's associates (to include family members) are or have been affiliated with any foreign government, foreign government-controlled organization or state-owned enterprise; and

   d. After completion of the consultation, the CPSO may, through the local DOE counterintelligence office, request a preliminary counterintelligence-focused risk assessment. If the results of this risk assessment indicate that it would not be feasible to continue with the LAA process, the CPSO will notify the requesting Program Secretarial Officer.

6. If the results of the risk assessment support continued processing, the CPSO will forward the results of the consultation and risk assessment, along with all other relevant information, to the Director.

7. After reviewing all available information, the Director in coordination with appropriate headquarters authorities, will:

   a. Determine to continue processing the LAA request, in which case the Director will notify the CPSO to commence processing the individual for a background investigation, or

   b. Determine that the individual will not be processed for an LAA. In this case, the Director will notify the CPSO and the applicable Program Secretarial Officer.

8. In the case of a determination as in 7.(a), above, the CPSO will process the individual for a background investigation in accordance with investigative and adjudicative procedures set forth in this Order.

9. When the CPSO has reached an adjudicative determination, the CPSO may coordinate a formal comprehensive counterintelligence-focused risk assessment with the local DOE counterintelligence office.

10. The CPSO will then forward the results of the adjudication and the risk assessment to the Director for concurrence.

11. The Director will approve/concur and instruct the CPSO to grant the LAA or will disapprove/non-concur and notify the CPSO and the applicable Program Secretarial Officer. The Director's determinations in these cases are final.

12. The CPSO must review all LAAs annually to ensure that they are still needed. The Program Secretarial Officer who initially requested the LAA must annually re-justify each request. Annual re-concurrence of the Director is not needed, provided the CPSO has no reason to believe the individual may no longer meet the requirements of the LAA. The Department retains authority to conduct routine reinvestigations as needed for individuals granted LAAs.

13. The CPSO must immediately withdraw an LAA upon receiving confirmation that the individual is no longer affiliated with DOE or otherwise no longer requires the access for which the LAA was granted, or at the direction of the Director.

14. The CPSO must immediately revoke an LAA should the CPSO come into possession of information that indicates the individual no longer satisfies the eligibility requirements for an LAA. Such revocations are not subject to the AR procedures set forth in 10 CFR 710.

ATTACHMENT 4:
TEMPORARY ELIGIBILITY

[This attachment provides information and/or requirements associated with DOE O 472.2A and is applicable to contracts in which the associated CRD (Attachment 1) is included.]

1. When urgent operational or contractual exigencies or exceptional circumstances exist, CPSOs may grant temporary security clearance eligibility in accordance with Security Executive Agent Directive 8 and this attachment.

2. Temporary Access to Classified Information (Interim Security Clearances).

   a. The need for temporary access to classified information must originate with the supervisory/management and be approved in writing by the Federal head of the applicable Departmental element in which the individual will be assigned (Note: individuals may not request temporary access on their own behalf).

   b. All such requests must be provided to the CPSO and must include a detailed justification which explains why:

      (1) A serious delay of, or interference in, an operation or project essential to a DOE program will occur unless the individual is granted access to classified information or SNM before completion of the normal security clearance process, and

      (2) The services of a qualified person who is currently cleared to access the necessary classified information or SNM cannot be obtained.

   c. Temporary access to classified information may only be requested in conjunction with, or following, the submission of an associated security clearance request, as set forth in this Order, including Attachment 2.

   d. The CPSO will review the individual's personnel security forms and PSF/ePSF (if one exists) to determine whether the case contains any information of a security concern. If so, the CPSO must notify the requester that the request for temporary access to classified information has been denied, and that the case must proceed according to normal processing procedures.

   e. Requests for temporary access to classified information in cases for which there is no information of a security concern will be approved by the CPSO and processed accordingly provided that:

      (1) The appropriate investigation has been submitted and expedited to the Investigative Service Provider (ISP).

(2) Approvals for Temporary Access to Confidential, Secret, and L require:

(a) Favorable review of a completed SF-86 by the authorized adjudicative agency;

(b) Citizenship verification; and

(c) Completion and favorable review of a Federal Bureau of Investigation (FBI) fingerprint check.

