

U.S. Department of Energy
Washington, D.C.

ORDER

DOE O 472.1A

Approved: 9-05-96

Sunset Review: 9-05-98

Expires: 9-05-00

SUBJECT: PERSONNEL SECURITY ACTIVITIES

1. **OBJECTIVES.** In accordance with Federal statutes, Executive orders, and Departmental regulations, establishes requirements to do the following:
 - a. Ensure that individuals are processed for, granted, and maintain 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;
 - (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 individual access authorizations to confirm eligibility for continued access and the need for access.
 - f. Ensure that DOE employees, contractors, and others involved in personnel security activities effectively and efficiently execute their personnel security related responsibilities and authorities.

Distribution:
All Departmental Elements

Initiated by:
Office of Nonproliferation
and National Security

- g. Prevent the use of personnel security activities for reprisal, discrimination, or any other unauthorized purpose.
 - h. Promote proactive participation in personnel security activities at the international, national, and inter-agency levels to ensure the adequate expression and consideration of DOE mission and program interests.
- 2. CANCELLATION. DOE O 472.1, PERSONNEL SECURITY ACTIVITIES, dated 9-25-95, is canceled. Cancellation of an Order does not, by itself, modify or otherwise affect any contractual obligation to comply with such an Order. Canceled Orders that are incorporated by the reference in a contract shall remain in effect until the contract is modified to delete the reference to the requirements in the canceled Orders.
- 3. APPLICABILITY. The provisions of this Order apply as follows:
 - a. DOE Elements.
 - (1) DOE Access Permittees, through the process of issuing Access Permits under Title 10, Code of Federal Regulations, Parts 725 and 1016.
 - (2) Other individuals who require DOE access authorizations in order to be afforded access to DOE classified matter and/or SNM.
 - b. Contractors. DOE contractors, and subcontractors at any tier, whose employees, consultants, and agents require access to DOE classified matter and/or SNM to perform work for DOE. Covered contracts shall contain a security clause or other provision that ensures compliance with the requirements of this Order. Attachment 1, the Contractor Requirements Document, sets forth requirements that are to be applied. Contractor compliance with the CRD will be required to the extent set forth in a contract. Contractors shall be directed to continue to comply with the requirements of Orders cancelled by this Order until their contracts are modified to delete the reference to the requirements of the canceled Orders.
- 4. REQUIREMENTS. Definitions of commonly-used terms are provided in the Safeguards and Security Definitions Guide, and selected definitions are also set forth in sections 710.5 (Subpart A) and 710.54 (Subpart B) of Title 10, Code of Federal Regulations, Part 710, hereafter referred to as "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 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 designated 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, Chapters I-IX of DOE 5631.2C, 10 CFR 710, or other DOE Orders or Manuals; e.g., DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM . (See Attachment 2, "Access to Classified Matter Allowed by Type of DOE Access Authorization and Initial Investigation Requirements" and "Access to SNM 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 which 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 Chapters I-IX of DOE 5631.2C, only United States citizens are eligible for access authorization.
- (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 Departmental funds and 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 any level of classified matter designated as "Top Secret," "CRYPTO," "COMSEC," or "Sensitive Compartmented Information."

- (7) An individual's DOE access authorization status shall not be a determining factor for DOE or DOE contractor employment, or used as a criteria in evaluating or deciding the award of a DOE contract.
- (8) Access authorizations shall not be processed (i.e., requested, granted, continued, reinstated, transferred, or extended) to:
 - (a) Allow the dissemination of classified matter on other than a need-for-access basis;
 - (b) Preclude 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 pools of cleared employees;
 - (e) Accommodate an individual's personal convenience, expedience, gain, or advantage, or in 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 specifically 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 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;
 - (c) If insufficient, incorrect, or conflicting information is provided; or
 - (d) If the forms are illegible.

- (10) As a condition of access authorization approval, individuals shall 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) An individual shall not be granted access authorization for certain types of classified matter stipulated in Chapters I-IX of DOE 5631.2C, nor be allowed to occupy a position designated as requiring such access authorization, unless the individual:
 - (a) Files with the Secretary or designee a financial disclosure report, including information with respect to the individual's spouse and dependent children, as part of all background investigations and reinvestigations;
 - (b) Is subject to annual financial disclosure requirements, if selected by the Secretary or designee; and
 - (c) Files relevant information concerning foreign travel, as determined by the Security Policy Board under Executive Order 12968.
- (12) Except as authorized by the Director of Security Affairs, the determination to grant or reinstate access authorization shall be based on the favorable review of an investigation and report conducted for DOE by the Office of Personnel Management or the Federal Bureau of Investigation, or provided to DOE by another agency.
- (13) DOE shall take all reasonable measures to obtain existing investigative reports that may fulfill Departmental standards and specifications for the scope and extent of investigations, as established by the Secretary, for use as a basis to determine an individual's access authorization eligibility.
- (14) DOE shall, whenever possible, grant access authorizations based upon the interagency reciprocity procedures in Chapters I-IX of DOE 5631.2C.
- (15) DOE shall not submit a request for investigation to the Office of Personnel Management or Federal Bureau of Investigation 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.

- (16) 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 Chapters I-IX of DOE 5631.2C.
- (17) 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 governors and lieutenant governors.
- (18) A Foreign Ownership, Control, or Influence 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.
- (19) 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. 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.
- (20) 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.)
- (21) DOE employees authorized to render access authorization eligibility determinations shall receive training in decision-making prior to actually rendering such determinations.
- (22) All individuals processed for access authorizations shall be treated equally, regardless of their employment status, to preclude the appearance, inference, or practice partiality or favoritism.
- (23) 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.

