

**ORDER**

**DOE O 472.2**

Approved: 7-21-2011

# **PERSONNEL SECURITY**

---



**U.S. DEPARTMENT OF ENERGY**  
**Office of Departmental Personnel Security**



## **PERSONNEL SECURITY**

---

1. **PURPOSE.** To establish requirements that will enable the Department of Energy (DOE) to operate a successful, efficient and cost-effective personnel security program that will ensure accurate, timely and equitable determinations of individuals' eligibility for access to classified information and Special Nuclear Material (SNM).
  - a. This DOE Order sets forth requirements for personnel security program management and work practices that will ensure DOE's missions are accomplished in a secure environment by men and women in whom both the Department and the American people may 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. **CANCELLATION.** DOE M 470.4-5, *Personnel Security*, dated 8-26-05, DOE N 470.4, *Reciprocal Recognition of Existing Security Clearances/Access Authorizations*, dated 1-9-09, and DOE N 470.5, *Implementation of Section 1072 of the National Defense Authorization Act for Fiscal Year 2008*, dated 8-12-09. 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contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.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 that are engaged at any level in the processing of 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 Order. Nothing in this Order 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 will apply to contracts that include the CRD. All site/facility management contracts that involve classified information or SNM must include this CRD and DOE Acquisition Regulation (DEAR) clause 952.204-2, *Security Requirements*.
- c. 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 through 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. An access authorization is an administrative determination that an individual is eligible for access to particular types or categories of classified information or material. Unless otherwise indicated, the term “security clearance” encompasses access authorizations throughout this Order.
- (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, consultants and access permittees (see 10 CFR 725 for further information on DOE’s access permittee program).
- (3) No individual will be provided access to classified information or SNM unless that individual has been granted the appropriate security clearance and possesses a need-to-know. 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.
- (4) With the few exceptions noted in this Order and provided for in Executive Order 12968, section 3.3, individuals must not be afforded access to classified information or SNM until they have been granted a security clearance in accordance with the procedures in this Order.
- (5) Security clearances will not be processed in any manner 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 persons without security clearances within a controlled area. In certain instances, individuals who do not otherwise require access to classified information or SNM may be organizationally and/or physically situated such that they may inadvertently be exposed to classified information or SNM in the course of their duties. Site managers may require such individuals under their cognizance 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.

- (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.
- (6) Only individuals who are U.S. citizens and are at least 18 years of age may be processed for or granted a security clearance.
- (7) With the exception of circumstances described elsewhere in this Order, an individual's security clearance will be based on the review of investigative reports provided to DOE by the Office of Personnel Management (OPM), the Federal Bureau of Investigation (FBI), or other Federal agency authorized to conduct background investigations.
- (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 will be subject to appropriate disciplinary action.

b. Security Clearance and Access Authorization Types.

- (1) 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), Special Nuclear Material (SNM) or Sensitive Compartmented Information (SCI).
- (2) This section describes those security clearances and access authorizations which are processed by DOE cognizant personnel security offices (CPSOs). Other access determinations made by DOE appear in Attachment 2.
- (3) Security Clearances:
  - (a) Top Secret: A Top Secret security clearance is required for access to NSI, as defined by Executive Order 13526, classified at the Top Secret level and FRD (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 and FRD classified at the Secret and Confidential levels.
  - (b) Secret: A Secret security clearance is required for access to NSI and FRD classified at the Secret level. A Secret security clearance also permits access to NSI and FRD classified at the Confidential level.
  - (c) Confidential: A Confidential security clearance is required for access to NSI and FRD classified at the Confidential level.
- (4) Access Authorizations:
  - (a) Q: A Q access authorization is required for access to:
    - 1 RD, as defined by the AEA, classified at the Top Secret or Secret level.
    - 2 SNM, as defined by the AEA, designated as Category I and other categories with credible roll-up to Category I.
    - 3 A Q access authorization permits access to information and material described below for L access authorizations.
  - (b) L: An L access authorization is required for access to RD classified at the Confidential 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. Access to SNM designated as

Category IV does not require an access authorization unless a site vulnerability assessment, documented in associated site security plans, establishes such a need in order to minimize risk.

- (c) QX and LX: QX and LX access authorizations are granted to individuals employed by DOE access permittees. QX is required for access to Secret RD and LX is required for access to Confidential RD. Information regarding the DOE access permit program is found at 10 CFR 725.
- (5) Q and L access authorizations permit access to information listed under Top Secret and Secret security clearances, respectively.
- (6) Background investigative requirements for all security clearances are mandated by national standards.
- c. Central Personnel Clearance Index (CPCI). DOE personnel security staff must use the personnel security automated information system, the CPCI, for recording all security clearance actions. Unless otherwise indicated, all actions must be entered into CPCI within 48 hours of occurrence. Additional information and specific access requirements for the use of CPCI are set forth in the *WebCPCI User's Guide* that is available to all persons authorized to access the system.
- d. Contractors. Contractor applicants and employees will be processed for security clearances in the same manner as Federal applicants and employees except for such additional requirements or considerations which may be imposed by DOE M 470.4-1 Chg 2, *Safeguards and Security Program Planning and Management*, or any successor directive, and by the National Industrial Security Program Operating Manual (NISPOM). For additional information, see Attachment 1.
- e. Reciprocity.
  - (1) Individuals requiring a security clearance at DOE who have been determined to be currently eligible for access to classified information by another Federal agency or are in possession of a valid security clearance issued by another Federal agency must have an appropriate DOE security clearance reciprocally issued (see exceptions in Appendix B) without the conduct of any investigative or adjudicative work by DOE. The CPSO must use available automated databases to verify current security clearances and eligibility determinations. In circumstances where the CPSO is unable to verify a security clearance or eligibility for access to classified information electronically, the CPSO will request verification of the security clearance or access eligibility directly from the adjudicating agency.

- (2) The prohibition against conducting investigative or adjudicative work on individuals with valid security clearances or eligibility determinations includes the review of previously conducted background investigations or adjudicative actions taken by other Federal agencies. This information may be requested to construct the individual's DOE personnel security file (PSF), but only after the reciprocal security clearance has been issued by the CPSO.
  - (3) Existing Top Secret security clearances/eligibility determinations will be accepted as the basis for reciprocal Q access authorizations and existing Secret security clearances/eligibility determinations will be accepted as the basis for L access authorizations.
  - (4) Refer to Appendix B for additional information regarding reciprocity.
- f. Reinstatements. Individuals who no longer possess a security clearance may have a security clearance reinstated when a valid justification for access to classified information or SNM has been received by the CPSO and the previously-held security clearance was terminated for administrative, non-prejudicial reasons.
- (1) An individual who formerly held a DOE security clearance must have a security clearance reinstated at the previous or lower level if the individual meets the following criteria.
    - (a) The individual has remained employed by or under contract to (to include multiple, consecutive contracts) DOE since the prior security clearance was terminated.
    - (b) The individual certifies on a Standard Form 86 Certification (SF 86C) or updated SF 86 that there has been no change to adjudicatively relevant information provided at the time of the individual's last background investigation.
    - (c) The CPSO reviews the completed form and determines it to be free of any issues of security concern not previously disclosed and adjudicated.
    - (d) The CPSO is not already in possession of information regarding the individual which would tend to indicate the individual may no longer satisfy the requirements of eligibility for a security clearance.
    - (e) The required supporting background investigation is no older than five years regardless of the level of the currently-required security clearance. Where the background investigation is more than five years old, all information and items required for processing a

security clearance request (see paragraph 4.1. of this Order and Attachment 2, paragraphs 1 and 2) must be obtained by the CPSO. If the information received is favorable, the requested security clearance must be granted once the required reinvestigation has been initiated. If information received reveals derogatory information, or if the supporting background investigation is more than 10 years old, the requested security clearance will be processed in accordance with the procedures for processing security clearance requests set forth elsewhere in this Order.