(3) Approvals for Temporary Access to Top Secret and Q require:

(a) Favorable review of a completed SF-86 by the authorized adjudicative agency;

(b) Citizenship verification; and

(c) Completion and favorable review of the following:

1 FBI fingerprint check;

2 FBI name check; and

3 National Crime Information Center (NCIC) check.

f. Supporting rationale for all temporary access to classified information will be recorded in the individual's PSF/ePSF. All temporary access to classified information will be noted as such wherever security clearances are recorded, both internally within DOE and in all DOE submissions to national security clearance databases.

g. All individuals who are issued temporary access to classified information must be notified in writing that their continued security clearance is conditional upon favorable completion of the pending investigation, and may be canceled at any point where information of a security concern arises. Cancellations cannot be appealed and adjudication of the individual's eligibility for a security clearance will continue upon receipt of the completed investigation.

h. If DOE cancels an individual's temporary access to classified information, the individual's employer must ensure that the individual is precluded from access to classified information and/or SNM.

i. Access to other programs or types of information (SAP, COMSEC, CRYPTO, SCI, NATO, or SIGMA) based upon temporary access to classified information will be granted or denied at the sole discretion of the office with authority for such access.

3. Temporary Access to a Higher Level of Classified Information.

a. CPSOs may approve temporary access to a higher level of classified information and/or SNM for a covered individual granted access to a lower level when determined necessary to meet operational or contractual exigencies not expected to be of a recurring nature pursuant to EO 12968, as amended. Access approvals will remain valid until the exigency has abated or the access is terminated. In any case, access must not exceed 180 days. When access is expected to exceed 180 calendar days, the sponsor will request Temporary Access to Classified information in accordance with paragraph 1., above.

b. Temporary access to a higher level of classified information must be necessary to meet operational or contractual exigencies not expected to be of a recurring nature.

(1) Such higher level of access will be limited to specific, identifiable information and information access records must be maintained. The nature of this information must be referenced on the request for access.

(2) Acceptable temporary access to higher level of classified information is: L to Q or TS; S to Q or TS; and any C to L or S.

c. Requests for temporary access must include a justification and must be forwarded by the appropriate official (i.e., contractor, Federal site manager) with the request to the appropriate CPSO. This submission must set forth the expected duration of the higher level of access, identify the information to which the individual will be afforded access, and describe the exigent circumstances prompting the request.

d. If the CPSO is satisfied that exigent circumstances exist, that routine processing of the individual for the higher level of access to classified information would adversely impact mission needs, is not in possession of information indicating that access at the higher level of access to classified information would jeopardize Departmental interests or the national security, and that the request is not an attempt to circumvent normal security clearance processing requirements, the CPSO must grant the higher level of access. Otherwise, the request must be denied and returned to the requester with an explanation as to the reason(s) for the denial.

e. Recipients of temporary access to a higher level of information must possess a current security clearance and the access required will be limited to classified information or SNM one level higher than the recipient's current security clearance.

f. Temporary access to higher level of classified information must be recorded in the recipient's PSF/ePSF and in the CPCI, but will not be included in submissions to inter-agency databases. Such security clearances are not subject to reciprocity.

g. Access at the higher level will be facilitated under the general supervision of a fully-cleared individual. The individual charged with providing such supervision will be responsible for the general custody of the information provided.

h. Such higher level access must be canceled and associated access terminated promptly when no longer required, at the conclusion of the authorized period of access, upon notification from the granting authority, or after 180 calendar days from when access was granted, whichever comes first.

i. If, during the period of temporary higher level access, information of a security concern arises which indicates that suspension or revocation of the individual's permanent security clearance may be warranted, the temporary higher level access will be canceled and action will be taken under 10 CFR 710 regarding the permanent clearance. No due process or other procedural rights exist regarding temporary access to a higher level of classified information.

j. Temporary access to a higher level of classified information to other programs or types of information (SAP, COMSEC, CRYPTO, SCI, NATO, or SIGMA) based upon temporary access to a higher level classified information will be granted or denied at the sole discretion of the office with authority for such access.