- (24) Except as authorized by the Director of Security Affairs, individuals with access authorizations shall be periodically reinvestigated as stipulated in Chapters I-IX of DOE 5631.2C.
 - (25) DOE security officials have the authority to request updated security forms in the course of the Reinvestigation Program, or at any time when there is probable cause that the individual has engaged in an activity, or is subject to circumstances, that may affect continued access authorization eligibility.
 - (26) 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 Departmental programs or activities to be held responsible for the reimbursement of such costs.
 - (27) 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.
 - (28) DOE shall maintain, as stipulated in Chapters I-IX of DOE 5631.2C, a Personnel Security File, in either paper or electronic form, for all individuals processed for access authorization.
 - (29) DOE shall maintain a data management system for the timely recording of all access authorization transactions.
 - (30) In all matters related to personnel security activities, DOE retains absolute authority. The procedures in this Order, Chapters I-IX of DOE 5631.2C, and 10 CFR 710 are not subject to collective bargaining between Federal and contractor management and labor.
- c. Deviations. Requests for deviations from the requirements in this Order and Chapters I-IX of DOE 5631.2C shall be processed in accordance with 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 designated positions under subsections 710.55(a) and (b) of 10 CFR 710, Subpart B.
- (3) Submit requests for interim access authorizations to the Director of Security Affairs, through the Director of Safeguards and Security, in accordance with Chapters I-IX of DOE 5631.2C.
- (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 the access authorization requirement is 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 of Safeguards and 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 and the National Aeronautics and Space Administration;
 - (b) Employees, consultants, or agents of DOE contractors and subcontractors;
 - (c) Foreign nationals (refer to Chapters I-IX of DOE 5631.2C); 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 of Safeguards and Security.
 - (8) Provide written notification to the Director of Safeguards and 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.
 - (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 section 710.8 of 10 CFR 710 (a copy of which may be obtained from the Director of Safeguards and Security).
 - (9) Ensure that individuals under their cognizance who have been granted, or are in process for, access authorization are aware of the reporting requirements in subparagraphs 5p and 5q 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 Chapters I-IX of DOE 5631.2C. Unless such designation is made, procurement originators shall be responsible for coordinating the requirements of this Order and Chapters I-IX of DOE 5631.2C with the Director of Safeguards and Security.
- b. Director of Nonproliferation and National Security, through the Director of Security Affairs and the Director of Safeguards and Security, provides management direction and coordination in the development and

implementation of the comprehensive Safeguards and Security Program.

(1) Director of Security Affairs.

- (a) 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. (Delegation Order 0204-139, of 12-20-91.)
- (b) Acts as the Secretary's special designee to determine whether statements or evidence may be received by a Hearing Officer in accordance with subsections 710.26(l)(2) and 710.26(o)(1),(2) of 10 CFR 710.
- (c) Renders final determinations to grant or deny, or reinstate or revoke, DOE access authorizations under subsections 710.28(e) and (f) and performs other specific responsibilities under 10 CFR 710.
- (d) Promulgates and establishes safeguards and security policies, procedures, standards, and guidance for the PSAP and Personnel Security Program.
- (e) Authorizes field elements to implement, operate, and maintain Personnel Security Program activities as prescribed in this Order and Chapters I-IX of DOE 5631.2C.
- (f) Implements Headquarters Personnel Security Program activities.
- (g) 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.
- (h) Authorizes field elements annually to submit requests for investigations, on a scheduled basis, directly to the Office of Personnel Management and the Federal Bureau of Investigation within a specifically allocated total dollar amount, and/or total number of investigations by type.

- (i) Approves any adjustments to field element annual investigations allocations.
- (j) Coordinates with the Office of Personnel Management and Federal Bureau of Investigation on matters related to reimbursable costs for investigations and approves such reimbursements from Departmental funds.

(2) Director of Safeguards and Security.

- (a) Develops rules and directives for the PSAP and Personnel Security Program.
- (b) Performs all responsibilities specified in, and provides recommendations (as appropriate) to the Secretary or Director of Security Affairs on the disposition of cases processed under 10 CFR 710.
- (c) Approves requests to initiate access authorization processing on foreign nationals.
- (d) Reviews, evaluates, and recommends to the Director of Security Affairs approval of requests to authorize access to DOE classified matter and/or SNM prior to, or in lieu of, completion of required investigations.
- (e) Enters into Memoranda of Agreement or Understanding to allow and control access to DOE Personnel Security and Administrative Review Files, and/or access authorization data bases by representatives of DOE elements or other Federal agencies.
- (f) Establishes and manages a centralized automated information system to record all DOE access authorization transactions.
- (g) 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.
- (h) 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.

- (i) Conducts interagency liaison with the Office of Personnel Management and the Federal Bureau of Investigation on all personnel security activities and notifies these agencies of the cancellation of requests for investigation in Headquarters cases.
- (j) Represents DOE in interagency efforts related to personnel security activities.
- (k) Initiates investigation of spouses of all individuals who marry after being processed for access authorization.
- (l) Initiates investigations and grants DOE access authorizations for Restricted Data for Department of Defense and National Aeronautics and Space Administration personnel assigned for duty with DOE or a DOE contractor, or with other Federal agencies.
- (m) Initiates investigations and grants DOE access authorizations to other Federal agency personnel when required.
- (n) Accepts properly executed security clearance certifications for Department of Defense and National Aeronautics and Space Administration personnel assigned for duty with DOE who require access to DOE classified matter and/or SNM.
- (o) Updates periodically the list of DOE "positions of a high degree of importance or sensitivity." (See Attachment 3.)
- (p) 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.
- (q) Conducts periodic program reviews, as directed or requested, of Headquarters and field element personnel security activities to ensure uniform, fair, and objective implementation and application of the requirements in this Order, Chapters I-IX of DOE 5631.2C, and 10 CFR 710.

