

ERRATA SHEET

The Office of Primary Interest has identified several minor errors in DOE O 472.1C, *Personnel Security Activities*, dated 3-25-03. This Errata Sheet corrects the following errors:

- In paragraphs 5.a.(9) and 5.o.(4), the reference to paragraph “5q” should be “5p”.
- In Attachment 2, paragraph 4.a.(4) the reference to paragraph “3c” should read “3d” instead.
- In Attachment 2, paragraph 5.c., “or Oak Ridge, Tennessee” should be added after “New Mexico”.
- In Attachment 4, last line, “Page II-3” should be “Page II-2”.

The changes have been made in this Order.

This Errata Sheet is to remain with DOE O 472.1C.

Approved: 3-25-03
Sunset Review: 3-25-05
Expires: 3-25-07

SUBJECT: PERSONNEL SECURITY ACTIVITIES

1. OBJECTIVES. In accordance with Federal statutes, Executive Orders, Department of Energy (DOE) regulations, and the mission of the National Nuclear Security Administration (NNSA) establish requirements to:
 - a. ensure that individuals are processed for, granted, and retain a DOE access authorization only when their official duties require such access;
 - b. allow access to DOE classified matter and special nuclear materials (hereafter referred to as SNM) only when it has been determined that such access will not endanger the common defense and security and is clearly consistent with the national interest;
 - c. maintain the numbers and types of access authorizations at the minimum levels necessary to ensure the operational efficiency of DOE classified and SNM programs and operations;
 - d. conduct personnel security activities in a manner that ensures:
 - (1) timely and efficient processing of initial access authorization requests and reinvestigations;
 - (2) consistent, objective, and fair interpretation and application of criteria and procedures in every access authorization action;
 - (3) timely review and adjudication of investigative reports and other information related to an individual's access authorization eligibility; and
 - (4) maintenance of accurate, complete, and timely access authorization file and record information, the availability of such information to authorized users, and the protection of such information against unauthorized disclosure;
 - e. periodically evaluate individuals retaining access authorizations to confirm their continued need-for-access and access authorization eligibility;
 - f. ensure that DOE employees, contractors, and others involved in personnel security activities effectively and efficiently execute their personnel security related responsibilities and authorities;

work, the site/facility management contractors with the CRD incorporated into their contracts are responsible for compliance with the requirements of the CRD. Affected site/facility management contractors are responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure the site/facility management contractors' compliance with the requirements.

- c. Exclusion. Consistent with the responsibilities identified in Executive Order 12344, the Deputy Administrator, Naval Reactors, shall determine the applicability of this Order for activities and facilities under his control.
4. REQUIREMENTS. Definitions of commonly used terms are provided in the *Safeguards and Security Glossary of Terms*, and selected definitions are also set forth in sections 710.5 (Subpart A) and 710.54 (Subpart B) of 10 CFR 710.
- a. Personnel Security Assurance Program (PSAP).
 - (1) An individual shall not be processed under 10 CFR 710, Subpart B, to determine suitability for Federal, contractor, or other employment.
 - (2) An individual shall not occupy a PSAP-designated position (hereafter referred to as a "PSAP position") until approval has been granted by a PSAP Approving Official.
 - (3) A PSAP Implementation Plan shall be prepared for each site or facility with PSAP positions.
 - b. Personnel Security Program.
 - (1) No individual shall be permitted access to classified matter and/or SNM under DOE control until that individual has been determined to be eligible for such access in accordance with the procedures in this Order, DOE M 472.1-1B, 10 CFR 710, or other DOE Orders or Manuals, e.g., DOE O 470.1, *Safeguards and Security Program*, Chapter VIII, dated 9-28-95. (See Attachment 3, "Access to Classified Matter Allowed by Type of DOE Access Authorization and Initial Investigation Requirements," and Attachment 4, "Access to Special Nuclear Materials Allowed by Type of DOE Access Authorization.")
 - (2) For DOE employees and contractors, access authorizations shall be requested only for individuals selected to occupy positions that require the incumbent to have access to classified matter and/or SNM in order to perform official work for DOE.
 - (3) DOE shall accept and process requests for, and grant or reinstate, only Q and L access authorizations.

- (4) Except as authorized by this Order and DOE M 472.1-1B, only United States citizens are eligible for access authorizations.
- (5) A request for access authorization shall be processed only when the need for access is clearly justified, and of the type (Q or L) required, to avoid the unnecessary expenditure of DOE funds and other resources and the unwarranted invasion of an individual's privacy.
- (6) Individuals under DOE cognizance must possess a DOE Q access authorization prior to being afforded access to classified matter designated as "CRYPTO," "COMSEC," "Sensitive Compartmented Information," or Weapon Data, Sigma 14 or Sigma 15.
- (7) The dissemination of personnel security information and personnel security file data shall be controlled in accordance with the Privacy Act of 1974, as amended, and DOE directives.
- (8) Access authorizations shall not be processed (i.e., granted, continued, reinstated, transferred, or extended) to:
 - (a) allow the dissemination of classified matter on other than a need-for-access basis;
 - (b) avoid the use of access controls or physical barriers to distinguish perimeters among security areas or between security and open areas;
 - (c) alleviate responsibilities for escorting uncleared individuals within a security area;
 - (d) establish a pool of cleared employees;
 - (e) accommodate an individual's personal convenience, expedience, gain, or advantage, or anticipation of unspecified future classified work; or
 - (f) determine suitability for Federal, contractor, or other employment. [NOTE: For Federal employees, the investigative reports provided to DOE for determining access authorization eligibility may also be used to determine employment suitability; however, an access authorization may not be requested solely for the purpose of obtaining investigative reports for an employment suitability determination.]

- (9) Initial access authorization requests, reinvestigations, or other requests for an access authorization action shall not be processed:
 - (a) unless all of the required forms have been legibly completed, signed (when appropriate), and provided by the applicant, access authorization holder, and/or sponsor;
 - (b) if the preprinted content of the forms has been altered; or
 - (c) if insufficient, incorrect, or conflicting information is provided.
- (10) As a condition of access authorization approval, individuals may be required to execute a consent form for investigative agencies to obtain, on behalf of DOE and during the access authorization period and for 3 years thereafter, their commercially available financial records, consumer credit reports, and travel records.
- (11) Except as authorized by the Director, Office of Security, an individual's access authorization eligibility shall 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 another Federal agency authorized to conduct background investigations.
- (12) DOE shall take all reasonable measures to obtain existing investigative reports that may fulfill DOE standards and specifications for the scope and extent of investigations, as established by the Secretary, for use in determining an individual's access authorization eligibility.
- (13) DOE shall, whenever possible, grant access authorizations based on the interagency reciprocity procedures in DOE M 472.1-1B.
- (14) DOE shall not submit a request for investigation to the OPM or the FBI if the individual being processed by DOE is currently being investigated by these or another agency for access authorization or security clearance purposes, unless the type of investigation, when completed, will not be sufficient for DOE's needs.
- (15) The use of interim access authorizations shall be kept to the absolute minimum and considered only when properly requested in accordance with procedures in this Order and DOE M 472.1-1B.
- (16) Determinations for access to Restricted Data pursuant to section 145b, Atomic Energy Act of 1954, as amended, shall be used only for the President and Vice President; Federal justices, judges, and magistrates; members of Congress; and State governors and lieutenant governors.

- (17) A Foreign Ownership, Control, or Influence (FOCI) determination shall be rendered for a covered contractor by DOE before DOE acts to grant, reinstate, continue, extend, or transfer an access authorization for the contractor's personnel.
- (18) When information contained in investigative reports, or the receipt of other reliable information, raises a question concerning an individual's access authorization eligibility, additional actions may be authorized for collecting relevant information pertaining to the eligibility determination. If the question is favorably resolved, the access authorization shall be granted, continued, or reinstated. If the question cannot be favorably resolved, the individual's access authorization shall be determined under 10 CFR 710, Subpart A.
- (19) Only DOE employees who are so authorized in writing shall determine an individual's access authorization eligibility or render other formal determinations that affect an individual's access authorization status. [NOTE: This requirement does not preclude a contractor from having an employee execute a "Security Termination Statement" or restricting an employee's access to classified matter or SNM prior to notifying the cognizant DOE office.]
- (20) DOE employees authorized to render access authorization eligibility determinations shall receive training in decision making prior to actually rendering such determinations.
- (21) All individuals processed for access authorizations shall be treated equally, regardless of their employment status, to preclude the appearance, inference, or practice of partiality or favoritism.
- (22) Any DOE officer or employee who uses personnel security activities to coerce, restrain, threaten, intimidate, or retaliate against individuals for exercising their rights under any statute, regulation, or DOE directive shall be subject to appropriate disciplinary action.
- (23) Except as authorized by the Director, Office of Security, individuals with access authorizations shall be periodically reinvestigated as stipulated in DOE M 472.1-1B.
- (24) DOE security officials are authorized to request updated security forms in order to process a periodic reinvestigation, or at any time when there is probable cause that the individual may have engaged in an activity, or been subject to circumstances, that affect continued access authorization eligibility.