4. <u>One-Time Access to Classified Information</u>.

a. During exceptional circumstances, CPSOs may approve one-time access to classified information when it is determined to be in the national security interest. One-time access must be limited to individuals whose expertise offers specialized and important benefit and value to the United States Government (USG), or to individuals to whom access to classified information needs to be provided in the interest of national security.

b. One-time access must be limited to the period needed to accomplish the national security requirement and must not exceed one year. Where access is expected to last more than one year, the individual is required to be sponsored by a program office for a security clearance.

c. One-time access must only be granted to U.S. citizens with a willingness and ability to abide by regulations governing the use, handling, and protection of classified information.

d. A statement of compelling need must accompany a one-time access request, and must include the following elements:

(1) The unique qualifications of the individual(s) and/or the unique circumstances that require access to classified information;

(2) The expected benefit to the USG and national security;

(3) The expected nature, extent, and level of access to classified information; and dates for which access is required.

e. CPSOs must record, document, and maintain one-time access to classified information and the dates for which one-time access was granted locally in the Clearance Action Tracking System only.

f. One-time access will not be active for multiple national security requirements unless specifically authorized by the Program Secretarial Officer.

g. Investigative checks and required information identified below must be obtained, corroborated, and favorably adjudicated prior to granting one-time access. CPSOs must also obtain all required SF-86 consent forms:

(1) Confidential, Secret, and L Access. The following information, including PII, will be obtained from the individual and corroborated as required in the Federal Investigative Standards (FIS) prior to access authorization:

(a) Full name;

(b) Date and place of birth;

(c) Social security number;

(d) Other names used;

(e) Citizenship to include dual/multiple citizenship;

(f) Current address;

(g) Current employment;

(h) Police record; and

(i) Prior investigations and clearance.

(2) The following records checks will be conducted and favorably adjudicated prior to approving access:

(a) Intelligence Community (IC) Scattered Castles (or successor);

(b) Defense Information System for Security (DISS) or Central Verification System (CVS) (or successor); and

(c) NCIC check.

(3) Top Secret and Q Access. The following information, including PII, must be obtained from the individual and corroborated as required in the FIS prior to access authorization:

(a) Full name;

(b) Date and place of birth;

(c) Social security number;

(d) Other names used;

(e) Citizenship to include dual/multiple citizenship;

(f) Current address;

(g) Current employment;

(h) Foreign contacts, relatives, and travel;

(i) Police record; and

(j) Prior investigations and clearance.

(4) The following records checks must be conducted and favorably adjudicated prior to approving access:

(a) IC Scattered Castles (or successor);

(b) DISS or CVS (or successor);

(c) FBI name check;

(d) NCIC check; and

(e) Intelligence Indices.

h. One-time access will be restricted to specific, identifiable classified information, and will be limited only to information needed to fulfill the national security requirement.

i. Individuals approved for one-time access will not be permitted access to classified information technology systems, except under very limited conditions as approved by the Program Secretarial Officer. Such conditions require restricted access and continuous oversight and monitoring.

j. One-time access to SAP information requires the approval of the establishing authority or the designated program manager. Establishing authorities may implement policies and procedures for one-time access to their SAPs.

k. Programs must ensure classified information with dissemination control markings that require originator consent for further dissemination (e.g., Dissemination and Extraction of Information Controlled by Originator [ORCON]) be approved by

the originator to be shared with individuals who have a one-time access approval. Other control markings that restrict access to certain individuals (e.g., Caution-Proprietary Information Involved [PROPIN], ORCON-USGOV, etc.) must be adhered to.

l. Individuals approved for one-time access will receive a security briefing and be required to sign an approved nondisclosure agreement prior to receiving classified information.

m. Individuals will be debriefed immediately when access is no longer required.

n. One-time access approvals are valid only within the agency granting such access and may be terminated at any time without appeal. CPSOs may accept one-time access approvals from other agencies based on their own assessment of risk on known information about the individual.

o. One-time access approvals are not to serve as the basis for a subsequent final security clearance; nor are they authorized for convenience or to fill positions that would otherwise require a security clearance.

p. One-time access may not be used in lieu of granting temporary access to classified information (interim security clearance).

ATTACHMENT 5:
REPORTING REQUIREMENTS

[This attachment provides information and/or requirements associated with DOE O 472.2A and is applicable to contracts in which the associated CRD (Attachment 1) is included.]

The reporting requirements set forth in this Attachment in accordance with 4.w. of the requirements section of the Order, and paragraph 7. of the CRD apply to all applicants for a security clearance and covered individuals who hold a security clearance or access authorization, and/or who occupy a national security position, as set forth in 5 CFR 1400 (collectively referred to herein as "covered individuals"). Specific details required when reporting this information, beyond those listed below, will be communicated to covered individuals by the responsible office. Covered individuals will submit reportable information using the appropriate DOE Security Executive Agent Directive (SEAD) 3 reporting form or system form to be developed.