- (r) 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.
- (s) Retains duplicate Personnel Security Files at Headquarters on selected field element officials as indicated in Chapters I-IX of DOE 5631.2C, and for all foreign nationals with a DOE access authorization.
- (t) Develops and/or approves all forms used in implementing personnel security activities.
- (u) Reviews PSAP Implementation Plans and subsequent changes for consistency with policy.
- (v) Develops and provides training curricula and materials for implementing PSAP.
- (w) Provides research and analysis in PSAP-related activities.
- (x) Provides Office of Contractor Employee Protection staff with access to personnel security files and data during any investigation into reprisal complaints alleging abuses of the personnel security requirements or procedures; and notifies the Inspector General of any reprisal complaint alleging improper conduct involving any Office of Nonproliferation and National Security official.
- (y) Executes the following personnel security management functions for DOE Headquarters, Energy Technology Centers, Power Marketing Administrations, and the Strategic Petroleum Reserve Project Office:
 - 1 Implements and administers PSAP and Personnel Security Program activities consistent with this Order, Chapters I-IX of DOE 5631.2C, and 10 CFR 710.
 - 2 Performs responsibilities in this Order assigned to Managers (except those that reflect a reporting, processing, or referral requirement to the Director of Safeguards and Security).

- c. General Counsel.
 - (1) Performs responsibilities in 10 CFR 710, Subpart A, for Headquarters Administrative Review cases.
 - (2) Reviews Administrative Review cases for legal sufficiency prior to a final determination by the Director of Security Affairs when the Hearing Officer and the Director of Hearings and Appeals are of one opinion, and the Director of Security Affairs is of the opposite opinion.
- 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. Director of Naval Nuclear Propulsion Program implements and oversees all policy and practices pertaining to this Order and Chapters I-IX of DOE 5631.2C for activities under the Director's cognizance.
- g. Director of Contractor Employee Protection investigates reprisal complaints alleging abuses of the personnel security requirements or procedures.
- h. Headquarters Servicing Personnel Offices.
 - (1) Process and transmit to the Director of Safeguards and Security all access authorization requests received from Headquarters Departmental 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 of Safeguards and Security.
- i. Managers of the Albuquerque, Chicago, Idaho, Nevada, Oakland, Oak Ridge, Richland, and Savannah River Operations Offices, the Rocky Flats Field Office, and the Pittsburgh and Schenectady Naval Reactors Offices 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 of Safeguards and 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 of the Plan's approval.
- (4) Approve PSAP Implementation Plan changes and notify the Director of Safeguards and Security of such changes.
- (5) Recommend to the Director of Safeguards and 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.

j. Managers of the Albuquerque, Chicago, Idaho, Nevada, Oakland, Oak Ridge, Richland, and Savannah River Operations Offices, the Rocky Flats Field Office, and the Pittsburgh and Schenectady Naval Reactors Offices 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, Chapters I-IX of DOE 5631.2C, and 10 CFR 710.
- (2) Ensure that training complies with the requirements in Chapters I-IX of DOE 5631.2C.
- (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 type of investigation to be conducted;
 - (b) Ensure that justification and security forms are adequate and complete;
 - (c) Verify that requests from Management and Operating contractors are accompanied by the preemployment checks

required by 48 CFR 970.2201(b)(1)(ii) and that all contractor requests are accompanied by a certification of United States citizenship (see Attachment 1);

- (d) Establish a Personnel Security File for the individual and enter appropriate data into the DOE data management system;
 - (e) Determine whether current investigative reports exist that can be obtained by DOE for determining the individual's access authorization eligibility; and
 - (f) Determine whether the individual is being concurrently processed for an access authorization or security clearance by another agency.
- (4) Initiate directly with the Office of Personnel Management and the Federal Bureau of Investigation requests for initial investigations, reinvestigations, supplemental/additional/upgrade investigations, and the cancellation of investigations in progress.
- (5) Implement procedures to require DOE and DOE contractor supervisors under their cognizance to provide the following:
- (a) Verbal notification to a designated DOE personnel security official within 8 working hours of becoming aware of information that an individual who has been granted, or is in process for, a DOE access authorization has been hospitalized or is otherwise being treated for a mental illness or such other condition as may cause a significant defect in their judgment or reliability. Verbal notification shall be confirmed in writing within 2 working days.
 - (b) Written notification to a designated DOE personnel security official within 2 working days of becoming aware of derogatory information of personnel security interest concerning an individual who has been granted, or is in process for, a DOE access authorization. Such information is characterized as reliable and relevant and as creating a question as to an individual's DOE access authorization eligibility, as exemplified in section 710.8 of 10 CFR 710.
- (6) Request the Director of Safeguards and Security to approve initiation of investigations on foreign nationals under their cognizance proposed for employment in positions requiring DOE access authorization.

- (7) Refer to the Director of Safeguards and Security for processing requests for DOE access authorizations for other Federal agency personnel.
Note: Access authorization processing for local Office of Personnel Management investigators may be coordinated directly between DOE field element and the local Office of Personnel Management supervisor. After such individuals have been granted access authorization, the field element is responsible for ensuring compliance with reinvestigation requirements and data entry/maintenance requirements to update the data management system.
- (8) Provide to the Director of Safeguards and Security for processing "Data Report on Spouse" forms completed by personnel under their cognizance who marry after having been granted, or while being processed for, DOE access authorization.
- (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 other agency security clearance 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 other agency security clearance for access to National Security Information, in accordance with the stipulations in Chapters I-IX of DOE 5631.2C.
- (11) Render a favorable Foreign Ownership, Control, or Influence determination for covered contractors prior to taking a final access authorization action.
- (12) Transmit to the Director of Safeguards and Security requests for interim access authorization for approval by the Director of Security Affairs.
- (13) Delegate authorities and responsibilities in writing to all DOE employees conducting program activities covered by this Order, Chapters I-IX of DOE 5631.2C, or 10 CFR 710, and maintain a current record of the following: (Note: Written delegation may be in the form of the duties listed in an individual's official position description.)
 - (a) DOE employees authorized to grant, continue, extend, reinstate, transfer, upgrade, and/or terminate access authorizations.
 - (b) DOE and DOE support contractor employees authorized to review Personnel Security Files.