- (25) Except for access permittees who reimburse DOE for investigation costs at rates established by DOE's Chief Financial Officer, DOE assumes security investigation costs associated with processing individuals for initial access authorizations and reinvestigations. DOE's Chief Financial Officer reserves the right to designate specific DOE programs or activities responsible for the reimbursement of such costs.
 - (26) Within 2 working days of receipt of notification that an individual no longer requires access to classified matter and/or SNM, DOE will terminate the individual's access authorization.
 - (27) DOE shall maintain, as stipulated in DOE M 472.1-1B, a personnel security file, in either paper or electronic form, for each individual processed for access authorization.
 - (28) DOE shall maintain a personnel security automated information system for recording all access authorization transactions.
 - (29) In all matters related to personnel security activities, DOE retains absolute authority. The procedures in this Order, DOE M 472.1-1B, and 10 CFR 710 are not subject to collective bargaining between Federal and contractor management and labor.
 - (30) Individuals under the age of 18 shall not be processed for or granted DOE access authorization.
- c. Deviations. Requests for deviations from the requirements in this Order and DOE M 472.1-1B shall be processed in accordance with paragraph 4f(3) of DOE O 470.1, *Safeguards and Security Program*. Requests for deviations from the requirements and procedures of 10 CFR 710 shall not be approved.

5. RESPONSIBILITIES AND AUTHORITIES.

- a. Heads of Headquarters Elements.
 - (1) Ensure that the PSAP is implemented for all applicable operations and/or activities for which they have programmatic responsibility.
 - (2) Recommend Headquarters positions for inclusion under PSAP when those positions are not identified as PSAP positions in 10 CFR 710.55(a) and (b).
 - (3) Submit interim access authorization requests to the Director, Office of Security, in accordance with DOE M 472.1-1B.
 - (4) Determine the access authorization requirement, if any, for each position under their cognizance occupied by a DOE employee, applicant for

employment, consultant, or other agency assignee and, when appropriate, ensure that access authorization requirements are stated in position descriptions, vacancy announcements, consultative agreements, and agreements with other agencies that provide for assignees to DOE.

- (5) Ensure that all requests for staff access authorizations are coordinated with their servicing personnel office.
- (6) Approve and transmit directly to the Director, Office of Security, for processing, with written justification, access authorization requests (including requests for access authorization reinstatement, extension, or transfer) for the following individuals under their cognizance:
 - (a) employees of other agencies assigned or detailed to DOE, including members of the Armed Forces and/or civilian employees of the Department of Defense (DoD) and the National Aeronautics and Space Administration (NASA);
 - (b) employees, consultants, or agents of DOE contractors and subcontractors;
 - (c) foreign nationals (see DOE M 472.1-1B); and
 - (d) any other individual who will perform work for, be trained by, or represent DOE under any formal agreement, understanding, contract, or treaty.
- (7) Provide written verification of the continuing need for access authorizations by individuals under their cognizance when periodically requested to do so by the Director, Office of Security.
- (8) Provide written notification to the Director, Office of Security, of the following conditions affecting access authorizations for individuals under their cognizance:
 - (a) within 2 working days for termination of an individual's access authorization;
 - (b) within 8 working hours upon becoming aware that an individual has been hospitalized or is otherwise being treated for a mental illness or such other condition as may cause a significant defect in the individual's judgment or reliability; and
 - (c) within 2 working days of becoming aware of derogatory information of personnel security interest concerning the individual. Such information must be reliable and relevant in

terms of the clearance criteria exemplified in 10 CFR 710.8 (a copy of which may be obtained from the Director, Office of Security).

- (9) Ensure that individuals under their cognizance granted, or in process for, access authorizations are aware of the reporting requirements in paragraph 5p below.
 - (10) Designate a staff representative(s) responsible for administering the coordinating functions required by, and the review of procurement falling within the scope of, this Order and DOE M 472.1-1B. Unless a designation is made, procurement originators shall be responsible for coordinating the requirements of this Order and DOE M 472.1-1B, with the Director, Office of Security.
 - (11) Notify contracting officers of affected site/facility management contracts to incorporate the CRD of this directive into those contracts. Ensure procurement requests for new non-site/facility management contracts require inclusion in the resulting contracts, if appropriate, of the clause at 48 CFR 952.204-2, Security, and the requirements of this CRD.
- b. Director, Office of Security, acts as the senior Agency official responsible for the direction and administration of the DOE Personnel Security Program. (Secretary of Energy Delegation Order No. 00-030-00, dated 12-6-01.)
- (1) Acts for the Secretary to authorize access to DOE classified matter and/or SNM prior to, or in lieu of, the completion of the required investigation in accordance with section 145b of the Atomic Energy Act of 1954, as amended, when such action is determined to be clearly consistent with the national interest.
 - (2) Promulgates and establishes regulations, requirements, procedures, standards, and guidance for the PSAP and Personnel Security Program.
 - (3) Authorizes field elements to implement, maintain, or terminate Personnel Security Program activities as prescribed in this Order and DOE M 472.1-1B.
 - (4) Implements Headquarters Personnel Security Program activities.
 - (5) Provides to the Chief Financial Officer annual estimates of the funds required to reimburse other agencies for investigations requested by DOE for access authorization and employment suitability determinations and for the conduct of program-related activities.

- (6) Authorizes field elements annually to submit requests for investigations, on a scheduled basis, directly to the OPM and the FBI within a specifically allocated total dollar amount and/or a specifically allocated total number of investigations by type.
- (7) Approves any adjustments to field element annual investigations allocations.
- (8) Coordinates with the OPM and the FBI on matters related to reimbursable costs for investigations and approves such reimbursements from DOE funds.
- (9) Approves requests to initiate access authorization processing of foreign nationals.
- (10) Enters into memoranda of agreement or understanding to allow and control access to DOE personnel security and administrative review files, and/or personnel security databases by representatives of DOE elements or other Federal agencies.
- (11) Establishes and manages a centralized automated information system to record all DOE access authorization transactions.
- (12) Authorizes access authorization certifications, verifications, or other related data in response to official requests or inquiries by other Federal agencies and by foreign governments with which agreements exist for DOE to provide such information.
- (13) Approves the review of Headquarters-maintained personnel security files by accredited representatives of Federal investigative agencies and such other routine users as specified under Privacy Act and DOE regulations and maintains official records of such reviews.
- (14) Conducts interagency liaison with the OPM and the FBI on all personnel security activities and notifies these agencies of the cancellation of requests for investigation in Headquarters cases.
- (15) Represents DOE in interagency efforts related to personnel security activities.
- (16) Initiates investigation of spouses or cohabitants of individuals who marry or cohabit after being processed for access authorizations.
- (17) Initiates investigations and grants DOE access authorizations for access to Restricted Data for DoD and NASA personnel assigned for duty with DOE or a DOE contractor, or with other Federal agencies.

- (18) Initiates investigations and grants DOE access authorizations to other Federal agency personnel when required.
- (19) Accepts properly executed security clearance certifications for DoD and NASA personnel assigned for duty with DOE and who require access to DOE classified matter and/or SNM.
- (20) Updates the list of DOE “positions of a high degree of importance or sensitivity.” (See Attachment 5.)
- (21) Ensures that specialized training is provided for DOE Personnel Security Specialists, program support personnel, and other DOE employees involved in the access authorization eligibility determination process.
- (22) Conducts periodic program reviews of DOE personnel security activities, as directed or requested, to ensure uniform, fair, and objective implementation and application of the requirements in this Order, DOE M 472.1-1B, and 10 CFR 710.
- (23) Serves as the sole contact with investigative agencies in determining whether sufficient personal history information can be obtained to determine an individual’s access authorization eligibility.
- (24) Retains duplicate personnel security files at Headquarters on selected field element officials, as indicated in DOE M 472.1-1B, and for all foreign nationals with a DOE access authorization.
- (25) Develops and/or approves all DOE forms used in implementing personnel security activities.
- (26) Reviews PSAP Implementation Plans and subsequent changes for consistency with requirements.
- (27) Develops and provides training curricula and materials for implementing PSAP.
- (28) Provides research and analysis in PSAP-related activities.
- (29) Executes the following personnel security management functions for DOE Headquarters, Energy Technology Centers, Power Marketing Administrations, and the Strategic Petroleum Reserve Project Office:
 - (a) implements and administers PSAP and Personnel Security Program activities consistent with this Order, DOE M 472.1-1B, and 10 CFR 710; and