Upon recognition that a covered individual's information may include potential counterintelligence indicators [as identified by the Office of Intelligence and Counterintelligence (IN)], Cognizant Personnel Security Offices (CPSO) will refer the information to the local counterintelligence office. In addition to SEAD 3 reporting requirements, SCI access holders are also subject to the reporting requirements set forth in Intelligence Community Standard 703-02, *Reporting Requirements for Individuals with Access to Sensitive Compartmented Information*, and DOE O 475.1, *Counterintelligence Program*, current version.

1. Unofficial Foreign Travel.

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

      (1) Full itinerary;

      (2) Dates of travel;

      (3) Mode(s) of transport, including identity of carriers;

      (4) Passport number;

      (5) Emergency point of contact;

      (6) Names and association of foreign national traveling companions, and

      (7) Planned interactions with foreign governments, companies or citizens during travel and reasons for contact (routine travel/tourism-related contacts excepted).

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

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

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

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

(1) Unplanned interactions with foreign governments, companies or citizens, and the reasons for the interaction(s) (not including routine travel/tourism-related contacts);

(2) Unusual or suspicious occurrences during travel, including those of a possible security or counterintelligence significance; and

(3) Any foreign legal or customs incidents.

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

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

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

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

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

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

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

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

   a. Direct involvement in a foreign business;

   b. Opening of a foreign bank account;

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

   d. Application for or receipt of foreign citizenship;

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

   f. Voting in a foreign election;

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

6. Other Reportable Information. The following occurrences/actions must be reported to the appropriate CPSO immediately, but in no event later than three (3) working days after occurrence. This report must be in writing.

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

b. Financial anomalies including, but not limited to:

(1) Bankruptcy;

(2) Wage garnishment;

(3) Delinquency more than 120 days on any debt;

(4) Unusual infusions of assets more than $10,000 or greater, such as inheritance, winnings, or similar financial gain.

c. Action to legally change one's name;

d. Change in citizenship;

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

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

g. Hospitalization for mental health reasons.

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

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

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

b. Unexplained affluence or excessive indebtedness;

c. Alcohol abuse;

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

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

f. Criminal conduct;

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

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

ATTACHMENT 6:
PERSONNEL SECURITY QUALITY AND TRAINING

[This attachment provides information and/or requirements associated with DOE O 472.2A and is applicable to the contractors is supporting the CPSO contracts in which the associated (CRD (Attachment 1) is included.]

1. General. Quality and training are both essential to the success of the DOE personnel security program. This Attachment outlines the measures and processes in place to ensure that individuals involved in the personnel security process are trained and qualified to perform their assigned tasks and that personnel security products and services meet or exceed customers' expectations.

2. Quality.

   a. Quality measures will be in place to determine:

      (1) The accuracy and consistency of investigations and adjudicative decisions;

      (2) Compliance with reciprocity of investigations and adjudicative decisions;

      (3) Whether the Cognizant Personnel Security Office (CPSO) has sufficient resources to fulfill its function in accordance with this Order;

      (4) The timeliness of personnel security actions; and

      (5) Whether individuals are afforded due process during the security clearance determination process.

   b. CPSOs are responsible for ensuring the quality of the personnel security operations under their purview. Such reviews should include a random sampling of cases and should be accomplished within the framework of DOE O 414.1, *Quality Assurance*, current version.

   c. CPSOs are to ensure that adjudicators report quality of background investigations in accordance with Quality Assessment Standards via the Office of the Director of National Intelligence Quality Assessment Reporting Tool.

3. Training. Employees must receive personnel security training in accordance with their duties and levels of responsibility to acquire and maintain job proficiency. Training requirements and certification standards will be jointly developed by the Office of Departmental Personnel Security and the National Training Center (NTC). The NTC will maintain the training records.

   a. Supervisors are responsible for ensuring that subordinate employees performing personnel security duties are trained in accordance with the requirements of this Order as developed by NTC.

b. The NTC is responsible for the development and implementation of training courses and certification processes for the Personnel Security Program in accordance with national and Departmental policy.

c. The NTC must ensure that the training modules sufficiently enable trainees to acquire the necessary knowledge and skills to perform their duties effectively.

d. Training is required for all adjudicators, adjudicative support staff and other key officials. Adjudicative personnel are prohibited from making security clearance determinations until they have completed the NTC's Adjudication Fundamentals Course or other nationally approved training and/or have received adequate initial on the job training, as determined by the CPSO.

e. Adjudicator Training (specifics regarding sequential course titles and order will be determined by current NTC course guidelines).