- (c) DOE and DOE support contractor employees authorized to access data contained in the DOE data management system.
- (14) Grant, continue, extend, reinstate, transfer, upgrade, 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
 - (b) Grant, reinstate, deny, or revoke an access authorization when the individual does not request a hearing before a DOE Hearing Officer.
- (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, denied, revoked, reinstated, granted, or terminated under 10 CFR 710 procedures.
- (18) Accept investigations and reports on the character, associations, and loyalty of individuals made by the Office of Personnel Management, Federal Bureau of Investigation, or another Federal agency that conducts personnel security investigations, provided that such investigations meet the scope and extent of DOE standards and were completed within the most recent 10 years and updated, as a minimum, with at least a National Agency Check in the most recent 5 years. (Refer to Chapters I-IX of DOE 5631.2C for acceptable variations of this requirement.)
- (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 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 relevant data on individuals processed for access authorization.

- (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 of the Privacy Act.
- (22) Ensure that all access authorization transactions effected for individuals under their cognizance are accurately recorded in the 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 of Safeguards and Security approval for the use of locally-generated forms in personnel security activities.
- (26) Ensure that all individuals under their cognizance performing personnel security activities are aware of the policy that prohibits reprisal or discrimination against any individual who has made a protected disclosure or engaged in protected activities.

k. PSAP Approving Officials.

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

l. 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 incumbents in, and applicants for, PSAP positions in accordance with 10 CFR 707.
- (3) Ensure that supervisory reviews and medical assessments are conducted and make recommendations on PSAP applicants and employees pursuant to 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 designated employee.

m. Site Occupational Medical Directors.

- (1) Conduct annual medical examinations of PSAP designated employees and initial medical examinations of applicants for PSAP positions as provided for in DOE medical standards for management.
- (2) Review and take appropriate action regarding referrals for unusual conduct of PSAP designated employees.
- (3) Recommend to the appropriate management official and PSAP Approving Official the temporary reassignment to non-PSAP duties of a PSAP designated employee in the event that the Site Occupational Medical Director becomes aware of a condition or circumstance that may affect the employee's judgment or reliability (see Section 710.8 of 10 CFR 710).
- (4) Advise the appropriate management official and PSAP Approving Official of any security concern regarding a PSAP designated employee.
- (5) Evaluate and recommend the return to work of PSAP designated employees following periods of sick leave of 5 or more consecutive workdays.

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

- (1) Conduct supervisory reviews under section 710.57 of 10 CFR 710.
 - (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) Notify the appropriate management official immediately of a security concern relating to a PSAP designated employee.
 - (4) Refer PSAP designated employees exhibiting unusual conduct to the Site Occupational Medical Director for review and appropriate action.
 - (5) Approve the return to work of a PSAP designated 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.
- o. DOE Contractors and Subcontractors, and Access Permittees.
- (1) DOE Contractors and Subcontractors shall follow requirements in Attachment 1, "Contractor Requirements Document."
 - (2) DOE Access Permittees for the Personnel Security Program shall implement and administer effective and efficient program procedures to ensure compliance with the requirements of 10 CFR 725 and 1016 and this Order.
- p. Individuals Assigned to a PSAP Designated Position.
- (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 for work, to the Site Occupational Medical Director following periods of sick leave of 5 or more consecutive workdays.
 - (4) Comply with the requirements listed below in subparagraph 5q.

- q. Individuals Applying For or Granted DOE Access Authorizations for the Personnel Security Program.
- (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 a personnel security background investigation or reinvestigation, and at any processing stage 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 subsection 710.6[a] of 10 CFR 710).
 - (2) Notify the cognizant DOE personnel security office within 5 working days of all arrests, criminal charges (including charges that are dismissed), or detentions by Federal, State, or other law enforcement authorities for any violations of the law, other than traffic violations for which a fine of \$250 or less was imposed, within or outside of the United States.
 - (3) Provide to the cognizant DOE personnel security office a completed DOE F 5631.34, "Data Report on Spouse," in accordance with the requirements of Chapters I-IX of DOE 5631.2C.
 - (4) Notify the cognizant DOE personnel security office within 5 working days of any of the following:
 - (a) Personal or business-related filing for bankruptcy.
 - (b) Garnishment of wages.
 - (c) Legal action effected for name change.
 - (d) Change in citizenship status.
 - (e) Employment by, representation of, or other business-related association with, a foreign or foreign-owned interest.
 - (f) Continuing contact with foreign nationals (i.e., any contacts which are more than casual in nature, whether in a business or social setting).

- (5) Notify the cognizant DOE security office or the facility security officer, as appropriate, immediately after any approach or contact by an individual seeking unauthorized access to classified matter or SNM. If such an approach or contact is made while on foreign travel, notification should be made to 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 DOE Director of Safeguards and Security.