- (2) An individual who left employment in which a security clearance was held less than 24 months ago must have a security clearance reinstated at the previous or lower level if the individual meets the following criteria.
  - (a) The individual certifies on a Standard Form 86 Certification (SF 86C) or updated SF 86 that there has been no change to adjudicatively-relevant information the individual provided at the time of his/her last background investigation.
  - (b) The CPSO reviews the completed form and determines it to be free of any issues of security concern.
  - (c) The CPSO conducts a check of the national level personnel security databases (i.e. the Clearance Verification System, etc.) and no issues of a security concern are revealed.
  - (d) The CPSO is not already in possession of information regarding the individual which would tend to indicate the individual may no longer satisfy the requirements of eligibility for a security clearance.
  - (e) The required supporting background investigation is no older than five years regardless of the level of the currently-required security clearance. Where the background investigation is more than five years old, all information and items required for processing a security clearance request (see paragraph 4.n. of this Order and Attachment 2, paragraphs 1 and 2) must be obtained by the CPSO. If the information received is favorable, the requested security clearance must be granted once the required reinvestigation has been initiated. If information received reveals derogatory information, or if the supporting background investigation is more than 10 years old, the necessary security clearance will be processed in accordance with the procedures for processing security clearance requests set forth elsewhere in this Order.
- (3) Individuals who fall outside the parameters of this section because of the age of their last background investigation or their length of separation

(e.g. retired DOE Federal or contractor employees) will 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 Site Manager may make a request, in writing, that these procedures be modified. The Site Manager must direct the CPSO to forward such requests to the Director, Office of Departmental Personnel Security (Director). The Director may, at his or her discretion, prescribe modified procedures for the granting of the security clearance, provided:

- (a) The individual held a security clearance commensurate with the level and category of the classified information or SNM to which access is now required, and
  - (b) The security clearance will be terminated by the CPSO when the need for access has expired, but in no case will the security clearance exceed 30 days' duration. Such clearances needed for longer than 30 days must be processed as applicant security clearance requests in accordance with the procedures set forth elsewhere in this Order.
- g. Classified Visits. Individuals requiring access to classified information or SNM will be processed for such access in accordance with the procedures prescribed in DOE M 470.4-1 Chg 2.
- h. Access by Persons Outside the Executive Branch.
  - (1) Attorneys and other individuals taking part in legal or administrative proceedings under the jurisdiction of DOE who will require access to classified information must be processed for a security clearance in accordance with requirements set forth in this Order. Certification is required by the Office of the General Counsel or the appropriate CPSO's Chief Counsel's Office 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 as possessing QB security clearances. Such CPCI entries will be created when the first

need for actual access arises, and will be coordinated between the Office of Headquarters Personnel Security and the appropriate CPSO. QB security clearances will not be submitted for inclusion in any database other than CPCI.

- (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 non-disclosure agreement applicable to all DOE Federal and contractor employees, and
  - (b) The Department must not be in possession of information suggesting that such access may not be in the best interests of the national security. If the Department is in possession of such information, the Director will be consulted prior to the issuance of the QB security clearance.
- (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 security clearance in accordance with the procedures set forth in this Order.

i. 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 non-U.S. citizens are not employed in duties that may 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. citizen possesses 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 will not be eligible for access to any greater level of classified information or material than the U.S. Government has determined may be releasable to the country of which the individual is currently a citizen. The DOE Office of the General Counsel will be consulted by the Director for this assessment. Such limited access may be approved only if a background investigation, of a type and scope prescribed by Executive Order 12968, or any successor national-level directive, 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.
- j. Temporary Security Clearance Upgrades.
  - (1) Circumstances may arise in which an urgent operational exigency exists requiring cleared DOE personnel to have one-time or short duration access to classified information or SNM at a higher level than is authorized by their existing security clearance. In some instances, the processing time required to upgrade the security clearance would prevent timely access to the information, adversely impacting mission needs.
  - (2) In such situations and only for compelling reasons in furtherance of the DOE mission, the Site Manager must certify the need for the temporary security clearance upgrade in writing and submit it to the appropriate CPSO. The CPSO will grant or deny the required security clearance in accordance with procedures set forth in Attachment 3.
- k. Interim Security Clearance Determinations (Interims). Under exceptional circumstances and when such action is clearly consistent with Departmental and national interests, an uncleared individual may, pending completion of the appropriate background investigation, be permitted to have an interim security clearance. Interims must be considered temporary measures pending completion of the investigation, which must be in process when the interim is granted. See Attachment 3 for additional information regarding interims.
- l. Processing Security Clearances.
  - (1) Requests for security clearances must be justified and submitted to the appropriate CPSO in accordance with established local procedures. CPSOs will have in place written procedures for submission and acceptance of security clearance requests.
  - (2) Security clearances will only be processed after the CPSO has received an appropriate written request. Security clearance cases, including those to be processed by the FBI (see Appendix A), will include completion of a Standard Form 86, *Questionnaire for National Security Positions*, utilizing OPM's Electronic Questionnaire for Investigations Processing (e-QIP) system. E-QIP 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 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) E-QIP submissions to the investigative service provider must be approved by a Federal employee.
  - (4) Data collected in the course of processing a security clearance request will contain personally identifiable information (PII). Loss or compromise of PII must be reported in accordance with DOE O 206.1, *Department of Energy Privacy Program*, dated 1-16-09, or any successor directive.
- m. Cancellation of Investigative Requests. A CPSO must immediately request the investigating agency to discontinue an ongoing investigation if information is received indicating the individual no longer requires a security clearance. If a security clearance request no longer needs to be processed at one CPSO because the individual is transferring to a location under the cognizance of another CPSO and that individual will still require a security clearance at the gaining CPSO, the losing CPSO must not discontinue the investigation. In such situations, the CPSOs must work together to ensure that the completed investigative report is received by the gaining CPSO.
- n. 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 investigative standards have been met, as appropriate for the level of security clearance being considered. The CPSO will 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 determine an individual's security clearance eligibility or render other formal determinations that affect an individual's security clearance status. A program of quality oversight, training and testing has been established for this purpose. Refer to Appendix C for more information on this program. Employees may begin assisting in determinations once their training regimen has begun. Rendering final determinations is an inherently governmental function. Contractor support staff may assist by performing actions in support of the security clearance and adjudication processes. This requirement does not preclude a contractor from having an employee execute a DOE F 5631.29, *Security Termination Statement* or restricting an individual's access to classified information or SNM before notifying the DOE.

- (4) All individuals' initial and continued eligibility for security clearances will be adjudged against the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Guidelines), as promulgated in accordance with Executive Order 12968, or successor national directives, and relevant Departmental requirements.
- (5) Where the CPSO has no information related to any of the areas of concern identified in the Guidelines, either from the report of investigation or from other sources, a favorable determination must be made.
- (6) Where the CPSO has information related to any areas of concern identified in the 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.
- (7) If questions as to the individual's security clearance eligibility can be favorably resolved in accordance with the processes and considerations set forth in the Guidelines, the appropriate security clearance must be granted or continued.
- (8) When 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) Conduct a personnel security interview (PSI). Only persons appropriately trained in DOE personnel security interviewing techniques and cognizant of all the questions or items of information to be explored are authorized to conduct such interviews. DOE F 5631.5, *The Conduct of Personnel Security Interviews under DOE Security Regulation*, and DOE F 5631.7, *Privacy Act Statement for Personnel Security Interviews and Related Release Forms*, must be properly executed for all PSIs. All PSIs must be recorded in audio or audio/video format and retained in the PSF. PSIs may be transcribed, at the discretion of the CPSO, to meet Privacy Act requests or if determined necessary to support additional adjudication actions (mental health evaluation, due process under administrative review, etc.).
  - (b) 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.
  - (c) Authorize a DOE-sponsored mental health evaluation.

- (d) Request the assistance of other CPSOs in different geographical locations to conduct a PSI or to obtain additional information. Assisting CPSOs must manage such requests in as timely a manner as possible.
  - (e) Request a polygraph examination of the individual in accordance with the provisions of 10 CFR 709, *Counterintelligence Evaluation Regulations*. Such requests must be routed through and receive the approval of the Headquarters Office of Intelligence and Counterintelligence.
  - (f) Consult with the cognizant counterintelligence office where questions as to the individual's loyalty, allegiance, foreign connections or unexplained affluence arise.
  - (g) Obtain a personal financial statement.
  - (h) Institute administrative review procedures, to include the suspension of an active security clearance, per 10 CFR 710.
- (9) If, in the opinion of the CPSO, the additional investigative and/or follow-up activities have adequately resolved the pertinent questions as to the individual's security clearance eligibility, the appropriate security clearance must be granted.
- (10) When these actions [excluding (h)] fail to favorably resolve the pertinent questions, the CPSO will initiate the Administrative Review procedures set forth at 10 CFR 710.
- o. Reinvestigations.
- (1) An investigation for cause may be initiated at any time if the CPSO learns of information related to any areas of concern set forth in the Guidelines. Such information may be resolved by the CPSO internally through a Letter of Interrogatory, a personnel security interview, a mental health evaluation, or other actions. Alternatively, an investigation for cause through the appropriate investigative agency may be conducted. The precise scope of such an investigation will depend upon the issues involved.
  - (2) Individuals with security clearances must be reinvestigated at intervals determined by national standards and promulgated via national level directives. Reinvestigations are designed to ensure that individuals with security clearances are routinely reevaluated to determine their continued need and eligibility for security clearances.