- (b) performs responsibilities in this Order assigned to managers.
- c. General Counsel performs responsibilities in 10 CFR 710, Subpart A, for Headquarters administrative review cases.
- d. Chief Counsels of Field Elements perform responsibilities in 10 CFR 710, Subpart A.
- e. Director of Hearings and Appeals performs responsibilities in 10 CFR 710, Subpart A.
- f. Deputy Administrator, Naval Reactors, where he has determined that this Order is applicable under paragraph 3.c. above, implements and oversees all requirements in this Order and DOE M 472.1-1B for activities under his cognizance.
- g. Headquarters Servicing Personnel Offices.
 - (1) Process and transmit to the Director, Office of Security, all access authorization requests received from Headquarters elements for DOE employees and applicants for employment.
 - (2) Resolve employment suitability issues for Headquarters DOE employees and applicants for employment prior to an initial or continuing access authorization eligibility determination by the Director, Office of Security.
- h. Managers of the Chicago, Idaho, Oak Ridge, Richland, and Savannah River Operations Offices, the Pittsburgh and Schenectady Naval Reactors Offices, and the Director, Service Center, Albuquerque, for PSAP.
 - (1) Identify individuals whose official duties fall within the definition of a “PSAP position” at a DOE site/facility under their cognizance.
 - (2) Ensure that a PSAP Implementation Plan is prepared for each site/facility with PSAP positions and provide the plan to the Director, Office of Security, for review and comment.
 - (3) Review and approve PSAP Implementation Plans and ensure that a PSAP is implemented at the site/facility within 30 working days after the Plan is approved.
 - (4) Approve PSAP Implementation Plan changes and notify the Director, Office of Security, of such changes.
 - (5) Recommend to the Director, Office of Security, additional positions for designation as PSAP positions as they are identified and justified.

- (6) Process requests for individuals to occupy PSAP positions and perform other responsibilities consistent with 10 CFR 710, Subpart B.
- i. Managers of the Chicago, Idaho, Oak Ridge, Richland, and Savannah River Operations Offices, the Pittsburgh and Schenectady Naval Reactors Offices, and the Director, Service Center, Albuquerque, for the Personnel Security Program.
 - (1) Ensure implementation, administration, and operation of program activities for all covered contractors, subcontractors, access permittees, and staff under their cognizance consistent with this Order, DOE M 472.1-1B, and 10 CFR 710.
 - (2) Ensure training complies with the requirements in DOE M 472.1-1B.
 - (3) Shall, prior to submitting a request for investigation to an investigative agency for an individual under their cognizance:
 - (a) determine the position access authorization requirements and the type of investigation to be conducted;
 - (b) ensure that the access authorization justification and security forms are adequate and complete;
 - (c) verify that the request from a management and operating contractor, or other specified contractor, is accompanied by the preemployment or pre-processing checks required by 48 CFR 970.2201(b)(1)(ii) and that, except for foreign nationals, each contractor request is accompanied by verification of the individual's United States citizenship (see Attachment 2, paragraph 3b);
 - (d) establish a personnel security file for the individual and enter appropriate data into the DOE personnel security data management system;
 - (e) determine whether current investigative reports exist that can be obtained and used by DOE as a basis for determining the individual's access authorization eligibility;
 - (f) determine whether the individual is being concurrently processed for an access authorization or security clearance by another agency; and
 - (g) verify that funds are available to reimburse the appropriate investigative agency.

- (4) Initiate requests directly with the OPM and the FBI for initial investigations; reinvestigations; supplemental, additional, or upgrade investigations; and cancellations of investigations in progress.
- (5) Implement procedures requiring DOE supervisors and DOE contractors under their cognizance to provide notification to a designated DOE personnel security official of the following conditions affecting an applicant's or employee's access authorization status (i.e., notification shall not be provided if the individual does not hold, or is not in process for, a DOE access authorization):
 - (a) verbal notification within 8 working hours and written confirmation within the next 10 working days when aware of an individual's hospitalization or other treatment for a mental illness or other condition that may cause a significant defect in the individual's judgment or reliability;
 - (b) verbal notification within 2 working days and written confirmation within the next 10 working days when aware of information of personnel security interest. Such information must be characterized as reliable and relevant and create a question as to an individual's access authorization eligibility as exemplified in 10 CFR 710.8 (see the reverse side of DOE F 5631.18, "DOE Security Acknowledgment"); and
 - (c) verbal notification within 2 working days and written confirmation within the next 10 working days when an individual's DOE access authorization should be terminated.
- (6) Request the Director, Office of Security, to approve initiation of an investigation of a foreign national under their cognizance proposed for employment in a position that will require the incumbent to possess a DOE access authorization.
- (7) Refer to the Director, Office of Security, DOE access authorization requests for other Federal agency employees, consultants, and contractors; members of Congress and congressional staffers; and State governors and lieutenant governors.
- (8) Provide to the Director, Office of Security, for processing "Data Report on Spouse/Cohabitant" forms completed by individuals under their cognizance who marry or cohabit after having been granted, or while being processed for, DOE access authorizations.
- (9) For access to Secret and/or Confidential National Security Information, and/or Formerly Restricted Data involved in DOE contracts and

subcontracts, accept written assurances that the facility personnel engaged in DOE work possess a final security clearance from another Federal agency at the appropriate level for access to National Security Information.

- (10) For the purpose of granting access to Confidential Restricted Data involved in DOE contracts and subcontracts, accept written assurances that facility personnel engaged in DOE work possess a final security clearance from another Federal agency at the appropriate level for access to National Security Information, in accordance with the stipulations in DOE M 472.1-1B.
- (11) Render a favorable Foreign Ownership, Control, or Influence determination for covered contractors prior to taking a final access authorization action.
- (12) Transmit requests for interim access authorization to the Director, Office of Security.
- (13) Delegate authorities and responsibilities in writing to all DOE employees conducting program activities covered by this Order, DOE M 472.1-1B, or 10 CFR 710 and maintain a current record of the following:
 - (a) DOE employees authorized to grant, continue, extend, reinstate, transfer, upgrade, downgrade, and/or terminate access authorizations;
 - (b) DOE and DOE contractor employees authorized to review personnel security files; and
 - (c) DOE and DOE contractor employees authorized to access data contained in the DOE personnel security data management system.

[NOTE: Delegations may be made in a DOE employee's official position description.]

- (14) Grant, continue, extend, reinstate, transfer, upgrade, downgrade, and terminate access authorizations for individuals under their cognizance in all cases except those processed under 10 CFR 710 procedures.
- (15) Render determinations, in accordance with 10 CFR 710 procedures, to:
 - (a) suspend processing an access authorization application or terminate an individual's access authorization;
 - (b) suspend an individual's access authorization; and

- (c) grant, reinstate, deny, or revoke an access authorization when the individual does not, or fails to, request a hearing before a DOE hearing officer or when the individual's administrative review case is remanded to the manager by the hearing officer for a determination.
- (16) Inform individuals in writing whose access authorization eligibility has been favorably resolved following a personnel security interview or other action, when individuals request such written notification.
- (17) Effect appropriate actions and notifications when the access authorization of an individual under their cognizance is suspended, granted, revoked, reinstated, denied, or terminated under 10 CFR 710 procedures.
- (18) Accept investigations and reports on the character, associations, and loyalty of individuals made by OPM, FBI, or another Federal agency that conducts personnel security investigations, provided that such investigations meet the scope and extent of DOE standards as specified in DOE M 472.1-1B.
- (19) Ensure, to the extent practicable, that personal history information on employment forms completed by DOE employees and applicants for employment is consistent with information reflected on existing or new personnel security forms. The comparability review shall be completed prior to forwarding personnel security forms to an investigative agency or effecting other personnel security actions.
- (20) Maintain and protect personnel security files containing copies of investigative reports and other pertinent and relevant data on individuals who are processed for access authorizations.
- (21) Approve and maintain records of the review of personnel security files by authorized other agency personnel and other routine users under DOE implementing regulations for the Privacy Act.
- (22) Ensure that all access authorization transactions effected for individuals under their cognizance are accurately recorded in the DOE personnel security data management system.
- (23) Ensure that investigative reports on DOE employees and applicants for employment under their cognizance are reviewed and adjudicated by the appropriate servicing personnel office for employment suitability issues prior to access authorization eligibility determinations.
- (24) Arrange with other office managers to provide operational and/or administrative support services or assistance when the location of an

individual or facility justifies such an arrangement as a practical matter of convenience, economy, or benefit to DOE.

- (25) Request Director, Office of Security, approval for the use of locally generated forms in the conduct of personnel security activities.
- (26) Ensure that all individuals under their cognizance performing personnel security activities are aware of the prohibition against reprisal or discrimination toward any individual who has made a protected disclosure or engaged in protected activities.
- (27) Review procurement requests for new non-site/facility management contracts and, if appropriate, ensure that the clause at 48 CFR 952.204-2, Security, and the requirements of the CRD of this directive are included in the contract.

j. PSAP Approving Officials.

- (1) Participate in the DOE personnel security review process to determine the eligibility of an applicant or incumbent to occupy a PSAP position.
- (2) Approve placement/continuation in PSAP positions of applicants and incumbents and advise appropriate management.
- (3) Ensure implementation of PSAP education and training.
- (4) Immediately notify, for the purpose of limiting access, the appropriate management official of a personnel security action that results in the suspension of access authorization of an individual in a PSAP position.

k. Managers of DOE Organizations and Contractors Having PSAP Positions.