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

BY ORDER OF THE SECRETARY OF ENERGY:



ARCHER L. DURHAM
Assistant Secretary for
Human Resources and Administration

CONTRACTOR REQUIREMENTS DOCUMENT

PERSONNEL SECURITY ACTIVITIES

1. **PURPOSE.** This document, which is equivalent to the Personnel Clearances Section of the National Industrial Security Program Operating Manual, prescribes requirements, restrictions, and other procedures necessary for Department of Energy (DOE) contractors to:
 - a. Prevent the unauthorized disclosure of classified matter;
 - b. Protect special nuclear materials (SNM); and
 - c. Control the authorized disclosure of classified matter released by the DOE and other Federal agencies.
2. **AUTHORITY.**
 - a. 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.
 - b. 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.
3. **INTERPRETATION.** Requests for interpretations of this document or implementation assistance may be made to the senior DOE Personnel Security Program manager or official at the DOE office responsible for processing the contractor's access authorization requests (hereafter referred to as the "cognizant DOE office").
4. **DEVIATIONS.** Written requests for deviations from these requirements shall be forwarded through established channels beginning with the senior DOE Personnel Security Program manager or official at the cognizant DOE office in accordance with DOE O 470.1. Deviations from requirements or procedures in the Code of Federal Regulations shall not be approved.
5. **GENERAL REQUIREMENTS.**
 - a. Requests for access authorization shall not be submitted until the contractor has been awarded a DOE contract and submitted to the DOE the required paperwork for a Foreign Ownership, Control or Influence (FOCI)

determination.

- b. Access authorization requests may be submitted to the DOE pending completion of the FOCI determination; however, a favorable FOCI determination must be rendered by the 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 the 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 for the DOE.
- 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, or 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 6 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 the DOE that access authorization has been granted, reinstated, extended, or transferred. Verbal notification from a DOE official may be accepted, to be followed by written confirmation of the action.

- g. Except as authorized by the DOE in paragraph 10 below, access authorizations shall be requested only for individuals who are United States citizens.
 - 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 the DOE and investigative agencies as reflected in paragraph 8e below for the conduct of initial investigations and periodic reinvestigations, and for reinvestigations that are conducted when the DOE determines that an employee has engaged in an activity or is subject to circumstances that may affect continued access authorization eligibility.
 - j. The provisions of DOE O 472.1A, Chapters I-IX of DOE 5631.2C, and Title 10, Code of Federal Regulations, Part 710 (10 CFR 710) may not be subject to collective bargaining between contractor management and labor; i.e., the DOE retains authority in all matters related to DOE personnel security activities.
 - 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 the DOE for DOE costs associated with processing the contractor's applicants or employees for investigations or other access authorization related actions.
 - 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 11c below.
6. **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: (**NOTE:** A Q access authorization also allows the individual access to the categories/levels of classified matter listed in subparagraph 6a[2] below.)
 - (a) Top Secret or Secret Restricted Data;
 - (b) Top Secret Formerly Restricted Data;
 - (c) Top Secret National Security Information; or
 - (d) Any category or level of classified matter designated as COMSEC, CRYPTO, or Sensitive Compartmented Information.
- (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. Reference DOE M 5632.1C-1, Table II-1. (**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 or transportation of Category I quantities may require additional measures such as Personnel Security Assurance Program or Personnel Assurance Program [reference DOE O 452.2, 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 Rollup 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.

7. **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 designated positions.
- b. The contractor shall require applicants and employees selected for a position requiring an access authorization to provide evidence of United States citizenship and shall verify such evidence to the DOE when requesting that the individual be processed for an access authorization (see paragraphs 7c[2] and 8a below). (**NOTE:** The contractor is **not** required to obtain and verify to the 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 is one created when a record was filed more than one year after the date of birth. Such a certificate 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. The requirements in this subparagraph apply only to DOE Management and Operating Contractors (reference 48 CFR 970.2201[b][1][ii]).
- (1) 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 the DOE:
 - (a) A credit check.
 - (b) Verification of high school degree/diploma or degree/diploma granted by an institution of higher learning within the past 5 years.
 - (c) Contacts with listed references.
 - (d) Contacts with listed employers for the past 3 years (excluding employment of less than 60 days duration, part-time employments, and craft/union employments).

- (e) 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.
- (2) The results of the checks conducted in the paragraph above shall be verified to the DOE with the individual's security forms, verification of United States citizenship as required in paragraph 8a below, 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 the DOE for each check conducted by the contractor:
 - (a) The date the check was conducted;
 - (b) The identity of the individual, office, or entity that provided the information; and
 - (c) A synopsis of the information provided to the contractor.
- (3) An applicant hired specifically for a position that will require an access authorization shall not be placed in that position prior to the access authorization being granted by the DOE unless an exception has been obtained from the Head of the Contracting Activity or designee.
- (4) The contractor shall not conduct the checks or provide verifications to the DOE stipulated in subparagraphs 7c(1) and 7c(2) above for:
 - (a) Individuals who hold a DOE access authorization or a security clearance granted by another Federal agency;
 - (b) Federal employees (including members of the Armed Forces) detailed or assigned to the contractor; or
 - (c) An employee previously granted access authorization or 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.
- d. 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 the

DOE. After the 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, coordination will be effected with the DOE to obtain information necessary for the granting of 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.

8. **PROCESSING ACCESS AUTHORIZATION REQUESTS TO THE DOE.**

- a. Access authorization requests shall be forwarded through established channels to the cognizant DOE office. Requests shall include the following documentation: (**NOTE:** 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,
 - (4) For DOE Management and Operating Contractors, verification that pre-pCRYPTO, or Weapon Data, the individual may be required to file Financial Disclosure Reports, copies of which shall be provided by the cognizant DOE office.) rocessing checks have been conducted as indicated in subparagraph 7c(2) above.
 - (5) The DOE Contract or Subcontract Number under which access authorization is being requested.
- b. Individuals shall be advised that his/her completed security forms will be reviewed by designated contractor employees for completeness prior to submission to the 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 to maintain 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, to include 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 the DOE; and,
 - (2) Informing all employees with access to completed security forms, pre-employment check information, and other access authorization related information of their responsibility to protect the information from unauthorized disclosure.
- d. Deficient access authorization requests may be returned to the contractor by the cognizant DOE office with an indication of the deficiency(ies). The contractor

shall ensure that the deficiency(ies) is (are) corrected and shall return the request to the cognizant DOE office for processing. The contractor shall ensure that the individual being processed for access authorization is not provided access to classified matter or SNM until the cognizant DOE office notifies the contractor that 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 management 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. Each DOE prime contractor shall be responsible for reviewing, approving, and submitting to the 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.