- (3) Reinvestigations should be submitted to the investigative agency at a regular frequency throughout the year, budgetary and other circumstances permitting.
- p. Intra-Agency Security Clearance Actions.
- (1) A security clearance issued by any CPSO will be considered to be a Departmental security clearance and will be recognized universally throughout the Department. Individuals in possession of a current DOE security clearance 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 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 office will annotate CPCI 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 with regard to the individual's security clearance, the information concerning shared access which has been recorded in 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 and for all other related matters will reside with the CPSO that granted the security clearance.
    - (b) 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 the CPSO holding the highest level of shared access.
  - (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 will be followed:
    - (a) If the individual requires access at the same security clearance level in the new position, his/her PSF will be forwarded to the gaining CPSO.
    - (b) If the individual requires a higher level security clearance in the new position, his/her PSF will be forwarded to the gaining CPSO

and procedures for requesting and granting security clearances, as set forth in this Order, must be followed.

- (c) If the individual will not require a security clearance in the new position, the individual must be given a termination briefing and execute a DOE F 5631.29. This process must be facilitated by the losing CPSO prior to reassignment or transfer.
  - (d) If the individual will require a lower level security clearance in the new position, his/her PSF will be forwarded to the gaining CPSO and the gaining CPSO will be responsible for downgrading the individual's security clearance to the appropriate level.
  - (e) The losing CPSO is responsible for completing any pending adjudicative actions prior to forwarding the PSF to the gaining CPSO, except where the gaining CPSO explicitly agrees to accept such responsibility.
- (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.

q. Administrative Withdrawal of Security Clearances.

- (1) In all instances, security clearances must be administratively withdrawn when there is termination of employment or a change of official duties such that the individual no longer requires access to classified information or SNM.
- (2) Where an individual's circumstances will temporarily eliminate the need for access to classified information or SNM for 90 calendar days or more (temporary change of duties, maternity or other extended leave [including leave covered under the Family Medical Leave Act], detail to another agency, military deployment, etc.), the individual's security clearance must be administratively withdrawn. The CPSO may elect to waive this requirement should the details of a particular case indicate such action would be in the interest of the Department. Such decisions, along with supporting specific details, will be documented in the PSF. Where such a security clearance has been retained, it is still subject to reinvestigation at the appropriate interval. However, if the individual is unavailable or cannot be located for investigative purposes (i.e., in case of military deployment) the security clearance will be administratively withdrawn and will be subject to reinvestigation upon the return of the individual.
- (3) When a security clearance is administratively withdrawn in accordance with the conditions set forth above, a completed DOE F 5631.29 must be

obtained from the individual within two (2) working days. 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.

- (4) Within two working days of receipt of a DOE F 5631.29 or written notice of administrative withdrawal, the CPSO must note the date the clearance was actually withdrawn in the individual's PSF and CPCI, and must notify any other CPSO's with shared access interests. Possession of the DOE F 5631.29 by the CPSO is not needed to effect an administrative withdrawal action.
  - (5) In all cases, administrative withdrawals are non-prejudicial, and do not entitle the individual to any of the due process procedures of 10 CFR 710. Should a security clearance be administratively withdrawn in accordance with guidance contained in this Order while there is unresolved derogatory information or adverse security clearance action(s) pending against the individual, this fact must be recorded by the CPSO in the individual's PSF and CPCI.
  - (6) Additional debriefing requirements may be found in DOE M 470.4-1 Chg 2.
- r. 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 at 10 CFR 710.
- s. Actions by the Secretary. Nothing in this Order will be construed to limit the Secretary's authorities and responsibilities under Executive Order 12968 (section 1.2(b), et al.), Executive Order 10865 (section 9), 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.
- t. Personnel Security Files.
- (1) Personnel security information and PSFs contain PII. Personnel security information and PSFs must be controlled in accordance with the Privacy Act of 1974, as amended, DOE Systems of Records Notice 43, *Personnel Security Files*, DOE Administrative Records Schedule 18, DOE O 243.1, *Records Management Program*, dated 02-06-06 (or any successor directive) and the requirements of the investigative agency or other entities whose records may be contained in the PSF. PSFs must not be released to representatives of DOE contractors (except those contractor employees engaged in support of the DOE personnel security

program). Detailed information concerning the organization of DOE PSFs and restrictions on their dissemination appear in Appendix D.

- (2) Loss or other problems involving a PSF that may involve a compromise of PII must be reported in accordance with DOE O 206.1. Unclassified PSFs must be transmitted in keeping with guidance provided in DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, dated 04-09-03. A record of all transfers must be kept in the PSF and in CPCI to ensure the current location of PSFs is maintained. Classified PSFs must be transmitted in accordance with guidance set forth in DOE M 470.4-4A Chg 1, *Information Security*, dated 10-12-10, or any successor directive.
- (3) PSFs 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 wish to review, amend or obtain a copy of the contents of their PSFs. 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 DOE Privacy Act Officer. Under no circumstances will individuals be given access to investigative reports from their PSF without prior, written approval of the originating agency. Absent such approval, individuals requesting access to these reports must be referred to the originating agency. PSFs and the associated information in CPCI or any other DOE database must be retained in accordance with National Archives and Records Administration (NARA)/DOE Records Schedule 18. Reports of investigation provided by other agencies will be retained as part of the PSF 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 DOE PSFs and CPCI accordingly.
- (4) PSFs that no longer need to be retained pursuant to this Order must be destroyed in accordance with guidance set forth in DOE M 471.3-1 or DOE M 470.4-4A Chg 1, as applicable.

u. Reporting Responsibilities and 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) Such matters (see Attachment 4) must be reported verbally and directly to the CPSO immediately upon the individual becoming aware of the situation or incident and in no event later than two (2) working days after the event. Thereafter, written confirmation of the information must be provided by the individual to the CPSO within three (3) additional working days.
- (3) All individuals must make a report to the CPSO whenever they learn of the presence of any such situations or incidents with regard to 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 two (2) working days after the event. Thereafter, written confirmation of the information must be provided by the individual to the CPSO within three (3) additional working days. Individuals making such reports regarding other persons must be aware that they may be asked by the CPSO to provide additional, corroborative information.
- (4) Federal management officials must notify within two (2) working days, followed by written confirmation within the next ten (10) working days, the CPSO of conditions affecting the status of an applicant's or employee's security clearance (e.g., death, employment termination, change in need for access to classified information or SNM).
- (5) All individuals must provide full, frank, and truthful answers to relevant and material questions.
- (6) When requested, all individuals must furnish, and authorize others to furnish if necessary, information that DOE deems pertinent to the security clearance eligibility process.
- (7) These responsibilities apply when completing security forms, during the course of all personnel security investigations and at any stage of the security clearance process including, but not limited to, letters of interrogatory, personnel security interviews, DOE-sponsored mental health evaluations and other authorized investigative activities.
- (8) 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 terminated or, for applicants, further processing of a security clearance request may be terminated. 10 CFR 710 sets forth the processes by which such actions will occur.
- (9) Security clearance applicants and holders must provide a completed DOE F 5631.34, *Data Report on Spouse/Cohabitant*, directly to the CPSO within forty-five (45) working days of marriage or cohabitation. NOTE: A cohabitant is a person who lives with the individual in a

spouse-like relationship or with a similar bond of affection or obligation but is not the individual's legal spouse, child, or other relative (in-laws, mother, father, brother, sister, etc.). A national agency check and other indices checks as may be warranted by national investigative standards will be requested on spouses and cohabitants. Security clearance applicants and holders who are approached by an individual seeking unauthorized access to classified information or SNM or who experience any other potentially counterintelligence-related incidents, must report this information in accordance with DOE O 475.1, *Counterintelligence Program*, dated 12-10-04, or any successor directive.