- (1) Prepare a PSAP Implementation Plan and manage PSAP activities consistent with 10 CFR 710, Subpart B, which includes the identification of PSAP positions at sites/facilities under their cognizance.
- (2) Conduct a drug testing program for PSAP position applicants and incumbents in accordance with 10 CFR 707.
- (3) Ensure that supervisory reviews and medical assessments are conducted and recommendations offered for PSAP position applicants and incumbents during the conduct of initial and annual reviews, and at any other time, as appropriate.

- (4) Immediately notify the PSAP Approving Official of information that represents a security concern regarding a PSAP employee.

l. Site Occupational Medical Directors.

- (1) Conduct initial and annual medical examinations of PSAP position applicants and employees as provided for in DOE medical standards for management.
- (2) Review and take appropriate action regarding referrals for unusual conduct of PSAP employees.
- (3) Recommend to the appropriate management official and PSAP approving official the temporary reassignment to non-PSAP duties of a PSAP employee when the site occupational medical director becomes aware of a condition or circumstance that may affect the employee's judgment or reliability. (See 10 CFR 710.8.)
- (4) Advise the appropriate management official and PSAP approving official of any security concern regarding a PSAP employee.
- (5) Evaluate and recommend the return to work of a PSAP employee who has been on sick leave for 5 or more consecutive workdays.

m. Supervisors and Selecting Officials of Individuals in PSAP Positions.

- (1) Conduct supervisory reviews of PSAP position applicants and incumbents in accordance with 10 CFR 710.57.
- (2) Ensure that individuals seeking or occupying PSAP positions are informed of their program responsibilities and have executed the appropriate PSAP releases, acknowledgments, and waivers to facilitate the collection and dissemination of information and the performance of drug testing and medical examinations.
- (3) Immediately notify the appropriate management official of a security concern relating to a PSAP employee.
- (4) Refer PSAP employees exhibiting unusual conduct to the Site Occupational Medical Director for review and appropriate action.
- (5) Approve the return to work of a PSAP employee who has been on sick leave for 5 or more consecutive workdays upon receipt of a written recommendation to return to work from the site occupational medical director.

n. Contracting Officers.

- (1) After notification by the appropriate program official, incorporate the CRD into the affected site/facility management contracts in accordance with the Laws, Regulations, and DOE Directives clause of the contracts.
- (2) Assist originators of procurement requests who want to incorporate the clause at 48 CFR 952.204-2, Security, and the requirements of the CRD of this directive in new non-site/facility management contracts, as appropriate.

o. DOE Employees Assigned to PSAP Positions.

- (1) Execute PSAP releases, acknowledgments, and waivers to facilitate the collection and dissemination of information and the performance of drug testing and medical examinations.
- (2) Notify the Site Occupational Medical Director immediately of a physical or mental condition requiring medication or treatment.
- (3) Report in person, prior to returning to work, to the Site Occupational Medical Director following sick leave of 5 or more consecutive workdays.
- (4) Comply with the requirements listed in paragraph 5p below.

p. Individuals Applying for or Granted DOE Access Authorizations.

- (1) Provide full, frank, and truthful answers to relevant and material questions and, when requested, furnish or authorize others to furnish information that DOE deems pertinent to the access authorization eligibility process. This obligation applies when completing security forms, during the course of an initial investigation and reinvestigation, and at any stage of access authorization processing including, but not limited to, letters of interrogatory, personnel security interviews, DOE-sponsored mental evaluations, and other authorized DOE investigative activities. An individual may elect not to cooperate; however, such refusal may prevent DOE from granting or continuing access authorization. In this event, any access authorization in effect may be terminated or, for applicants, further processing may be suspended [refer to 10 CFR 710.6(a)].
- (2) Directly notify the cognizant DOE personnel security office of the following: [NOTE: Verbal notification is required within 2 working days followed by written confirmation within the next 3 working days.]

- (a) all arrests, criminal charges (including charges that are dismissed), or detentions by Federal, State, or other law enforcement authorities for violations of law, other than traffic violations for which only a fine of \$250 or less was imposed, within or outside of the United States;
 - (b) personal or business-related filing for bankruptcy;
 - (c) garnishment of wages;
 - (d) legal action effected for name change;
 - (e) change in citizenship;
 - (f) employment by, representation of, or other business-related association with a foreign or foreign-owned interest or foreign national, and
 - (g) hospitalization or other treatment for a mental illness; treatment for drug abuse; or treatment for alcohol abuse.
- (3) Notify the cognizant DOE personnel security office or the facility security officer, as appropriate, immediately after any approach or contact by any individual seeking unauthorized access to classified matter or SNM. If such an approach or contact is made while on foreign travel, notify a Department of State official at the local United States Embassy or Consulate with a request that the Department of State report the incident to the Director, Office of Security, at DOE Headquarters. These requirements are in addition to any similar reporting requirements implemented under other DOE Orders or regulations.
- (4) Provide to the cognizant DOE personnel security office a completed DOE F 5631.34, "Data Report on Spouse/Cohabitant," in accordance with DOE M 472.1-1B.

6. CONTACT. Contact the Personnel Security Policy Program Manager at 301-903-6637 for assistance.

BY ORDER OF THE SECRETARY OF ENERGY:



KYLE E. McSLARROW
Deputy Secretary

**DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH
DOE O 472.1C, *Personnel Security Activities* IS APPLICABLE**

Office of the Secretary
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Independent Oversight and Performance Assurance
Office of the Inspector General
Office of Intelligence
Office of Management, Budget and Evaluation and Chief Financial Officer
National Nuclear Security Administration
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Secretary of Energy Advisory Board
Office of Security
Office of Worker and Community Transition
Office of Energy Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 472.1C, *Personnel Security Activities*

This Contractor Requirements Document (which is equivalent to the *National Industrial Security Program Operating Manual*, Chapter 2, Section 2, “Personnel Clearances”) prescribes requirements, restrictions, and other procedures necessary for Department of Energy (DOE) and National Nuclear Security Administration contractors to:

- prevent the unauthorized disclosure of classified matter;
- protect special nuclear materials (SNM); and
- control the authorized disclosure of classified matter released by DOE and other Federal agencies.

The Atomic Energy Act of 1954, as amended, provides the statutory basis for DOE’s Personnel Security and Personnel Security Assurance Programs, which encompass sets of activities for determining an individual’s eligibility for access to Restricted Data and SNM.

Executive Orders 10865, 12829, 12958, and 12968 establish DOE authority to determine an individual’s eligibility for access to other classified matter and to promulgate requirements for contractors to protect classified matter.

1. GENERAL REQUIREMENTS.

- a. Requests for access authorization shall not be submitted until the contractor has been awarded a DOE contract and has submitted to DOE the required paperwork for a Foreign Ownership, Control, or Influence (FOCI) determination.
- b. Access authorization requests may be submitted to DOE pending completion of the FOCI determination; however, a favorable FOCI determination must be rendered by DOE before an access authorization will be granted, reinstated, continued, extended, or transferred for the contractor’s applicant for employment (hereafter referred to as “applicant”) or employee.
- c. An access authorization request shall be submitted to DOE only after the contractor’s determination that the access authorization is essential for the individual to perform tasks or services stipulated in contract provisions (i.e., for an applicant or employee selected to occupy a position that requires the incumbent to access classified matter and/or SNM in order to perform work under the contract).
- d. An access authorization shall not be requested or continued to:
 - (1) allow the dissemination of classified matter on other than a need-for-access basis;

- (2) preclude the use of access controls or physical barriers to distinguish perimeters among security areas or between security areas and open areas;
 - (3) determine an individual's suitability for employment;
 - (4) alleviate responsibilities for escorting uncleared individuals within a security area;
 - (5) establish a pool of cleared employees; or
 - (6) accommodate an individual's personal convenience, expedience, gain, advantage, or anticipation of unspecified classified work.
- e. An access authorization shall be requested (or recertified as continuing to be needed) only when required, and only for the type (Q or L, see paragraph 2 below) required, to avoid the unnecessary expenditure of DOE resources and the unwarranted invasion of an individual's privacy.
- f. Individual access to classified matter or SNM shall not be permitted until notification has been received from DOE that access authorization has been granted, reinstated, extended, or transferred. Verbal notification from a DOE personnel security official may be accepted, to be followed by written confirmation of the action.
- g. Except as authorized by DOE in paragraph 6 below, access authorizations shall be requested only for individuals who are United States citizens and over 18 years old.
- h. Only authorized DOE employees can render a formal access authorization determination (such as eligibility and termination); however, contractors are authorized to effect actions that affect an individual's access, such as restricting access to classified matter or SNM when access eligibility terminates or obtaining a "Security Termination Statement" prior to the individual's departure.
- i. Logistical assistance shall be provided to DOE and investigative agencies, as reflected in paragraph 4, for the conduct of initial investigations and periodic reinvestigations, and for reinvestigations that are conducted when DOE determines that an employee may have been engaged in an activity or subject to circumstances that affect continued access authorization eligibility.
- j. DOE retains authority in all matters related to DOE personnel security activities, and personnel security activities are not subject to collective bargaining between contractor management and labor.
- k. An individual's active access authorization status shall not be used as a determining factor for hiring, entering into a consultant agreement, or awarding a subcontract.