(1) Initial Training. All newly appointed personnel security specialists performing adjudicative duties have one year to complete the NTC Adjudication Fundamentals Course.

(2) Adjudicative Support Training. Employees who are involved in the initial screening of cases, but do not conduct consultations or perform second or third tier reviews (e.g., security assistants, screeners) need a basic understanding of the DOE personnel security process to perform their duties effectively. All personnel performing adjudicative support functions have one year from their date of appointment to adjudicative duties to complete NTC's Adjudication Fundamentals Course.

(3) Adjudicators from other Federal Agencies. Adjudicators who are appropriately trained in accordance with the National Security Adjudicator Training Program will not have to complete NTC's Adjudication Fundamentals Course, as determined by the CPSO. The determination of the CPSO will be annotated with the NTC and a copy sent to the Office of Departmental Personnel Security.

f. Key Officials. Other employees involved in the personnel security process who have no or limited personnel security program experience require a basic understanding of the policies and procedures related to their responsibilities. These key personnel are defined as managers, deputy managers, hearing officers and hearing counsel involved with administrative review hearings conducted under 10 CFR 710, as well as DOE-sponsored consultant psychologists/ psychiatrists and appeal panel members, but may also include human resource managers, Human Reliability Program certifying officials and other managers who are less directly involved in the personnel security process. The NTC-developed and computer-based Personnel Security Awareness Briefing (or successor course/training tool) meets this briefing requirement.

ATTACHMENT 7: REFERENCES

[This attachment provides information and/or requirements associated with DOE O 472.2A and is applicable to contracts in which the associated CRD (Attachment 1) is included.]

1. 2008 National Defense Authorization Act (NDAA).
2. *Atomic Energy Act of 1954*, as amended.
3. *Privacy Act of 1974*, as amended.
4. Federal Personnel Vetting Core Doctrine
5. *National Nuclear Security Administration Act*, as amended.
6. 5 U.S.C. Section 552, *Freedom of Information Act*, as amended.
7. 15 U.S.C. Section 1681, *Fair Credit Reporting Act*, 01-03-12.
8. 21 U.S.C. 801 et. Seq *Controlled Substances Act*, 10-27-70.
9. 50 U.S.C. Section 2406, *Deputy Administrator for Naval Reactors*, 10-5-99.
10. 50 U.S.C. Section 2511, *Naval Nuclear Propulsion Program*, 02-01-82.
11. 5 CFR 1400, *Designation of National Security Positions*, 6-6-15.
12. 10 CFR 707, *Workplace Substance Abuse Programs at DOE Sites*, as amended.
13. 10 CFR 709, *Counterintelligence Evaluation Program*, 09-29-06.
14. 10 CFR 710, *Procedures for Determining Eligibility for Access to Classified Matter and Special Nuclear Material*, as amended.
15. 10 CFR 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Violations*, as amended.
16. 10 CFR 1008, *Records Maintained on Individuals* (Privacy Act), as amended.
17. 32 CFR 117, *National Industrial Security Program Operating Manual*, as amended.
18. Executive Order (E.O.) 10865, *Safeguarding Classified Information within Industry*, 02-20-60.
19. EO 12344, *Naval Nuclear Propulsion Program*, 02-01-82.
20. EO 12968, *Access to Classified Information*, as amended.

21. EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, as amended.

22. EO 13526, *Classified National Security Information*, 12-29-09.

23. EO 13549, *Classified National Security Information Program for State, Local, Tribal and Private Sector Entities*, 08-18-10.