- (10) All cleared DOE employees must also report foreign travel in accordance with DOE O 475.1.
  - (11) CPSOs are responsible for ensuring that security clearance applicants and holders under their cognizance are made aware of the foregoing reporting responsibilities.
  - (12) Individuals with active security clearances will be initially briefed and annually briefed regarding their personnel security responsibilities as required by DOE M 470.4-1 Chg 2.
- v. 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, with the servicing personnel offices for the DOE employees under their jurisdiction, procedures for the referral of such information so the servicing personnel office can 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.

## 5. RESPONSIBILITIES.

- a. Program Secretarial Officers. Approve requests to process non-U.S. citizens for Limited Access Authorizations.
- b. Federal Heads of Departmental Elements.
  - (1) Ensure that the requirements associated with determining the level of security clearance required and the means through which to request a

security clearance are communicated to and implemented by the appropriate offices, individuals and contracting/procurement officials under their cognizance.

- (2) Determine whether and when an interim security clearance 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. 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, nevertheless are situated such that inadvertent exposure cannot otherwise be reasonably prevented.
- (3) Determine whether and when to approve requests for temporary security clearance upgrades.
- (4) With the concurrence of the Director, Office of Departmental Personnel Security, determine whether and when to modify procedures for reinstating security clearances.
- (5) Communicate to all cleared DOE personnel under their cognizance their personal responsibilities with regard to holding a DOE security clearance. Such individuals are thereafter responsible for adhering to these responsibilities.

d. Contracting and Procurement Officials must 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 will provide necessary guidance, direction, clarification and assistance so that the requirements of this Order may be implemented correctly and consistently.

f. Cognizant Personnel Security Offices will ensure that the requirements of this Order are implemented in accordance with direction provided in this Order and by the Office of Departmental Personnel Security.

- g. Office of the General Counsel/Site Offices of Chief Counsel will provide notification to the CPSO when access to classified information is required by outside attorneys in proceedings involving the Department. The Office of the General Counsel will be consulted in determining what level of classified information is releasable by the United States government to specified foreign countries in support of Limited Access Authorizations.

6. REFERENCES.

- a. DOE O 243.1, *Records Management Program*, dated 02-02-06.
- b. Executive Order 13549, *Classified National Security Information Program for State, Local, Tribal and Private Sector Entities*, 08-18-10.
- c. Additional references may be found at the DOE Health, Safety and Security Policy Information Resources link at the Office of Departmental Personnel Security's web site.

7. DEFINITIONS.

- a. Cognizant Personnel Security Office (CPSO). A Federal personnel security office that is authorized to submit investigative requests to investigative service providers and to adjudicate security clearances.
- b. Site Manager. The senior Federal management official at any DOE facility with a CPSO.
- c. Classified Information. Any information that has been determined pursuant to Executive Order 13526, or successor Orders, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and that is so designated.
- d. Director. Director, Office of Departmental Personnel Security.
- e. 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.
- f. 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.
- g. 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 in order to perform tasks or services essential to the fulfillment of an official United States Government program.

- h. Additional definitions may be found at the DOE Health, Safety and Security Policy Information Resources link at the Office of Departmental Personnel Security's web site
8. CONTACT. Questions concerning this Order should be addressed to the Office of Health, Safety and Security, Office of Departmental Personnel Security, at 202-586-3249.

BY ORDER OF THE SECRETARY OF ENERGY:



DANIEL B. PONEMAN  
Deputy Secretary

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

Per section 145 e. 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 Office of Personnel Management (OPM).

Additionally, per section 145 f. of the AEA, the Department 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 RECIPROCITY**

1. The Cognizant Personnel Security Office (CPSO) must initiate a reinvestigation immediately *after* granting a reciprocal security clearance if the supporting investigation is between 4.5 and 7 years old for Q and Top Secret security clearances, 9.5 and 10 years old for L and Secret security clearances and 14.5 and 15 years old for Confidential security clearances.
2. The “Checklist of Permitted Exceptions to Reciprocity” (available at the Office of Departmental Personnel Security web site), or any successor national-level work-aid must be completed in all cases in which a security clearance based upon reciprocity is considered.
  - a. The checklist details conditions under which agencies are not bound to reciprocally grant a security clearance where the appropriate investigative conditions have otherwise been met.
  - b. If the answer to any question on the checklist is affirmative, processing of the security clearance request under reciprocity procedures must be discontinued and the request for security clearance will be handled in accordance with the appropriate provisions set forth in this Order. The completed checklist must be maintained in the individual’s personnel security folder (PSF), affixed to the right side along with other adjudicative and investigative materials (see Appendix D).
  - c. Individuals or offices submitting requests for security clearances must notify the CPSO if they have reason to believe that the individual has been deemed eligible for access to classified information by another agency or holds a security clearance granted by another agency. If the CPSO is unable to verify the existence of such eligibility or a security clearance, in accordance with procedures set forth in paragraph 4.e.(1) of this Order, the security clearance request will be processed in accordance with the appropriate provisions set forth in paragraph 4l. of this Order.
3. Other Considerations: Access to special programs or information (see Attachment 2) is generally not subject to reciprocity or other considerations, and may be reviewed to ensure eligibility in accordance with the requirements for the specific program.



## **APPENDIX C PERSONNEL SECURITY QUALITY AND TRAINING**

1. GENERAL. Quality and training are both essential to the success of the DOE personnel security program. This Appendix 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. It is incumbent upon the individual CPSOs to plan and budget for any costs associated with peer reviews and personnel security training, as described in this Appendix.
  
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 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. Managers 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 414.1C, *Quality Assurance*, dated 06-17-05, or any successor directive.
  
  - c. The Office of Independent Oversight and the Office of the Inspector General are responsible for assessing the personnel security processes within the Department to ensure their compliance with national and Departmental policy.
  
  - d. The Office of Departmental Personnel Security provides policy oversight for the personnel security program, to include enhancing program quality through:
    - (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) Managing the Personnel Security Peer Review Program (PSPRP). The PSPRP involves adjudicators from one or two CPSOs visiting a third CPSO to review a small percentage of randomly-sampled adjudicative decisions that have previously been made by the third CPSO's adjudicative staff. The primary objective of the visits is to determine if the security clearance decisions made by DOE adjudicators are consistent with the national adjudicative standards. In addition, such visits allow for peer exposure to other CPSO operations and the sharing of best practices and lessons learned among the participating CPSO representatives. These visits are informal, collaborative snapshots of each CPSO's adjudicative processes and procedures, and are not a replacement for or affiliated with the formal inspections of the Department of Energy Personnel Security Program conducted by the Office of Independent Oversight or the Office of Inspector General. The Office of Departmental Personnel Security will share crosscutting issues with the personnel security community and will independently work with and provide assistance to the manager(s) and staffs of the reviewed CPSOs to improve any areas in which significant challenges are present, and conduct program staff assistance visits at the CPSOs, as deemed appropriate.

3. TRAINING. DOE Federal employees must receive personnel security training in accordance with their duties and levels of responsibility in order 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 this Order and NTC requirements.

- 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 cleared DOE employees, adjudicators, adjudicative support staff and other key officials.
  - (1) Cleared DOE employees must be informed of their personnel security responsibilities as part of the safeguards and security awareness process outlined in DOE M 470.4-1 Chg 2. Such training will be included in all comprehensive orientation briefings provided to employees upon receipt of security clearances and before receiving initial access to classified information or SNM.
  - (2) Adjudicator Training (specifics regarding sequential course titles and order will be determined by current NTC course guidelines).
    - (a) Initial Training. All newly appointed personnel security specialists performing adjudicative duties have two years to complete the NTC personnel security training suite.
    - (b) Continuing Education. On an annual basis, personnel security specialists performing adjudicative duties are required to take the NTC's annual personnel security refresher training. New adjudicators who have not completed the first two courses of the NTC's personnel security training suite are not required to complete the annual refresher course unless local management deems it appropriate. This online refresher course is revised annually to provide personnel security specialists with updates on trends, policies and procedures.
    - (c) Adjudicative personnel are prohibited from making security clearance determinations until they have at least completed the initial course of the NTC's personnel security training suite and have received adequate initial on-the-job training, as determined by the CPSO. In addition, adjudicative personnel are prohibited from conducting second or third tier reviews and making final security clearance determinations until they have at least completed the first 3 courses of the NTC's personnel security training suite and have received adequate advanced on-the-job training, as determined by the CPSO.
    - (d) Adjudicative Support Training. Employees who are involved in the initial screening of cases, but do not conduct interviews or perform

second or third tier reviews (e.g., security assistants, screeners) need a basic understanding of the DOE personnel security process in order to perform their duties effectively. All personnel performing adjudicative support functions have one year from their date of appointment to complete the first course and should also complete the second course of the NTC's personnel security training suite in order to ensure their familiarity with the adjudicative process.