- l. DOE personnel security requirements and procedures shall not be used by contractor management or other employees to coerce, restrain, threaten, intimidate, or retaliate against individuals for exercising their rights under any statute, regulation, or DOE directive.
 - m. Unless otherwise stipulated, the contractor shall not be required to reimburse DOE for DOE costs associated with processing the contractor's applicants or employees for investigations or other actions related to access authorization.
 - n. Access authorizations shall be requested and maintained at the minimum number necessary to ensure operational efficiency, and shall be terminated as required in paragraph 7 below.
2. ACCESS AUTHORIZATION DETERMINATION REQUIREMENTS. When the duties of a position will require the incumbent to access DOE classified matter and/or SNM, the contractor shall process the selectee for either a DOE Q or L access authorization if the selectee does not already possess the appropriate type of DOE access authorization. The type of access authorization to be requested will depend on the category (Restricted Data, Formerly Restricted Data, or National Security Information) and level (Top Secret, Secret, or Confidential) of classified matter and/or category of SNM (I, II, III, or IV) to which the incumbent will require access.
- a. For Access to Classified Matter.
 - (1) Q Access Authorization shall be requested when the duties of the position require access to any of the following:
 - (a) Top Secret or Secret Restricted Data;
 - (b) Top Secret Formerly Restricted Data;
 - (c) Top Secret National Security Information; or
 - (d) Classified matter designated as "COMSEC," "CRYPTO," "Sensitive Compartmented Information," or Weapon Data, Sigma 14 or Sigma 15.

[NOTE: A Q access authorization also allows the individual access to the categories/levels of classified matter listed in paragraph 2a(2) below.]
 - (2) L Access Authorization shall be requested when the duties of the position require access to any of the following:
 - (a) Confidential Restricted Data;
 - (b) Secret or Confidential Formerly Restricted Data; or
 - (c) Secret or Confidential National Security Information.

- b. For Access to SNM. DOE M 473.1-1, Physical Protection Manual, Chapter II, Table 1 provides access authorization descriptions. [NOTE: An access authorization granted for SNM also allows the individual access to the appropriate categories/levels of classified matter on a need-to-know basis.]
- (1) Category I. Q access authorization. [NOTE: Hands-on access to or transportation of Category I quantities may require additional measures, such as Personnel Security Assurance Program or Personnel Assurance Program (see DOE O 452.2B, *Safety of Nuclear Explosive Operations*) participation and/or enhanced nuclear material surveillance procedures to further reduce the probability of an insider act.]
 - (2) Category II with Credible Roll-Up to Category I. Q access authorization.
 - (3) Categories II and III. An L access authorization unless special circumstances determined by a site vulnerability assessment, and documented in the site safeguards and security plan, require a Q access authorization.
 - (4) Category IV. None unless special circumstances determined by a site vulnerability assessment, and documented in the site safeguards and security plan, require an access authorization to minimize risk.

3. PRE-EMPLOYMENT AND PRE-PROCESSING REQUIREMENTS.

- a. The following statement shall be included in advertisements for positions that require the selectees to be processed for an access authorization: “Applicants selected will be subject to a Federal background investigation and must meet eligibility requirements for access to classified matter.” The statement may be modified, as appropriate, to reflect access to SNM and/or that additional reviews and/or testing procedures are required for selectees to Personnel Security Assurance Program or Personnel Assurance Program positions.
- b. The contractor shall require applicants and employees selected for positions requiring access authorizations to provide evidence of United States citizenship and shall verify such evidence to DOE when requesting that the individuals be processed for access authorizations. (See paragraphs 3d and 4a below.) [NOTE: The contractor is **not** required to obtain and verify to DOE evidence of United States citizenship if the individual was previously granted access authorization and was a United States citizen when the access authorization was granted.] Acceptable evidence of United States citizenship consists of the following:
- (1) For an individual born in the United States, a birth certificate is the primary and preferred means of citizenship verification. Acceptable certificates must show that the birth record was filed shortly after birth and it must be certified with the registrar’s signature. It 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 1 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 or circumcision 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 shall be original or certified.

- (2) For an individual claiming citizenship by naturalization, a certificate of naturalization that reflects the individual's name is required.
 - (3) For an individual claiming citizenship acquired by birth abroad to a United States citizen, one of the following (reflecting the individual's name) is required:
 - (a) a Certificate of Citizenship issued by the Immigration and Naturalization Service;
 - (b) a Report of Birth Abroad of a Citizen of the United States of America (Form FS-240); or
 - (c) a Certificate of Birth (Form FS-545 or DS-1350).
 - (4) A United States passport, current or expired.
 - (5) A Record of Military Processing—Armed Forces of the United States (DD Form 1966), provided it reflects that the individual is a United States citizen.
- c. When an access authorization will be required for an applicant or employee, the contractor shall conduct the following checks, as appropriate, to establish the individual's job qualifications and suitability before submitting the access authorization request to DOE:
- (1) a credit check;
 - (2) verification of a high school degree or diploma or a degree or diploma granted by an institution of higher learning within the past 5 years;
 - (3) contacts with listed references;

- (4) contacts with listed employers for the past 3 years (excluding employment of less than 60 days duration, part-time employments, and craft/union employments);
 - (5) local law enforcement checks when such checks are not prohibited by State or local law, statute, or regulation, and when the individual has resided in the jurisdiction where the contractor is located.
- d. The results of the checks conducted in the paragraph above shall be verified to DOE with the individual's security forms, verification of United States citizenship as required in paragraph 4a, and a statement that all information concerning the individual has been favorably reviewed in accordance with the contractor's personnel policies. The following information shall be provided to DOE for each check conducted by the contractor:
 - (1) the date the check was conducted;
 - (2) the identity of the individual, office, or entity that provided the information; and
 - (3) a synopsis of the information provided to the contractor.
- e. An applicant hired specifically for a position that will require an access authorization shall not be placed in that position until the access authorization has been granted by DOE unless an exception has been obtained from the head of the contracting activity or designee.
- f. The contractor shall not conduct the checks or provide verifications to DOE stipulated in paragraphs 3c and 3d for:
 - (1) individuals who hold a DOE access authorization or a security clearance granted by another Federal agency;
 - (2) Federal employees (including members of the Armed Forces) detailed or assigned to the contractor; or
 - (3) an employee previously granted an access authorization or a security clearance at the contractor's request that was subsequently terminated because it was no longer needed, if the individual has been continuously employed by the contractor since that time.
- g. The contractor shall not concurrently process an applicant or employee for an access authorization and a security clearance with another Federal agency. If an applicant or employee is selected to occupy a position that will require both a DOE Q access authorization and another agency Top Secret security clearance, the request for a Q access authorization shall first be submitted to DOE. After DOE has granted a Q access authorization, the contractor should then request the other

agency Top Secret security clearance for the individual, noting the date DOE granted a Q access authorization and the individual's DOE personnel security file number. When the other agency receives the contractor's request, the individual's security forms, and DOE access authorization information, it will coordinate with DOE to obtain information necessary for granting the Top Secret security clearance. The same procedure shall be followed for an individual who will require both a DOE L access authorization and another agency Secret security clearance. For dissimilar types of access (e.g., Q and Secret, or L and Top Secret), concurrent DOE and other agency requests may be processed. Further implementation guidance concerning this requirement may be obtained from the cognizant DOE office.

- h. An individual who claims dual citizenship may be processed for DOE access authorization as a foreign national. Further guidance concerning this issue may be obtained from the cognizant DOE office.

4. PROCESSING ACCESS AUTHORIZATION REQUESTS TO DOE.

- a. Access authorization requests shall be forwarded through established channels to the cognizant DOE office. Requests shall include the following documentation (additional documentation may be required by the cognizant DOE office):

- (1) A cover letter or form (if one is provided by the cognizant DOE office) that requests Q or L access authorization and provides justification for access authorization processing. The justification shall describe in detail (without revealing classified information) the duties of the position and the category(ies)/level(s) of classified matter and/or category of SNM to be accessed. The contractor shall also identify any other Federal agency access authorization or security clearance that has been granted to the individual at the contractor's request.

NOTE: General statements such as "Access authorization is required to perform contractual duties," or "Access authorization is required in support of Contract Number _____," are unacceptable, as are statements that corporate policy requires all applicants or employees to be processed for access authorizations. The following represents an acceptable justification: "Mr./Ms. ____ is a computer systems engineer with ABC, Inc., and 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 Restricted Data. Contract No ____."