9. **INTERIM ACCESS AUTHORIZATION REQUEST.**

- a. The contractor may request that an individual who is being processed for Q access authorization also be processed for an interim access authorization (IAA) based on the following justification: (**NOTE:** Specific information substantiating the following must be provided.)
 - (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.
- b. The IAA request shall accompany the required documentation in subparagraph 8a above.

- c. Individuals who require 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. 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 request has been approved. The DOE shall also notify the contractor if the IAA request is not approved.
- e. Non-approval of an IAA request is not a denial of access authorization and is not appealable. DOE full access authorization procedures will continue in either case.
- f. If an individual's IAA approval is withdrawn by the 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. The DOE shall confirm the verbal notification in writing. Withdrawal of an individual's IAA by the DOE is not a denial or revocation of access authorization and is not appealable. Withdrawal of an individual's IAA does not halt the processing of the Q access authorization request.
- g. If the DOE grants final Q access authorization, the individual's IAA will be withdrawn and the contractor so notified in writing.
- h. The contractor shall not request an IAA for individuals requiring L access authorizations or for non-United States citizens.

10. **ACCESS AUTHORIZATION REQUEST FOR A FOREIGN NATIONAL.**

- a. A request for an access authorization for a foreign national shall be processed 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 not possessed to a comparable degree by an available United States citizen, and is essential to the DOE's mission.
- c. The request shall not be processed by the DOE if sufficient information cannot be obtained by an investigation to determine the individual's access authorization eligibility.

- d. A foreign national granted access authorization shall not be provided access to the following types of classified matter:
- (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.

11. **REPORTING AND OTHER REQUIREMENTS.**

- a. Contractor Reporting Requirements. Verbal notification shall be provided through established channels to the cognizant DOE office within 2 working days of the following conditions affecting an applicant's or employee's access authorization status. The verbal notification shall be confirmed by the contractor in writing, through established channels, to the cognizant DOE office within the next 10 working days.
- (1) When an applicant declines the offer of employment or fails to report for duty.
 - (2) For any reason iterated in subparagraph 11c 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.
 - (6) When the contractor restricts or withdraws an employee's access to classified matter or SNM without DOE direction.
- b. Individual Reporting Requirements. Contractors shall inform individuals under their cognizance applying for or granted access authorizations that they are personally responsible for the following: (**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.)
- (1) Providing 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) Directly notifying 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.
- (3) Notifying 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, notification should be made to 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 of Safeguards and Security at DOE Headquarters. This requirement is in addition to any similar reporting requirements implemented under DOE 5670.3, COUNTERINTELLIGENCE PROGRAM, of 9-4-92.
- (4) Providing a completed DOE F 5631.34, "Data Report on Spouse," directly to the cognizant DOE office within 45 calendar days of marriage to an individual who does not currently hold access authorization. These forms shall be provided by the cognizant DOE office.
- 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 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 to maintain the individual's access authorization in an active status 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 access authorization. The contractor shall inform the cognizant DOE office of the individual's employment status at the end of the 3-month interval.)
- (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 DOE access authorization for an applicant or employee when the contractor is aware that the individual previously was granted 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 6 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 6 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 active access authorizations: under the cognizance of two or more DOE offices; under two or more employers; or for one employer under two or more contract numbers. 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 when the individual has an active access authorization granted by the DOE at the request of another employer **and** 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 number.)
- (2) For an employee when the individual will be assigned to perform classified work under a second (or more) DOE contract number and must retain the original access authorization in connection with his/her continued work under the first DOE contract number.

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 number 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 subparagraph 11c 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 active access authorization granted by the 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.)
- (2) For an employee when the individual will be assigned to perform classified work under a different contract number than the one for which he/she was originally granted access authorization, and will no longer require access to classified matter associated with the original contract number. **(NOTE:** This action involves a change of contract numbers 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 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 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 cognizant 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 access authorization. If so directed, the contractor shall retrieve from the employee any identification reflecting active access authorization. The cognizant DOE office is responsible for notifying other DOE offices or 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 have 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 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) Current records shall be maintained 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 the 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 for each applicant and employee access authorization matters 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 contractor requests the DOE to terminate the individual's access authorization, 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 pre-employment 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 organizations other than DOE, other Federal agency, State, or local officials approved by 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 authorization, 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 subparagraph 8e above).

12. **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, prepared in accordance with 10 CFR 710 and DOE directive requirements, shall reflect the PSAP requirements to which the contractor has agreed.

13. **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.

- a. Withdrawal of an IAA is not a denial or revocation of access authorization and is not appealable during this stage of the processing.
- b. The contractor shall not request IAA for individuals requiring L access authorizations or for non-United States citizens.
- c. When DOE grants final Q access authorization, the IAA shall be withdrawn and the contractor shall be so notified in writing.

14. **REQUESTS FOR ACCESS AUTHORIZATIONS FOR FOREIGN NATIONALS.**

- a. Requests for DOE access authorization for foreign nationals shall be processed in accordance with the guidance provided by the cognizant DOE office.
- b. Such requests shall be made, and granted, only when the contractor provides clear evidence that the applicant has talents or skills not possessed to a comparable degree by an available United States citizen and is essential to the Department's mission.
- c. The request shall not be processed by DOE if sufficient information cannot be obtained by a background investigation to determine the individual's access authorization eligibility.
- d. Foreign nationals granted DOE access authorization may not be provided access to the following types of classified matter:
 - (1) Top Secret, "COMSEC," or "CRYPTO" information.
 - (2) 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.