- (3) Key Officials. Other employees involved in the personnel security process 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 Title 10, Code of Federal Regulations, Part 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. On an annual basis, the Office of Departmental Personnel Security reminds senior managers to identify employees who have been placed into key official positions since the last briefing notification and ensure that those newly-assigned key officials complete the awareness briefing.

## **APPENDIX D PERSONNEL SECURITY FILES**

### **1. SAFEGUARDING.**

- a. The Privacy Act of 1974 [5 U.S.C. 552a(b)(1)] sets forth strict safeguarding requirements for Federal records relating to individuals, to include training, rules of conduct and other requirements for persons whose duties involve maintaining such records. It also establishes penalties for violations of these requirements. Additionally, data contained in PSFs will include a significant amount of PII. Loss or compromise of PII must be reported in accordance with DOE O 206.1. Per OPM requirements, because of the privileged nature of the information contained in PSFs, those files may 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, 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;
  - (6) Ensure compliance with DOE requirements, or
  - (7) Conduct mental health evaluations at the request of DOE personnel security staff which may tend to impact an individual's eligibility for a security clearance (does not apply to HRP-related mental health evaluations).
- b. Maintenance, storage and control of PSFs (both active and terminated files) is the responsibility of CPSOs, and may not be delegated or otherwise assigned to local or contractor security offices.
- 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 persons must show that they have an official purpose for reviewing the investigation. With the one exception noted below in paragraph 1.d., such individuals must not be given copies of an investigation conducted by another Federal agency. 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.

- d. Representatives from the Office of Intelligence and Counterintelligence (IN) may, in support of official IN evaluations and inquiries, be provided copies of OPM and/or FBI investigative reports when requested. The investigative reports cannot be maintained once a disposition of the IN case is reached. Investigative reports must not be re-disseminated by IN to other organizations (to include law enforcement agencies, other Federal agencies, or other DOE offices). Any requests for re-dissemination must be referred to the Office of Departmental Personnel Security.
- e. Pursuant to the Privacy Act of 1974, [5 U.S.C. 552a(b)(7)], 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 that is desired, and the justification for seeking such information.
- f. A record of each disclosure made in accordance with the preceding paragraphs (with the exception of disclosures made within CPSOs amongst staff for purposes related to routine security clearance processing) must be recorded in the PSF, 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,
  - (5) Whether and what documents were copied and provided, and
  - (6) The name and position of the person releasing the information.
- g. In all instances, before releasing classified information from a PSF 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.

## 2. CONTENTS AND ARRANGEMENT OF DATA IN PERSONNEL SECURITY FILES.

- a. A PSF must be maintained in paper or electronic form for each individual processed for a security clearance. The CPSO must assign a unique DOE case number to each file. The PSF number will always be used to identify the 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, will 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 fastened to the left side and adjudicative and investigative material is fastened to 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 interviews; security advisory letters; suspension correspondence, notification letters, and responses thereto; correspondence relating to special security clearances and access authorizations; security badge and briefing forms; and similar data. A 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, and security acknowledgment; reports of investigation from any Federal agency or local law enforcement activity, the Office of the Inspector General, or contractor security personnel; reciprocity checklists 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; interview transcripts or summaries; letters of interrogatory to the individual and responses thereto; 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 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 M 470.4-1.
  - (1) Information that must be included in all PSFs:
    - (a) File Summary Sheet (DOE F 5631.16) or equivalent record approved by the Office of Departmental Personnel Security
    - (b) Access Justification Form
    - (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 as necessary:
- (a) SF 86
  - (b) Copy of Birth Certificate
  - (c) Education Documentation
  - (d) Credit Reports
  - (e) OPM/FBI Investigative Results
  - (f) Fingerprint cards
  - (g) Other Government Agency Reports
  - (h) Special Access Documentation (e.g., SCI, HRP)
  - (i) Clearance Verification Forms (Reciprocity)
  - (j) Letter of Interrogatory and Response
  - (k) Controlled correspondence receipts (e.g., PS form 3811, *Domestic Return Receipt*)
  - (l) Request for Personnel Security Interview
  - (m) Results of Personnel Security Interview
  - (n) The Conduct of Personnel Security Interviews Under DOE Security Regulations (DOE F 5631.5)
  - (o) Privacy Act Statement for Personnel Security Interviews and Related Release Forms (DOE F 5631.7)
  - (p) Fair Credit Reporting Act Authorization (DOE F 472.1)
  - (q) Waiver (*Consent to Undergo a Mental Evaluation to be Conducted by a Psychiatrist or Licensed Clinical Psychologist*, DOE F 472.2)
  - (r) Psychiatric, psychological, or other mental health evaluations or reports
  - (s) Medical Documents
  - (t) Notification of Clearance Determination
  - (u) Clearance Extension Documentation
  - (v) Drug Certification (DOE F 5631.9)
  - (w) Requests for Polygraph

- (x) Polygraph Examination Report
  - (y) Name/marital status change
  - (z) Data Report on Spouse/Cohabitant (DOE F 5631.34)
  - (aa) Security Incident/Infraction /Issue Report Documentation
  - (bb) Foreign Travel Request
  - (cc) Counterintelligence Correspondence
  - (dd) Privacy Act Release Correspondence
  - (ee) Request for Reinvestigation
  - (ff) Statement of Charges
  - (gg) Administrative Review Documentation
  - (hh) Appeal Documentation
  - (ii) File Transfer Record (DOE F 5631.25)
  - (jj) Notes to File
  - (kk) Other miscellaneous documents that direct relate to the adjudicative process
- e. Electronic PSFs must be arranged in a manner which mirrors, to the extent practical, the contents and arrangement requirements for paper PSFs.



## APPENDIX E

### ADJUDICATIVE CONSIDERATIONS RELATED TO STATUTORY REQUIREMENTS AND DEPARTMENTAL REQUIREMENTS

1. Illegal use of controlled substances:
  - a. Security clearance applicants who are determined to have illegally used a controlled substance within 12 months of their SF 86 signature date through self-admission or a confirming drug test must have their security clearance process terminated with no appeal rights.
  - b. Security clearance applicants who are determined to have illegally used controlled substances within 12 months of their SF 86 signature date through self-admission, a confirming drug test or via other credible and convincing means after their background investigation has been opened by the investigative agency must have their security clearance process suspended, and may appeal this decision to the Director, in accordance with provisions of 10 CFR 710.
  - c. Where information with respect to the illegal use of controlled substances within 12 months of an applicant's SF 86 signature date surfaces via other means after the background investigation has been opened, and such evidence is neither credible and convincing nor capable of being favorably adjudicated, the applicant's case must be processed for administrative review in accordance with the provisions of 10 CFR 710.
2. Section 1072 of the National Defense Authorization Act for Fiscal Year 2008
  - a. This provision (commonly referred to as the Bond Amendment) identifies additional factors to be considered when rendering adjudicative determinations. In any case in which the Bond Amendment applies, as detailed below, all correspondence (notification letters, referral letters, etc.) must expressly indicate this fact.
    - (1) The Bond Amendment:
      - (a) Prohibits persons who are addicted to, or who are unlawful users of, controlled substances (as defined in section 102(1) of the *Controlled Substances Act* (21 U.S.C. 802) from holding any security clearance. Within DOE, cleared incumbents determined to have illegally used controlled substances within 12 months of the signature date on their SF 86 or within 12 months of DOE becoming aware of the illegal use through other means will be considered subject to the Bond Amendment. All such cases will be immediately processed for administrative review.