- (2) Verification of the individual's evidence of United States citizenship.
- (3) Required security forms, usually a Standard Form 86, fingerprint cards, and a DOE Security Acknowledgment. [NOTE: Security forms and

instructions shall be provided by the cognizant DOE office. When the duties of the position will involve access to Special Access Programs, information classified as “Top Secret,” or classified matter designated as “Sensitive Compartmented Information,” “CRYPTO,” or “Weapon Data,” the individual may be required to file financial disclosure reports, copies of which shall be provided by the cognizant DOE office.]

- (4) Verification that pre-processing checks have been conducted as indicated in paragraph 3d above.
 - (5) The DOE contract or subcontract number under which access authorization is being requested.
- b. Contractor shall advise their employees and applicants for employment that their completed security forms will be reviewed by designated contractor employees for completeness prior to submission to DOE. The contractor may elect to maintain, or not 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 shall 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, his/her security forms that are maintained by the contractor. The contractor shall recommend to the individual that he/she maintain copies of the completed security forms for his/her personal records. NOTE: The cognizant DOE office shall establish local procedures governing contractor access to the completed Part 2 of the Standard Form 86.
- c. Written procedures shall be established for the protection of access authorization information, including the procedures for—
- (1) designating the employees responsible, and trained in the procedures, for reviewing the individual’s completed security forms prior to their submission to DOE; and
 - (2) informing all employees with access to completed security forms, pre-employment or pre-processing check information, and other access authorization related information of their responsibility to protect the information from unauthorized disclosure.
- d. When deficient access authorization requests are returned to the contractor with an indication of the deficiency(ies), the contractor shall ensure that the deficiency(ies) is (are) corrected and return the request to the cognizant DOE office for processing. The contractor shall ensure that the individual being processed for an access authorization is not provided access to classified matter or SNM until the cognizant DOE office notifies the contractor that an access authorization has been granted, reinstated, extended, or transferred. Verbal

notification of the access authorization action from the cognizant DOE office will be confirmed by a DOE written notification.

- e. Contractor shall assist in the timely processing of access authorization actions by:
 - (1) cooperating with investigative agency and DOE requests for access to the individual's contractor employment or personnel information (such requests shall be accompanied by an appropriate release signed by the individual);
 - (2) ensuring the availability of the individual for the conduct of personal interviews by investigative agency or DOE personnel security staff; and
 - (3) ensuring that other employees are made available to provide background information during the conduct of initial investigations and reinvestigations.
- f. Contractor is responsible for reviewing, approving, and submitting to DOE access authorization requests for their subcontractor, consultant, or agent applicants or employees. Such requests shall be kept to a minimum in accordance with DOE requirements.

5. INTERIM ACCESS AUTHORIZATION (IAA) REQUEST.

- a. The contractor may request that an individual who is being processed for a Q access authorization also be processed for an IAA based on the following justification:
 - (1) serious delay of or interference in a DOE program may be experienced unless the named individual is granted an access authorization prior to the completion of full access authorization procedures; and
 - (2) the services of a qualified person with an active Q access authorization cannot be obtained.

[NOTE: Specific information substantiating the justification must be provided.]

- b. The IAA request shall accompany the required documentation in paragraph 4a above.
- c. Individuals processed for an IAA may be asked to voluntarily participate in the DOE Accelerated Access Authorization Program, which involves psychological, drug, and counterintelligence polygraph testing at the Accelerated Access Authorization Program Center, Albuquerque, New Mexico, or Oak Ridge, Tennessee. Transportation and per diem costs for such processing are the contractor's responsibility. Additional information concerning the Accelerated Access Authorization Program is available from the cognizant DOE office.

- d. The contractor may provide the individual access to classified matter upon receipt of written notification from the cognizant DOE office that the IAA has been approved. DOE shall also notify the contractor if the IAA is not approved. Non-approval of an IAA is not a denial of access authorization and is not appealable. DOE full access authorization procedures will continue in either case.
- e. If an individual's IAA approval is withdrawn by DOE, the contractor shall, upon receipt of verbal notification from the cognizant DOE office, ensure that the individual is precluded from access to classified matter. DOE shall confirm the verbal notification in writing. Withdrawal of an individual's IAA approval by DOE is not a denial or revocation of an access authorization and is not appealable. Withdrawal of an individual's IAA approval does not halt the processing of the Q access authorization request.
- f. If the DOE grants a final Q access authorization, the individual's IAA approval will be withdrawn and the contractor so notified in writing.
- g. The contractor shall not request an IAA for individuals requiring L access authorizations or for foreign nationals.

6. ACCESS AUTHORIZATION REQUEST FOR A FOREIGN NATIONAL.

- a. Contractor shall process a request for an access authorization for a foreign national in accordance with the guidance provided by the cognizant DOE office.
- b. The request shall be made only when the contractor can provide clear evidence that the individual has talents or skills essential to the DOE's mission and not possessed to a comparable degree by an available United States citizen.
- c. The request shall not be processed by DOE if sufficient information cannot be obtained by an investigation to determine the individual's access authorization eligibility.
- d. The contractor shall not provide access to the following types of classified matter to a foreign national granted access authorization:
 - (1) "Top Secret," "CRYPTO," or "COMSEC" information.
 - (2) Intelligence information.
 - (3) Information that has not been determined releasable by a United States Government Designated Disclosure Authority to the country of which the individual is a citizen.
 - (4) NATO Information; however, a foreign national of a NATO member nation may be authorized access to NATO Information provided that:

- (a) a NATO Security Clearance Certificate is obtained by DOE from the individual's home country; and
 - (b) NATO Information access is limited to performance on a specific NATO contract.
- (5) Information for which foreign disclosure has been prohibited in whole or in part.
 - (6) Information provided to the United States Government in confidence by a third party government and classified information furnished by a third party government.

7. REPORTING AND OTHER REQUIREMENTS.

- a. Contractor Reporting Requirements. Except for item (3) below, verbal notification within 2 working days followed by written confirmation within the next 10 working days shall be provided through established channels to the cognizant DOE office of the following conditions affecting an applicant's or employee's access authorization status:
 - (1) when an applicant declines the offer of employment or fails to report for duty;
 - (2) for any reason iterated in paragraph 7c below;
 - (3) when aware of an individual's hospitalization or other treatment for a mental illness or other condition that may cause a significant defect in the individual's judgment or reliability;
 - (4) when made aware of information of personnel security interest. Such information must be characterized as reliable and relevant and create a question as to an individual's access authorization eligibility as exemplified in 10 CFR 710.8 (see the reverse of DOE F 5631.18);
 - (5) when a foreign national under the contractor's cognizance becomes a United States citizen through naturalization or effects any other change in his/her citizenship status; or
 - (6) when the contractor restricts or withdraws an employee's access to classified matter or SNM without DOE direction.
- b. Individual Reporting Requirements. Contractor shall inform employees and applicants who are applying for or granted access authorization that they must:
 - (1) Provide full, frank, and truthful answers to relevant and material questions, and when requested, furnishing or authorizing others to furnish information that DOE deems pertinent to the access authorization

eligibility process. This applies when completing security forms, during the course of an initial investigation and reinvestigations, and at any stage of access authorization processing including but not limited to letters of interrogatory, personnel security interviews, DOE-sponsored mental evaluations, and other authorized DOE investigative activities. An individual may elect not to cooperate; however, such refusal may prevent DOE from granting or continuing access authorization. In this event, any access authorization then in effect may be terminated or further processing may be suspended.

- (2) Provide direct notification to the cognizant DOE office of the following:
[NOTE: Verbal notification is required within 2 working days followed by written notification within the next 3 working days.]
 - (a) all arrests, criminal charges (including charges that are dismissed), or detentions by Federal, State, or other law enforcement authorities for violations of the law, other than traffic violations for which only a fine of \$250 or less was imposed, within or outside of the United States;
 - (b) personal or business-related filing for bankruptcy;
 - (c) garnishment of wages;
 - (d) legal action effected for name change;
 - (e) change in citizenship;
 - (f) employment by, representation of, or other business-related association with a foreign or foreign-owned interest, or foreign national; and
 - (g) hospitalization or other treatment for a mental illness; treatment for drug abuse; or treatment for alcohol abuse.
- (3) Provide notification to the cognizant DOE office or the facility security officer, as appropriate, immediately after any approach or contact by any individual seeking unauthorized access to classified matter or SNM. If such an approach or contact is made while on foreign travel, individuals should notify a Department of State official at the local United States Embassy or Consulate with a request that the Department of State report the incident to the Director, Office of Security, at DOE Headquarters. This requirement is in addition to any similar reporting requirements implemented under DOE Orders or regulations.
- (4) Provide a completed DOE F 5631.34, "Data Report on Spouse/ Cohabitant," directly to the cognizant DOE office within 45 calendar days

of marriage to, or cohabitation with, an individual who does not currently hold access authorization. These forms shall be provided by the cognizant DOE office.