24. EO 13764*, Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters*, 1-17-17.

25. Security Executive Agent Directive (SEAD) 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position*, 06-12-17.

26. SEAD 4, *National Security Adjudicative Guidelines*, 6-08-17.

27. SEAD 6, *Continuous Evaluation*, 01-12-18.

28. SEAD 7, *Reciprocity of Background Investigations and National Security Adjudications*, 11-09-18.

29. SEAD 8, *Temporary Eligibility*, 05-18-20.

30. *Federal Investigative Standards*, 12-14-12

31. Department of Energy (DOE) Acquisition Regulation (DEAR) 48 CFR 952.204-2, *Security Requirements*, as amended.

32. DOE O 206.1, *Department of Energy Privacy Program*, current version.

33. DOE O 206.2, *Identity, Credential, and Access Management*, current version.

34. DOE O 243.1, *Records Management Program*, current version.

35. DOE O 343.1, *Federal Substance Abuse Testing Program*, current version.

36. DOE O 414.1, *Quality Assurance*, current version.

37. DOE O 452.7, *Protection of Use Control Vulnerabilities and Designs*, current version.

38. DOE O 452.8, *Control of Nuclear Weapon Data*, current version.

39. DOE O 457.1, *Nuclear Counterterrorism*, current version.

40. DOE O 470.4, *Safeguards and Security Program*, current version.

41. DOE O 470.5, *Insider Threat Program*, current version.

42. DOE O 470.6, *Technical Security Program*, current version.

43. DOE O 471.6, *Information Security*, current version.

44. DOE O 471.7, *Controlled Unclassified Information*, current version.

45. DOE O 475.1, *Counterintelligence Program*, current version.

46. DOE O 475.2, *Identifying Classified Information*, current version.

47. DOE Administrative Records Schedule 18, *Security, Emergency Planning & Safety Records*, 3-1-2020.

48. DOE System of Records 43, *Personnel Security Clearance Files*, 01-09-09.

ATTACHMENT 8: DEFINITIONS

[This attachment provides information and/or requirements associated with DOE O 472.2A and is applicable to contracts in which the associated CRD (Attachment 1) is included.]

1. Access Authorizations. An administrative determination under the Atomic Energy Act of 1954, Executive Order 12968, or 10 CFR part 710 that an individual is eligible for access to classified matter or is eligible for access to, or control over, special nuclear material.

2. Active National Security Eligibility. An individual who is currently cleared by another federal agency with the completion of an adjudicated background investigation and subsequently has access to classified information.

3. Agency. Any "Executive agency" as defined in Section 105 of Title 5, United States Code (U.S.C.), including the "military department," as defined in Section 102 of Title 5, U.S.C., and any other entity within the Executive Branch that comes into possession of classified information or has positions designated as sensitive.

4. Authorized Adjudicative Agency. An agency authorized by law, executive order, or designation by the Security Executive Agent (SecEA) to determine eligibility for access to classified information in accordance with Executive Order (EO)12968, as amended, or eligibility to hold a sensitive position.

5. Authorized Investigative Agency. An agency authorized by law, EO, or designation by the SecEA to conduct a background investigation of individuals who are proposed for access to classified information or eligibility to hold a sensitive position or to ascertain whether such individuals continue to satisfy the criteria for retaining access to such information or eligibility to hold such positions.

6. Classified National Security Information or Classified Information. Information that has been determined pursuant to EO 13526 or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure.

7. Cognizant Personnel Security Office (CPSO). A DOE personnel security office that is authorized to submit investigative requests to investigative service providers and to adjudicate security clearances.

8. Consultation (formerly, Personnel Security Interview). A follow-up with the individual to obtain relevant information to resolve an issue(s) related to granting or continuing their eligibility for a security clearance.

9. Continuous Evaluation. Reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information.

10. Contractor. An expert or consultant (not appointed under section 3109 of title 5, U.S.C.) to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of any agency, including all subcontractors; a personal services contractor; or any other category of person who performs work for or on behalf of an agency (but not a Federal employee).

11. Controlled Substance. A drug or other substance, or their immediate precursors, included in schedule I, II, III, IV, or V of part B of 21 USC 802. This does not include distilled spirits, wine, malt beverages, or tobacco, as defined or used in subtitle E of the Internal Revenue Code of 1986.

12. Covered Individual.

    a. A person who performs work for or on behalf of the executive branch who has been granted access to classified information or holds a sensitive position; but does not include the President or (except to the extent otherwise directed by the President) employees of the President under 3 U.S.C. 105 or 107, the Vice President, or (except to the extent otherwise directed by the Vice President) employees of the Vice President under 3 U.S.C. 106 or annual legislative branch appropriations acts.

    b. A person who performs work for or on behalf of a state, local, tribal, or private sector entity, as defined in EO 13549, who has been granted access to classified information, but does not include duly elected or appointed governors of a state or territory, or an official who has succeeded to that office under applicable law.

    c. A person working in or for the legislative or judicial branches who has been granted access to classified information and the investigation or determination was conducted by the executive branch, but does not include members of Congress, Justices of the Supreme Court, or Federal judges appointed by the President.

    d. Covered individuals are not limited to government employees and include all persons, not excluded under paragraphs (a), (b), or (c) of this definition, who have access to classified information or who hold sensitive positions, including, but not limited to, contractors, subcontractors, licensees, certificate holders, grantees, experts, consultants, and government employees.