- (1) Disqualifies persons from holding a Q or L access authorization (and SCI and SAP access) who have:
    - 1 been convicted in any court of the United States for a crime, was sentenced to imprisonment for a term exceeding one year for that crime, and was incarcerated as a result of that sentence for not less than 1 year;
    - 2 been discharged or dismissed from the armed forces under dishonorable conditions, or
    - 3 been determined mentally incompetent by a proper adjudicative authority, based upon an evaluation by a duly qualified mental health professional employed by, or acceptable to and approved by, the United States Government.
  - (2) In such a case as in 1, 2 or 3, the individual's access authorization will be adjudicated in accordance with the Guidelines 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 (1) above. Full AR rights apply.
  - (3) If application of the Guidelines and the procedures set forth in this Order indicate a favorable adjudication is warranted, this will be considered a waiver of the applicable Bond Amendment disqualifier(s). The CPSO will forward the case file to the Director with a recommendation that a favorable determination (Bond Amendment waiver) be made.
  - (4) If the Director concurs, the file will be returned to the CPSO with direction to grant the Q or L. The Director will retain a list of all such waivers for periodic reporting purposes.
  - (5) If the Director does not concur, the Director will communicate with the CPSO to discuss the proper course of action.
3. Security clearance applicants and holders determined to have illegally used a controlled substance outside the 12 month parameters set forth in this Appendix may be asked to certify in writing on a DOE F 5631.9, *Drug Certification*, that they will not again engage in such use. The signing of a *Drug Certification*, in and of itself, will not be considered as mitigation of conduct involving illegal use of controlled substances; such conduct must still be subject to the requirements of this Appendix and the Guidelines. Individuals refusing to sign the *Drug Certification* will be processed under 10 CFR 710 for non-cooperation.

**CONTRACTOR REQUIREMENTS DOCUMENT**  
**DOE O 472.2, PERSONNEL SECURITY**

This Contractor Requirements Document (CRD) prescribes requirements and procedures necessary for U.S. Department of Energy, including National Nuclear Security Administration (hereafter referred to uniformly as DOE, unless otherwise specified), contractors to properly and efficiently process their employees for DOE security clearances. These requirements incorporate and supplement requirements found in the National Industrial Security Operating Manual (NISPOM), and the CRD attached to DOE M 470.4-1 Chg 2, *Safeguards and Security Program Planning and Management*, dated 10-20-10.

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 the requirements. Unless otherwise specified, all references in this CRD to contractors apply to sub-contractors.

A violation of the provisions of this CRD relating to the safeguarding or security of Restricted Data (RD), SNM or other classified information or matter, may result in a civil penalty pursuant to section 234B of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2282b). The procedures for the assessment of civil penalties are in Title 10, Code of Federal Regulations (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 Attachments 2, 3, and 4 to DOE O 472.2 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 DEAR clause 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 requirements.

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*, dated 01-16-09, as applicable.

The Atomic Energy Act 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 will be managed in accordance with DOE M 470.4-1 Chg 2, and the NISPOM.
- b. A security clearance request must be submitted to DOE only after the contractor determines that the security clearance is essential for the individual to perform tasks or services stipulated in the contract.
- c. A security clearance must not be requested 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 persons without security clearances within a controlled area. In certain instances, contractor employees who do not otherwise require access to classified information or SNM may be organizationally and/or physically situated such that they may inadvertently be exposed to classified information or SNM in the course of their duties. Federal site managers may 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; or
  - (6) Anticipate unspecified classified work.
- d. A security clearance must be requested only when required so as to avoid the unnecessary expenditure of DOE resources and the unwarranted invasion of an individual's privacy.
- e. 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.

- f. Security clearances must be requested only for individuals who are U.S. citizens and are at least 18 years of age.
- g. 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.
- h. Logistical assistance (see paragraph 4.e.) must be provided to DOE and Federal investigative agencies for conducting initial investigations, periodic reinvestigations, and additional investigations when authorized by DOE.
- i. 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.
- j. An individual's security clearance status must not be used as a determining factor for hiring, entering into a consultant agreement, or awarding a subcontract.
- k. DOE personnel security requirements and procedures must not be used by contractor management or other employees to coerce, restrain, threaten, intimidate, or retaliate against individuals for exercising their rights under the Constitution or under any statute, regulation, or DOE directive.
- l. Unless otherwise stipulated, the contractor will not be required to reimburse DOE for DOE costs associated with processing the contractor's applicants or employees for investigative or other types of actions related to security clearances.
- m. Security clearances must only be requested and maintained at the minimum number necessary to ensure operational efficiency.

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), Restricted Data (RD), Special Nuclear Material (SNM) or Sensitive Compartmented Information (SCI). Unless otherwise specified, access authorizations and security clearances will be 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 (CPSOs) are responsible. Other access authorizations issued by DOE appear in Attachment 2.

c. Security Clearances

- (1) Top Secret: A Top Secret security clearance is required for access to NSI, as defined by Executive Order 13526, classified at the Top Secret level and Formerly Restricted Data (FRD, 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 and FRD classified at the Secret and Confidential levels.
- (2) Secret: A Secret security clearance is required for access to NSI and FRD classified at the Secret level. A Secret security clearance also permits access to NSI and FRD classified at the Confidential level.
- (3) Confidential: A Confidential security clearance is required for access to NSI and FRD classified at the Confidential level.

d. Access Authorizations

- (1) Q: A Q access authorization is required for access to:
  - (a) RD, as defined by the AEA, classified at the Top Secret or Secret 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.
- (2) L: An L access authorization is required for access to RD classified at the Confidential 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. Access to SNM designated as Category IV does not require an access authorization unless a site vulnerability assessment, documented in associated site security plans, establishes such a requirement in order to minimize risk

- e. Q and L access authorizations permit access to information listed under Top Secret and Secret security clearances, respectively

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 to DOE when requesting that the individuals be processed for security clearances. Acceptable evidence of U.S. citizenship consists of the following:

- (1) For an individual born in the United States, a current U.S. passport 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 persons 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.
  - (2) For an individual claiming citizenship by naturalization, a *Certificate of Naturalization* (Form N-550 or N-570) showing the individual's name is required.
  - (3) 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:
    - (a) Certificate of Citizenship (Form N-560 or N-561),
    - (b) Report of Birth Abroad of a Citizen of the U.S. of America (State Department Form FS 240),
    - (c) *Certificate of Birth* (Form FS 545 or DS 1350),
    - (d) A current U.S. passport, or
    - (e) *Record of Military Processing-Armed Forces of the U.S.* (DD Form 1966), provided it reflects that the individual is a U.S. citizen.
- b. 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 in order to perform 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.

4. PROCESSING DOE SECURITY CLEARANCE REQUESTS.

- a. Security clearance requests must be forwarded through established channels to the CPSO. Requests must include the following (additional documentation may be required by the CPSO):
  - (1) A cover letter or form that requests the security clearance and provides the justification for processing. 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 corporate policy requires all applicants or employees to be processed for security clearances. The following represents an acceptable justification:

“Mr./Ms. \_\_\_\_\_ is a computer systems 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.b. above.
  - (3) The DOE contract or subcontract number under which the security clearance is being requested.
  - (4) Additional documentation set forth in Attachment 2.
- b. The contractor must ensure, and advise employees and applicants for employment in writing, that completed security forms and all related material will be reviewed only by designated contractor employees for adequacy and completeness before they are submitted to DOE, and that such information will not be used for any other purpose within the company. The contractor may elect 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. Contractors must 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 have the opportunity to 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 the request is 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 agency or DOE personnel security staff, and
  - (2) Ensuring that other employees are made available, as needed, to provide background 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. INTERIM AND RELATED SECURITY CLEARANCE REQUESTS.

- a. 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 an interim security clearance. Interims must be considered temporary measures pending completion of the 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)] but determinations with regard to

whether any individual is afforded such access is solely the purview of Federal CPSO staff. See Attachment 3 for additional information regarding interims.

b. Temporary Security Clearance Upgrades

- (1) Circumstances may arise where an urgent operational or contractual exigency exists requiring a cleared DOE contractor employee to have one-time or short duration access to classified information or SNM at a higher level than is authorized by their existing security clearance. In some instances, the processing time required to upgrade the security clearance would prevent timely access to the classified information or SNM, adversely impacting mission needs.
- (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 Site Manager is satisfied that exigent circumstances exist, the 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 3.