[NOTE: Requirements for the individual to report circumstances of security interest directly to the cognizant DOE office do not preclude the contractor from requiring the individual to also report these circumstances to the contractor's personnel security office or facility security officer.]

- c. Access Authorization Termination Requests. The contractor shall request the cognizant DOE office(s) to terminate an employee's access authorization and shall provide a DOE F 5631.29, "Security Termination Statement," completed by the employee whenever any of the following occur: [NOTE: The purpose of the DOE F 5631.29 is to ensure that the individual is aware of his/her continuing responsibilities to protect classified matter after termination of an access authorization. The cognizant DOE office shall be requested to terminate an employee's access authorization even though a completed DOE F 5631.29 cannot be immediately provided.]
- (1) employment by the contractor is terminated;
 - (2) access authorization is no longer required;
 - (3) the individual is on a leave of absence or on extended leave and will not require access for 90 consecutive calendar days. Upon request, this interval may be adjusted at the discretion of the cognizant DOE office;
 - (4) access to classified matter or SNM is no longer required due to transfer to a position not requiring such access [NOTE: The cognizant DOE office may approve a contractor request for an individual to retain an access authorization when the contractor verifies that the individual shall be reemployed or reassigned by the contractor within the next 3 months in a position that will require an access authorization. The contractor must inform the cognizant DOE office of the individual's employment status at the end of the 3-month interval.]; or
 - (5) the individual leaves for foreign travel, employment, assignment, education, or residence of more than 3 months duration not involving official United States Government business. [NOTE: This requirement applies even if the individual remains employed by the contractor.]
- d. Access Authorization Reinstatement Requests. The contractor shall request the cognizant DOE office to reinstate access authorization for an applicant or employee when the contractor is aware that the individual previously was granted an access authorization. The cognizant DOE office shall advise the contractor whether the individual must complete a new set of security forms or update information that the individual previously provided.

- e. Access Authorization Upgrade Requests. The contractor shall request the cognizant DOE office to upgrade an employee's access authorization from L to Q in accordance with the new access requirements associated with the duties of the position (reference paragraph 2 above). The request shall be accompanied by appropriate security forms and a revised access authorization justification statement, as directed by the cognizant DOE office.
- f. Access Authorization Downgrade Requests. The contractor shall request the cognizant DOE office to downgrade an employee's access authorization from Q to L in accordance with the new access requirements associated with the duties of the position (reference paragraph 2 above). The request shall be accompanied by a revised access authorization justification statement.
- g. Access Authorization Extension Requests. Extension of an access authorization is the process that allows an individual to hold concurrent access authorizations: under the cognizance of two or more DOE offices; under two or more employers; or for one employer under two or more contracts. A Q access authorization can be extended as either a Q or L access authorization, but an L access authorization can only be extended as an L access authorization. The contractor shall request an access authorization extension under the following circumstances:
 - (1) for an applicant who has an access authorization granted by DOE at the request of another employer and who must retain that access authorization in connection with his/her other employment [NOTE: This is a common situation for consultants. A contractor may request an extension for more than one DOE contract.]; or
 - (2) for an employee when the individual will be assigned to perform classified work under more than one DOE contract and must retain the original access authorization in connection with his/her continued work under the first DOE contract.

The contractor's request for access authorization extension shall be accompanied by a written access authorization justification statement and shall reference the individual's full name, and Social Security Account Number, and, if known, DOE personnel security file number and type/date of access authorization. The cognizant DOE office shall advise the contractor if additional security forms are required to effect the extension. The contractor shall ensure that the individual is precluded from access to classified matter or SNM associated with the second contract until notified by the cognizant DOE office that the extension request has been approved. Under the extension process, an employee's access authorization can be terminated under one contract while being maintained in an active status under another contract(s). The contractor shall notify all cognizant DOE offices when the employee no longer requires access authorization under any of the contractor's DOE contracts (reference paragraph 7c above).

- h. Access Authorization Transfer Requests. Transfer of an access authorization is the process that allows an individual's access authorization to be simultaneously terminated under one contract and granted under another contract. A transfer can be effected only for like access authorizations (i.e., Q to Q, or L to L). The contractor shall request an access authorization transfer under the following circumstances:
- (1) for an applicant when the individual has an access authorization granted by DOE at the request of his/her current employer that will be terminated when the individual leaves that employment [NOTE: This action involves a change of employers for the individual.]; or
 - (2) for an employee when the individual will be assigned to perform classified work under a different contract than the one for which he/she was originally granted an access authorization, and will no longer require access to classified matter associated with the original contract. [NOTE: This action involves a change of contracts for the individual under one employer.]

The contractor's request for access authorization transfer shall be accompanied by a written access authorization justification statement and shall reference the individual's full name, Social Security Account Number, and, if known, DOE personnel security file number and type/date of access authorization. The cognizant DOE office shall advise the contractor if additional security forms are required to effect the transfer action. The contractor shall ensure that the individual is precluded from access to classified matter or SNM until notified by the cognizant DOE office that the transfer request has been approved. When applicable, the cognizant DOE office processing the transfer request is responsible for ensuring that the DOE office that originally granted the individual's access authorization is notified to terminate the individual's access authorization associated with his/her previous employment.

- i. Access Authorization Suspension, Revocation, and Denial.
- (1) The cognizant DOE office is responsible for notifying the contractor in writing when an employee's access authorization is suspended. Upon receipt of such notification, the contractor shall ensure that the employee is precluded from access to classified matter and/or categories of SNM requiring an access authorization. The cognizant DOE office is responsible for notifying other DOE offices or Federal agencies where the employee has been approved/certified for access to classified matter. When the security issue(s) concerning the employee's access authorization status has been resolved, the contractor shall be notified in writing by the cognizant DOE office of whether the employee's access authorization has been reinstated or revoked.

- (2) The cognizant DOE office shall notify the contractor in writing when an applicant or employee has been denied access authorization. Upon receipt of such notification, the contractor shall ensure that the individual is precluded from access to classified matter and/or categories of SNM requiring an access authorization.
- (3) Suspension, denial, or revocation of an individual's access authorization does not preclude the contractor from assigning or transferring the individual to duties that do not require an access authorization.

j. Records Maintenance.

- (1) Contractor shall maintain current records which reflect by contract number all employees granted access authorizations. The listing shall include the employee's name, DOE file number, and the date the contractor was notified by DOE that the employee's access authorization was granted, reinstated, extended, or transferred.
- (2) Copies of correspondence to and from the cognizant DOE office(s) that reflect access authorization matters for each applicant and employee shall be maintained, including: the request for access authorization, notification that access authorization action was effected, and access authorization termination actions. Such copies shall be maintained while the individual holds an access authorization at the contractor's request and for a period of 2 years after the date the individual's access authorization is terminated, at which time they may be destroyed.
- (3) All records and information pertaining to applicant and employee access authorization matters, including copies of security forms and information collected from the conduct of preemployment or pre-processing checks, shall be protected against unauthorized disclosure in accordance with the Privacy Act of 1974 (Title 5, United States Code, 552a) and/or DOE directives. Information collected by the contractor for access authorization processing shall not be used by the contractor for any purpose other than that for which it is intended and shall not be provided to non-contractor employees or any other entity or organization without prior approval from the cognizant DOE office.

k. Recertifications and Reinvestigations.

- (1) The contractor shall comply with periodic DOE requests to recertify its employees' access authorization status. Usually, the cognizant DOE office will furnish the contractor with a listing of its applicants and employees who hold or are being processed for access authorizations, and request that the contractor annotate the listing with any corrections or adjustments and return the listing in a timely manner. Recertification, or an examination of

access authorization records, also may be requested during the conduct of a DOE security survey. Specific recertification guidance shall be provided by the cognizant DOE office.

- (2) The contractor shall assist DOE in the conduct of periodic reinvestigations in accordance with guidance provided by the cognizant DOE office (reference paragraph 4e above).
8. PERSONNEL SECURITY ASSURANCE PROGRAM REQUIREMENTS. The contractor shall prepare a Personnel Security Assurance Program (PSAP) Implementation Plan when its site, facility, or an operation is identified as having PSAP Positions, and shall implement the provisions of the PSAP Implementation Plan within 30 working days of its approval. The PSAP Implementation Plan shall reflect the PSAP requirements to which the contractor has agreed (see 10 CFR 710 and related directive requirements).
9. DOE AND NUCLEAR REGULATORY COMMISSION (NRC) ACCESS AUTHORIZATIONS. Both the DOE and the NRC grant Q and L access authorizations. The term “access authorization(s)” in this document refers only to DOE access authorizations.