13. Departmental Element. A first-tier organization at Headquarters and in the field. First-tier at Headquarters encompasses heads of the major Headquarters line programs, e.g., Program Secretarial Officers. First-level field element refers to first-level organizations located outside the Washington Metropolitan area and encompasses Operations Offices, Site Offices, Field Offices, and Regional Offices.

14. Director. Director, Office of Departmental Personnel Security.

15. Drug Test. An examination of biologic material to detect the presence of specific drugs and determine prior drug usage, carried out in accordance with procedures, protocols and

standards established at Title 10, Code of Federal Regulations, Part 707, Workplace Substance Abuse Programs at DOE Sites, or DOE O 343.1, *Federal Substance Abuse Testing Program*, current version, and other applicable DOE policies.

16. Dual Citizen. An individual who is a citizen of more than one country.

17. Federal Head of Departmental Element. The senior Federal official with cognizance over a Departmental Element, as identified in the most current edition of the Department's Executive Secretariat Style Guide.

18. Federal Site Manager. The senior Federal management official at any DOE facility.

19. Foreign Intelligence Entity. Known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.

20. Foreign National. Any person who is not a U.S. citizen.

21. Investigative Service Provider (ISP). A federal agency authorized to conduct investigations utilizing federal staff and/or contractor personnel.

22. Key Management Personnel. An entity's senior management official (SMO), facility security officer (FSO), Insider Threat Program Senior Official (ITPSO), and all other entity officials who either hold majority interest or stock in, or have direct or indirect authority to influence or decide issues affecting the management or operations of, the entity or classified contract performance.

23. Media. Any person, organization, or entity, other than Federal, state, local, tribal, and territorial governments who are:

    a. Primarily engaged in the collection, production, or dissemination of information in any form, which includes print, broadcast, film, and Internet to the public; or

    b. Otherwise engaged in the collection, production, or dissemination of information to the public in any form related to topics of national security, which includes print, broadcast, film, and Internet.

24. National Security. Those activities directly concerned with the foreign relations of the U.S. or protection of the nation from internal subversion, foreign aggression, or terrorism.

25. National Security Eligibility. Eligibility (after background investigation was completed and adjudicated) for access to classified information or eligibility to hold a sensitive position, to include access to sensitive compartmented information, restricted data, and controlled or special access program information.

26. Need-to-Know. A determination made by a possessor of classified information or SNM that a prospective recipient, in the interest of national security, has a requirement for

access to, knowledge of, or possession of the classified information or SNM to perform tasks or services essential to the fulfillment of an official U.S. Government program.

27. Non-U.S. Citizen. A person without U.S. citizenship or nationality (may include a stateless person). This term is synonymous with "alien" as defined in section 101(a)(3) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(3)).

28. Program Secretarial Officer. The Federal head of a major DOE Headquarters line program, as identified in the most current edition of the Department's Executive Secretariat Style Guide.

29. Reasonably Exhaustive Efforts. The appropriate level of effort to resolve issues or corroborate discrepant information. This may include multiple attempts or techniques to satisfy the issue, attempts to corroborate the activity through references from the background investigation, and/or attempts to obtain and pursue additional leads through other aspects of the investigation.

30. Security Clearance. An administrative determination that an individual is eligible for access to classified matter and/or SNM. DOE grants Q and L clearances to individuals who require access to RD information at a classification level equal to or less than their security clearance level. DOE also grants Top Secret, Secret, or Confidential clearances to individuals approved for access to National Security Information or Formerly Restricted Data at classification levels equal to or less than their security clearance level.

31. Sensitive Position. Any position within or in support of an agency in which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on national security regardless of whether the occupant has access to classified information and regardless of whether the occupant is an employee, military service member, or contractor.

32. Unauthorized Disclosure. A communication or physical transfer of classified information to include Special Nuclear Material to an unauthorized recipient.