6. NON-U.S. CITIZENS.

- a. Only U.S. citizens are eligible for a security clearance. Contractors must make every effort to ensure that non-U.S. citizen employees are not 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 consideration of 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 United States citizen.
- b. LAAs will not permit access to any greater level of classified information than the U.S. Government has determined may be releasable to the country of which an individual is currently a citizen. DOE's Headquarters Office of the General Counsel will make this assessment. LAAs may only be approved if a background investigation at the level required by Executive Order 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 AND OTHER REQUIREMENTS.

- a. 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 two (2) working days followed by written confirmation within the next ten (10) working days, and include:
- (1) When a contractor applicant declines an offer of employment or fails to report for duty;
  - (2) When made aware of any other information of a personnel security interest, as delineated in Attachment 4, concerning a contractor applicant or employee;
  - (3) When a contractor applicant or employee effects any change in their citizenship status;
  - (4) When the contractor restricts or withdraws a contractor employee's access to classified information or SNM without DOE direction;
  - (5) When made aware of the death of a contractor applicant or employee;
  - (6) When a cleared contractor employee terminates employment with the contractor;
  - (7) When a cleared contractor employee no longer requires access to classified information or SNM, or
  - (8) 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).
- b. 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. They 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 that may have the tendency to impact the individual's eligibility for a security clearance (see Attachment 4) verbally and directly to DOE immediately upon the individual becoming aware of the situation or incident and in no event later than two (2) working days after the event.
  - (4) Notify DOE whenever they learn of the presence of any such situations or incidents with regard to 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 two (2) working days after the event.
  - (5) Provide DOE a completed DOE F 5631.34, *Data Report on Spouse/Cohabitant*, to the contractor within forty-five (45) days of marriage or cohabitation. NOTE: A cohabitant is a person who lives with the individual in a spouse-like relationship or with a similar bond of affection or obligation but is not the individual's legal spouse, child, or other relative (in-laws, mother, father, brother, sister, etc.). A national agency check and other indices checks as may be warranted by national-level standards will be requested by the CPSO on spouses and cohabitants of contractor employees.
- c. The foregoing responsibilities apply when completing security forms, during the course of all personnel security investigations and at any stage of the security clearance process including, but not limited to letters of interrogatory, personnel security interviews, DOE-sponsored mental health evaluations and other authorized investigative activities.
  - d. 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 terminated or, for contractor applicants, further processing of a security clearance request may be suspended.
  - e. Contractor security clearance applicants and holders must report matters of potential counter-intelligence interest (to include approaches by individuals seeking unauthorized access to classified information or SNM and foreign travel) in accordance with the CRD attached to DOE O 475.1, *Counterintelligence Program*, dated 12-10-04.
  - f. Contractors must ensure that contractor security clearance applicants and holders under their cognizance are made aware of the foregoing reporting responsibilities. 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 M 470.4-1.

8. ADMINISTRATIVE WITHDRAWAL OF SECURITY CLEARANCES.

- a. The contractor must request that the CPSO administratively withdraw a contractor employee's security clearance, and must provide the CPSO a DOE F 5631.29, *Security Termination Statement*, completed by the contractor employee, within two (2) working days from any of the following:
- (1) Termination of the contractor employee (except as provided for in section 9 of this CRD).
  - (2) A determination that a security clearance is no longer required.
  - (3) The individual's failure or refusal to cooperate with authorized and appropriate personnel security-related requests.
  - (4) If an individual's circumstances will temporarily eliminate the need for access to classified information or SNM for 90 calendar days or more (temporary change of duties, maternity or other extended leave, detail to another agency, military deployment, etc.). In such instances, the contractor may request the CPSO to waive this withdrawal requirement should the details of a particular case indicate such action would be prudent.
- 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. The CPSO must be requested to administratively withdraw an employee's security clearance even in cases where a completed DOE F 5631.29 cannot be immediately provided. 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(1) 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 60 calendar days to a position that will require a security clearance.

10. SECURITY CLEARANCE REINSTATEMENT REQUESTS. The contractor must request that the CPSO consider reinstating 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 the DOE personnel security Order.

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 receipt of notification from the CPSO of an employee's security clearance suspension or denial of final security clearance after previous approval of an interim, the contractor must ensure that the employee is precluded from access to classified information and SNM.
  - b. Suspension, denial, or revocation of an individual's security clearance does not preclude 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 particular duties and responsibilities, in accordance with national and Departmental requirements.
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, DOE file 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 effected, 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 comply with periodic DOE requests to recertify its employees' security clearance status.
- b. 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.
- c. The contractor must ensure that cleared contractor employees cooperate fully with DOE requirements concerning reinvestigations.

17. ACTIONS BY THE SECRETARY.

Nothing in this CRD will be construed to limit the Secretary's authorities and responsibilities under Executive Order 12968 (section 1.2(b), et al), Executive Order 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 due process procedures set forth at 10 CFR 710.

18. DEFINITIONS.

- a. Cognizant Personnel Security Office (CPSO). A Federal personnel security office that is authorized to submit investigative requests to investigative service providers and to adjudicate security clearances and access authorizations.
- b. Classified Information. Any information that has been determined pursuant to Executive Order 13526, or successor Orders, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and that is so designated.
- c. 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.
- d. Site Manager. The senior Federal management official at any DOE facility with a CPSO.

- e. Additional definitions may be found at the DOE Health, Safety and Security Policy Information Resources link at the Office of Departmental Personnel Security web site.

## SECURITY CLEARANCE REQUESTS/JUSTIFICATIONS AND ACCESS AUTHORIZATIONS

[This attachment provides information and/or requirements associated with DOE O 472.2 and 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 reinvestigative actions) must contain the following:
  - a. Full name of the individual;
  - b. Individual's Social Security Number, and date and place of birth;
  - c. Individual's status (Federal employee/contractor employee);
  - d. Contractor name (if contractor applicant/employee);
  - e. Contract or subcontract number (if contractor applicant/employee);
  - f. Primary program code, e.g., EM, FE, IG, OE, SC;
  - g. Facility code (if contractor employee)
  - h. Level of security clearance required, i.e. Top Secret, Secret, Confidential, 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 and title and telephone number of the requester; and
  - k. Signature of the requester.
  
2. All initial security clearance requests must include the justification, as set forth above, and (except in cases where reciprocity applies, as indicated by an '\*'):
  - a. Negative results of a drug test taken within 60 calendar days of the individual's SF 86 signature (not required for employees of state or local governments);
  - b. A complete e-QIP submission which indicates no illegal use of controlled substances for at least 12 months preceding the date of the individual's signature;\*
  - c. An SF-87, *Fingerprint Chart* (for Federal employees), a FD 258, *Applicant Fingerprint Chart* (for all others) or fingerprints taken electronically via an

- approved capture method (e.g., at a GSA-provided HSPD-12 enrollment center), when available (not required if a previous investigation included a classifiable fingerprint search by the FBI);\*
- d. Optional Form (OF) 612, *Optional Application for Federal Employment*, or a resume (for Federal applicants and employees only);\*
  - e. DOE F 5631.18, Security Acknowledgement; and
  - f. A completed fair credit reporting disclosure authorization, compliant with the Fair Credit Reporting Act, codified at 15 U.S.C. s1681 et seq. and approved for use by the Director (once obtained, this authorization may be used by DOE for conducting credit checks directly with consumer agencies as part of its personnel security program).\*
3. In addition to Q and L access authorizations, 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 his/her designated representative within the Office of Intelligence and Counterintelligence.
  - b. Cryptographic Information (CRYPTO): CRYPTO access is approved by the Office of the Chief Information Officer.
  - c. Communications Security (COMSEC): COMSEC access is approved by the Office of the Chief Information Officer.
  - d. Nuclear Weapon Data (SIGMA): Requirements and procedures for access to nuclear weapon data (categorized as SIGMA information) is determined and promulgated by the National Nuclear Security Administration using DOE and NNSA directives. For additional information, consult DOE O 5610.2, *Control of Weapon Data Chg 1*, dated 09-02-86, DOE O 452.7, *Protection of Use Control Vulnerabilities and Designs*, dated 05-14-10, DOE O 457.1, *Nuclear Counterterrorism*, dated 02-07-06, and DOE M 457.1-1, *Control of Improvised Nuclear Device Information*, dated 08-10-06, or any successor directives.
  - 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 by the head of the agency or office that created or has cognizance over the program.