**ACCESS TO CLASSIFIED MATTER
ALLOWED BY TYPE OF DOE ACCESS AUTHORIZATION
AND INITIAL INVESTIGATION REQUIREMENTS**

TYPES OF CLASSIFIED MATTER AND CLASSIFICATION LEVELS			
Type of DOE Access Authorization	Restricted Data	Formerly Restricted Data	National Security Information
Q* allows access to these levels of classified matter	Top Secret Secret Confidential	Top Secret Secret Confidential	Top Secret Secret Confidential
L** allows access to these levels of classified matter	----- Confidential	Secret Confidential	Secret Confidential
<p>* For an initial DOE Q access authorization, an Office of Personnel Management (OPM) Single-Scope Background Investigation or Federal Bureau of Investigation (FBI) Background Investigation is required. Completed investigations by other agencies can be obtained and used by DOE for determining an individual's Q access authorization eligibility if the scope and extent of the investigation meets DOE specifications.</p>			
<p>** For an initial DOE L access authorization, an OPM Access National Agency Check and Inquiries (ANACI) is required for DOE employees and applicants for employment; and at least an OPM National Agency Check with Law and Credit (NACLC) is required for all other individuals. A more extensive investigation can be used as a basis for determining an individual's L access authorization eligibility. DOE Q access authorization is required for access to Restricted Data or Formerly Restricted Data designated as Weapon Data, Sigma 14 or Sigma 15.</p>			

The type of investigation scheduled with the OPM may be upgraded at the discretion of DOE personnel security officials when information provided by the individual on the security forms, or from other sources, reflects the need to obtain more detailed information than is normally provided as the result of an ANACI or NACLC.

DOE will not normally request a concurrent investigation for an individual who is already being investigated by an agency for personnel security purposes unless the resultant reports of investigation will not be sufficient in scope and extent to use as a basis for determining the individual's eligibility for a DOE access authorization.

**ACCESS TO SPECIAL NUCLEAR MATERIALS
ALLOWED BY TYPE OF DOE ACCESS AUTHORIZATION**

Special Nuclear Materials Category	Type of DOE Access Authorization Required	Remarks
I	Q	Hands-on access or transportation of Category I quantities may require additional measures such as Personnel Security Assurance Program or Personnel Assurance Program participation and/or enhanced material surveillance procedures to further reduce the probability of insider acts.
II with credible roll-up to I	Q	
II and III	L	Unless special circumstances determined by site vulnerability assessment require a Q access authorization to minimize risk. Document in site safeguards and security plan.
IV	None	Unless special circumstances determined by site vulnerability assessment require an access authorization to mitigate risk. Document in site safeguards and security plan.
See Page II-2, DOE M 473.1-1, of 12-23-02, which also defines the SNM Categories.		

POSITIONS OF A HIGH DEGREE OF IMPORTANCE OR SENSITIVITY

When an individual is selected to occupy one of the positions listed below, his/her security forms shall be submitted to the Federal Bureau of Investigation (FBI) for the conduct of a background investigation. DOE shall review the resultant reports of investigation to determine employment suitability and eligibility for an access authorization.

If an individual will occupy a position in DOE requiring confirmation by the United States Senate, an FBI background investigation will be scheduled by the White House staff before the individual's name is sent to the United States Senate for confirmation hearings. After an individual has been confirmed by the United States Senate, DOE will obtain a copy of the FBI reports of investigation.

A. DOE HEADQUARTERS

Secretary of Energy

Deputy Secretary of Energy

Under Secretary of Energy for Energy, Science and Environment

Under Secretary and Administrator for Nuclear Security, National Nuclear Security Administration (NNSA)

Principal Deputy Assistant Administrator, NNSA

Chief, Office of Defense Nuclear Counterintelligence, NNSA

Chief, Office of Defense Nuclear Security, NNSA

Deputy Administrator, Defense Programs, NNSA

Deputy Administrator, Defense Nuclear Nonproliferation, NNSA

Deputy Administrator, Naval Reactors, NNSA

Director, Office of Emergency Operations, NNSA

Assistant Secretary for Congressional, and Intergovernmental Affairs

Director, Office of Counterintelligence

Assistant Secretary for Environment, Safety, and Health

Assistant Secretary for Environmental Management

General Counsel

Director, Office of Hearings and Appeals

Inspector General
Director, Office of Intelligence
Director of Nuclear Energy, Science and Technology
Director, Office of Independent Oversight and Performance Assurance
Assistant Secretary for Policy and International Affairs
Director, Office of Science
Director, Office of Security (SO)
Director, Office of Special Operations, SO
Director, Security Policy Staff, SO
Director, Office of Headquarters Security Operations, SO
Director, Office of Foreign Visits, Assignments and Travel, SO
Director, Office of Operations Support, SO

B. DOE FIELD ELEMENTS

Director, Service Center, Albuquerque
Manager, Chicago Operations Office
Manager, Idaho Operations Office
Manager, Oak Ridge Operations Office
Manager, Y-12 Site Office
Manager, Ohio Field Office
Manager, Pittsburgh Naval Reactors Office
Manager, Richland Operations Office
Manager, Savannah River Operations Office
NNSA Savannah River Site Office
Manager, Schenectady Naval Reactors Office

REFERENCES

1. Title 5, United States Code, 552a, "Privacy Act of 1974," as amended, which establishes the legal requirements for collecting and retaining information on individuals.
2. Title 21, United States Code, 802, "Controlled Substances Act of 1970," which defines illegal drugs.
3. Title 42, United States Code, 2011, et seq., "Atomic Energy Act of 1954, as amended," which provides statutory authority for establishing and implementing a Department of Energy (DOE) security program for controlling access to Restricted Data and special nuclear materials.
4. Title 5, Code of Federal Regulations, Part 732, "National Security Positions," which implements Executive Order 10450 throughout the Federal agencies.
5. Title 5, Code of Federal Regulations, Part 736, "Personnel Investigations," which deals primarily with the conduct of investigations by the Office of Personnel Management.
6. Title 10, Code of Federal Regulations, Part 707, "Workplace Substance Abuse Programs at DOE Sites," which establishes procedures for drug testing in DOE.
7. Title 10, Code of Federal Regulations, Part 710, "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material," which establishes procedures for determining an individual's eligibility for a DOE access authorization (Subpart A) or for occupying a DOE Personnel Security Assurance Program designated position (Subpart B).
8. Title 10, Code of Federal Regulations, Part 725, "Permits for Access to Restricted Data," which establishes procedures and standards for the issuance of Access Permits.
9. Title 10, Code of Federal Regulations, Part 1008, "Records Maintained on Individuals (Privacy Act)," which establishes the procedures to implement the provisions of the Privacy Act of 1974 within DOE.
10. Title 10, Code of Federal Regulations, Part 1016, "Safeguarding of Restricted Data," which establishes requirements for protecting Secret and Confidential Restricted Data received or developed under an access permit.
11. Title 48, Code of Federal Regulations, 970.2201, "Basic Labor Policies," which establishes employment standards for management and operating contractors, including pre-employment check requirements.
12. "Department of Health and Human Services: Mandatory Guidelines for Federal Workplace Drug Testing Programs," which contains requirements for conducting drug testing. *53 Federal Register* 51118-51119, dated 9-30-97.

13. Executive Order 10450, "Security Requirements for Government Employees," dated 4-27-53, as amended, which establishes the requirements for determining that all Federal employees are loyal, reliable, trustworthy, and of good conduct and character.
14. Executive Order 10865, "Safeguarding Classified Information Within Industry," dated 2-20-60, as amended, which establishes the basis for the industrial security program for civilian personnel.
15. Executive Order 12564, "Drug-Free Federal Workplace," dated 9-15-86, which establishes the requirement to conduct drug testing of Federal employees in sensitive positions.
16. Executive Order 12829, "National Industrial Security Program," dated 1-6-93, as amended, which establishes a program to protect Federal classified information released to its contractors, licensees, and grantees.
17. Executive Order 12958, "Classified National Security Information," dated 4-17-95, as amended, which prescribes a uniform system for classifying, protecting, and declassifying national security information.
18. Executive Order 12968, "Access to Classified Information," dated 8-2-95, which establishes a uniform Federal personnel security program for employees who will be considered for initial or continuing access to classified information.
19. Director of Central Intelligence Directive (DCID) No. 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," dated 7-2-98.
20. Department of Defense, *National Industrial Security Program Operating Manual* (DoD 5220.22-M), dated January 1995, and the *National Industrial Security Program Operating Manual Supplement* (DoD 5220-22-M-Sup 1), dated February 1995, which establish minimum security requirements for the protection of classified matter by Government contractors and which replace the Department of Defense *Industrial Security Manual for Safeguarding Classified Information*, dated January 1991.
21. DOE M 473.1-1, Physical Protection Manual, dated 12-23-02, which establishes the requirements for the protection and control of DOE safeguards and security interests, including DOE access authorization requirements for access to Categories I, II, III, and IV of SNM.
22. DOE Integrated Safeguards and Security, "CPCI User Guide," dated March 2000, which establishes for system users the system requirements, operations, and data input procedures for the Central Personnel Clearance Index and other system components.
23. Office of Safeguards and Security, "Glossary of Terms," dated 12-18-95, which contains Safeguards and Security Program, National Industry Security Program, and related terms and definitions.