- (3) Intelligence information.
- (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 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.

15. **REPORTING AND OTHER REQUIREMENTS.**

- a. Contractor Reporting Requirements. Verbal notification shall be provided by the contractor through established channels to the cognizant DOE office of the following conditions affecting an employee's DOE access authorization status. Verbal notification shall be confirmed in writing within 2 working days as follows:
 - (1) When an applicant for employment declines the offer of employment or fails to report for duty.
 - (2) When the need for access shall be terminated in accordance with the requirements of subparagraph 11c below.
 - (3) Within 8 working hours of becoming aware that an individual under their cognizance has been hospitalized or is otherwise being treated for a mental illness or such other condition that may cause a significant defect in judgment or reliability.
 - (4) When made aware of derogatory information of personnel security interest. Such information must be characterized as reliable and relevant and create a question as to an individual's DOE access authorization eligibility as exemplified in section 710.8 of 10 CFR 710 (see the reverse of DOE F 5631.18).

- (5) When an employee becomes employed by or a representative of a foreign or foreign-owned interest, engages in a business-related association with a foreign or foreign-owned interest, or when the employee's status regarding the aforementioned is materially changed.
 - (6) When a foreign national under their cognizance becomes a United States citizen through naturalization or affects some other change in citizenship.
 - (7) When an employee's access to DOE classified matter or SNM is withdrawn or restricted by the contractor without explicit direction by DOE.
 - (8) An effort by any individual, regardless of nationality, to obtain unauthorized access to classified matter or SNM, or to compromise or exploit an employee.
- b. Individual Reporting Requirements. Contractors shall inform individuals under their cognizance applying for or granted DOE access authorization that they are personally responsible for the following:
- (1) Providing full, frank, and truthful answers to relevant and material questions, and when requested, furnishing or authorize others to furnish information that DOE deems pertinent to the access authorization eligibility. This applies when completing security forms, during the course of a personnel security investigation or 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 then in effect may be terminated or further processing may be suspended.
 - (2) Notifying DOE within 5 working days of all arrests, criminal charges (including charges that are dismissed), or detentions by Federal, State, or other law enforcement authorities for any violations of the law, other than traffic violations for which a fine of \$250 or less was imposed, within or outside of the United States. Notification shall be made by the individual directly to the cognizant DOE office personnel security office.
 - (3) Providing a completed DOE F 5631.34, "Data Report on Spouse," directly to the cognizant DOE office personnel security office within 45

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

- (4) Providing written notification to the cognizant DOE office personnel security office within 5 working days, of any of the following:
 - (a) Personal or business-related filing for bankruptcy.
 - (b) Garnishment of wages.
 - (c) Legal action effected for name change.
 - (d) Change in citizenship.
 - (e) Employment by, representation of, or other business-related association with a foreign or foreign-owned interest.
 - (f) Continuing contact with foreign nationals (i.e., any contacts which are more than casual in nature, whether in a business or social setting).
 - (5) Notifying the cognizant DOE security office or the facility security officer, as appropriate, immediately after any approach or contact by an individual seeking unauthorized access to classified matter or SNM. If such an approach or contact is made while on foreign travel, notification should be made to 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 DOE Director of Safeguards and Security.
- c. Requests for Access Authorization Termination. Contractors shall request the cognizant DOE office(s) to terminate an employee's DOE access authorization and provide a DOE F 5631.29, "Security Termination Statement," completed and signed by the employee as follows:
- (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 termination of employment or transfer to a position not requiring such

access. An exception may be authorized by the cognizant DOE office upon certification by the contractor that the individual shall be reemployed or reassigned with access within 3 months and that DOE shall be kept informed of the individual's status.

- (5) The individual leaves for foreign travel, employment, assignment, education, or residence of more than 3 months not involving official United States government business.

(NOTE: The purpose of the DOE F 5631.29 is to ensure that the individual is aware of continuing responsibilities to protect classified matter after termination of access authorization. The cognizant DOE office shall be requested to terminate an employee's access authorization even though a completed and signed DOE F 5631.29 cannot be immediately provided.)

- d. Reinstatement of an employee's DOE access authorization shall be requested of the cognizant DOE office when the contractor is aware that the employee previously was granted DOE access authorization. The cognizant DOE office shall advise the contractor whether the individual must complete updated security forms.
- e. Upgrading of an employee's DOE access authorization (from L to Q) shall be requested of the cognizant DOE office in accordance with the new access requirements required by the duties of the position (reference paragraph 6 above). The written request for upgrading shall be accompanied by appropriate security forms and a revised justification for access authorization statement.
- f. Downgrading of an employee's DOE access authorization (from Q to L) shall be requested of the cognizant DOE office in accordance with the new access requirements required by the duties of the position (reference paragraph 6 above). The written request for downgrading shall also reflect a revised justification for access authorization statement.
- g. Extension of a DOE access authorization is the process that allows an employee to hold concurrent active access authorizations under the cognizance of two or more DOE offices. A contractor's DOE access authorization is associated with a specific contractual agreement with DOE. If the contractor is awarded another DOE contract requiring classified work or tasks by a second DOE office, a separate access authorization is required for an employee who will be performing work or tasks under the new contract. If an employee already has a DOE access authorization, the employee cannot have access to classified matter

under the new contract until DOE access authorization has been formally extended to the new cognizant DOE office. The request for an extension of an employee's access authorization shall be sent to the new cognizant DOE office with a written justification for access authorization statement and shall reference the employee's full name and Social Security Account Number and, if known, DOE Personnel Security File number, and type/date of access authorization granted. The new cognizant DOE office shall advise the contractor if additional security forms are required to effect the extension. When the extension action is effected, the new cognizant DOE office shall provide written notification to the contractor. Under the extension process, an employee's access authorization can be terminated under one contract and be maintained in an active status under another contract(s). All cognizant DOE offices shall be notified by the contractor when the employee no longer requires access authorization under any DOE contracts.