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



**LIMITED ACCESS FOR NON-U.S. CITIZENS  
TEMPORARY SECURITY CLEARANCE UPGRADES  
AND INTERIM SECURITY CLEARANCES**

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

1. Limited Access Authorizations for Non-U.S. Citizens.
  - a. This section deals solely with non-U.S. citizens who have not been investigated or cleared 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 O 142.1, *Classified Visits Involving Foreign Nationals*, dated 01-13-04, or any successor directive.
  - b. 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 United States Government has determined may be releasable to the country of which the individual is currently a citizen. The DOE Office of the General Counsel must be consulted by the Director to make this assessment. Such limited access may be approved only if an investigation of the level required by Executive Order 12968, or successor national standards, for a Top Secret security clearance can be conducted.
  - c. 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 CPSO.
  - d. Upon receipt of the request, the CPSO will conduct an interview with the non-U.S. citizen to determine:
    - (1) The nature and extent of the individual's contacts and continuing associations with persons outside the United States (to include family members);
    - (2) The degree to which the individual exercises his or her foreign citizenship;
    - (3) Whether the individual or any of the individual's associates (to include family members) are or have been affiliated with any foreign government, and

- (4) The degree to which it is likely that an appropriate background investigation can be conducted on the individual.
- e. After completion of the interview, the CPSO will, through the local DOE counterintelligence office, ensure that a preliminary CI-focused risk assessment is completed. 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.
- f. If the results of the risk assessment support continued processing, the CPSO will forward the results of the interview and risk assessment, along with all other relevant information, to the Director, Office of Departmental Personnel Security. The Director will, in coordination with appropriate headquarters authorities, determine whether processing the non-U.S. citizen for an LAA is appropriate.
- g. The Director will either:
  - (1) Determine to continue to processing the LAA request, in which case the Director will notify the CPSO to commence processing the individual for a background investigation, or
  - (2) Determine that the individual will not be processed for an LAA. In this case, the Director will so notify the CPSO and the applicable Program Secretarial Officer.
- h. In the case of a determination as in g.(1), the CPSO will process the individual for a background investigation in accordance with investigative and adjudicative procedures set forth in this Order.
- i. When the CPSO has reached an adjudicative determination, the CPSO will coordinate a formal comprehensive CI-focused risk assessment with the local DOE counterintelligence office.
- j. The CPSO will then forward the results of the adjudication and the risk assessment to the Director for concurrence. The Director will concur and instruct the CPSO to grant the LAA, or will non-concur and notify the CPSO and the applicable Program Secretarial Officer. The Director's determinations in these cases are final.
- k. All LAAs must be reviewed annually by the CPSO to ensure that they are still needed. An annual re-justification by the Program Secretarial Officer who initially requested the LAA is required. 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.

- l. Denials of LAAs are final and not subject to review under the procedures set forth in 10 CFR 710.
  - m. LAAs must be administratively withdrawn by the CPSO immediately 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.
  - n. LAAs must be immediately revoked should the CPSO come into possession of information that indicates the individual no longer satisfies the eligibility requirements for an LAA, or at the direction of the Director. . Such revocations are not subject to the administrative review procedures set forth in 10 CFR 710.
  - p. 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:
    - (1) Top Secret, Top Secret CRYPTO, RD, FRD or Special Access Program (SAP) information.
    - (2) Information that has not been determined by a U.S. Government Designated Disclosure Authority to be releasable to the country of which the individual is a citizen.
    - (3) COMSEC information.
    - (4) SCI or Intelligence information.
    - (5) 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.
    - (6) Information for which foreign disclosure has been prohibited in whole or in part (identified as NOFORN).
    - (7) Classified information provided to the U. S. Government by a third party government and information furnished in confidence to the U.S. Government by a third party government.
2. Temporary Security Clearance Upgrades.
- a. Conditions.
    - (1) Such security clearances must be necessary to meet operational or contractual exigencies not expected to be of a recurring nature;

- (2) Such security clearances will remain valid until the exigencies have abated, but must in no case exceed 180 calendar days, and
- (3) Such security clearances will be limited to specific, identifiable information. The nature of this information must be referenced on the request for access.

b. Procedures.

- (1) Requests for such security clearances will include a justification and will 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 security clearance, identify the information to which the individual will be afforded access, and describe the exigent circumstances prompting the request.
- (2) If the CPSO is satisfied that exigent circumstances exist, that routine processing of the individual for the higher level security clearance would adversely impact mission needs, is not in possession of information indicating that access at the higher level would jeopardize Departmental interests or the national's security, and that the request is not an attempt to circumvent normal processing requirements, the CPSO will grant the upgrade request. Otherwise, the request will be denied and returned to the requester with an explanation as to the reason(s) for the denial.
- (3) Recipients of temporary security clearance upgrades 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.
- (4) Temporary security clearance upgrades must be recorded in the recipient's PSF and in CPCI, but will not be included in submissions to inter-agency databases. Such security clearances are not subject to reciprocity.
- (5) 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.
- (6) Such security clearances will 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.

- (7) If, during the period of such a security clearance, information of a security concern arises which indicates that suspension or revocation of the individual's permanent security clearance may be warranted, the temporary security clearance will be canceled and action will be taken under 10 CFR 710 regarding the permanent clearance. No due process or other procedural rights exist with regard to temporary security clearance upgrades.
- (8) Temporary upgrades to or among other access programs such as COMSEC, CRYPTO, SCI, NATO or SIGMA remains within the domain of the appropriate program.
- c. Subsequent requests for temporary security clearance upgrades for individuals previously granted a temporary upgrade may be considered by the CPSO, in accordance with the procedures set forth in this section, but must be accompanied by documentation necessary to process the individual for the required security clearances, as set forth elsewhere in this Order. Once the subsequent temporary upgrade has been granted, the CPSO will process the individual for the security clearance in accordance with the requirements of this Order.

3. Interim Security Clearances.

- a. The need for an interim security clearance must originate with the requester (individuals may not request interim access on their own behalf) and be approved in writing by the Federal head of the applicable Departmental element in which the individual will be assigned.
- 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. An interim security clearance 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 (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 an

interim security clearance has been denied, and that the case must proceed according to normal processing procedures.

- e. Requests for interims on 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 opened by the investigative service provider,
  - (2) The CPSO is not in possession of any information of a security concern, and
  - (3) Minimal investigative checks, as indicated below, have been completed with no information of a security concern revealed.
    - (a) For interim L, Secret and Confidential security clearances, a credit check must be completed.
    - (b) For interim Q and Top Secret security clearances, OPM, Department of Defense and FBI investigative indices along with an FBI fingerprint check and a credit check must be completed.
- f. Supporting rationale for all interim security clearances will be recorded in the subject's PSF. All interim security clearances 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 interim security clearances must be notified in writing that their continued security clearance is conditioned upon a 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. The CPSO should take steps to expedite investigative and adjudicative activities in all cases where interim security clearances have been issued.
- i. If DOE cancels an individual's interim security clearance, the individual's employer must ensure that the individual is precluded from access to classified information and SNM.
- j. When DOE grants, denies, or stops processing the security clearance, the interim security clearance must be canceled.
- k. Access to other programs or types of information (COMSEC, CRYPTO, SCI, NATO or SIGMA) based upon an interim will be granted or not at the sole discretion of the office with authority for such access.

## **REPORTING REQUIREMENTS**

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

Information which must be reported in accordance with paragraph 4.u. of this Order and paragraph 7.b.(3) of the CRD includes, but is not limited to:

1. Legal action effected for a name change;
2. Change in citizenship;
3. Any use of an illegal drug, or use of a legal drug in a manner that deviates from approved medical direction;
4. Any arrests, criminal charges (including charges that are dismissed), citations, tickets, summons or detentions by Federal, State, or other law enforcement authorities for violations of law within or outside of the U. S. Traffic violations for which a fine of up to \$300 was imposed need not be reported, unless the violation was alcohol- or drug-related;
5. An immediate family member assuming residence in a sensitive country;
6. Hospitalization for mental health reasons or treatment for drug or alcohol abuse;
7. Employment by, representation of, or other business-related association with a foreign or foreign-owned interest or non-U.S. citizen or other individual who is both a U.S. citizen and a citizen of a foreign country;
8. Personal or business-related filing for bankruptcy, or
9. Garnishment of wages.