- h. Transfer of a DOE access authorization simultaneously allows an employee's access authorization to be terminated at one cognizant DOE office and granted at another. The process is used when a contractor desires to transfer an employee's access authorization from one DOE contract to another DOE contract awarded by a separate cognizant DOE office. The request for transfer of access authorization shall be made to the new cognizant DOE office with a written justification for access authorization statement and shall reference the employee's full name and Social Security Account Number, and, if known, DOE Personnel Security File number, and type/date of access authorization granted. The new cognizant DOE office shall advise the contractor if additional security forms are required. When the transfer is effected, the new cognizant DOE office shall provide written notification to the contractor. The contractor shall be responsible for ensuring that the cognizant DOE office that originally granted the employee's access authorization is notified in writing to terminate the employee's access authorization.
- i. Access Authorization Suspension, Revocation, and Denial.
 - (1) The cognizant DOE office shall be responsible for notifying the contractor in writing when an employee's DOE 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 access authorization. If so directed, the contractor shall retrieve from the employee any identification reflecting active DOE access authorization. The cognizant DOE office shall be responsible for written notification to other DOE offices or

agencies where the employee has been approved/certified for access to classified matter. When a DOE final determination is rendered, the contractor shall be notified in writing whether the employee's access authorization has been reinstated or revoked.

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

j. Records Maintenance.

- (1) The contractor shall maintain a current record reflecting for each facility, by contract number, all employees granted access to classified matter or SNM. The listing shall include the employee's name, DOE file number, and the date the contractor was notified by DOE that the employee's DOE access authorization was granted, reinstated, extended, or transferred.
- (2) The contractor shall maintain copies of correspondence to and from the cognizant DOE office(s) that reflect for each employee the request for access authorization, notification from DOE that access authorization action was effected, and notification to terminate access authorization. Such copies shall be maintained for a period of 2 years after the contractor has requested DOE to terminate the employee's access authorization, at which time they may be destroyed.

k. Recertification and Reinvestigation.

- (1) The contractor shall comply with periodic DOE requests to recertify its employees' DOE access authorization status. The contractor shall be furnished with a listing by the cognizant DOE office of employees who hold DOE access authorization, requested to annotate the listing with

any corrections or adjustments, and return the listing in a timely manner. Specific guidance shall be provided by the cognizant DOE office.

- (2) The contractor shall assist DOE in periodic reinvestigations in accordance with guidance provided by the cognizant DOE office.

16. **PERSONNEL SECURITY ASSURANCE PROGRAM REQUIREMENTS.**

Contractors shall prepare a Personnel Security Assurance Program (PSAP) Implementation Plan when their site, facility, or operations are identified as having PSAP Positions and implement the provisions of the PSAP Implementation Plan within 30 working days of its approval. The PSAP Implementation Plan, prepared in accordance with requirements in 10 CFR 710, Subpart B and DOE O 472.1A, shall reflect the PSAP requirements to which the contractor has agreed.

CANCELLED

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

(See below for Special Nuclear Materials)

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

*For an initial DOE Q access authorization, an Office of Personnel Management Single-Scope Background Investigation or Federal Bureau of Investigation Background Investigation (for "Positions of a High Degree of Importance or Sensitivity") is required. Completed investigations by other agencies can be obtained and used by DOE as an adjudicative basis for a Q access authorization if the scope and extent of the investigation meets DOE specifications.

**For initial DOE L access authorization, an Office of Personnel Management: Limited Background Investigation is required for DOE employees and applicants for employment; at least a National Agency Check with Credit is required for other agency employees; and, a National Agency Check with Credit is required for DOE and other agency contractor and subcontractor employees and Access Permittees. A more extensive investigation can, of course, be used as a basis for adjudicating an individual's eligibility for L access authorization.

The type of investigation scheduled with the Office of Personnel Management 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 a Limited Background Investigation or National Agency Check with Credit.

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

(See above for Classified Matter)

SPECIAL NUCLEAR MATERIALS CATEGORY	TYPE OF DOE 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 inside acts.
II with credible rollup to I	Q	
II and III	L	Unless special circumstances determined by site vulnerability assessment require Q access authorization to minimize risk. Document in Site Safeguards and Security Plan.
IV	None	Unless special circumstances determined by site vulnerability assessment require access authorization to mitigate risk. Document in Site Safeguards and Security Plan.

(Reference: Page II-3, DOE M 5632.1C-1, of 7-15-94)

POSITIONS OF A HIGH DEGREE OF IMPORTANCE OR SENSITIVITY

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

In instances where an individual will occupy a position in DOE requiring confirmation by the United States Senate, a Federal Bureau of Investigation background investigation will be scheduled by The White House staff prior to the individual's name being 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 Federal Bureau of Investigation reports of investigation. This listing shall be periodically updated and reissued as circumstances warrant.

A. DOE HEADQUARTERS

<u>Position</u>	<u>Headquarters Routing Symbol</u>
The Secretary of Energy	S
The Deputy Secretary	DS
The Under Secretary	US
Assistant Secretary for Congressional and Intergovernmental Affairs	CI-1
Assistant Secretary for Defense Programs	DP-1
Deputy Assistant Secretary for Military Application and Stockpile Support	DP-20
Assistant Secretary for Environment, Safety and Health	EH-1
Assistant Secretary for Environmental Management	EM-1
General Counsel	GC-1
Assistant Secretary for Human Resources and Administration	HR-1
Inspector General	IG-1
Director of Nuclear Energy	NE-1
Director of Nonproliferation and and National Security	NN-1
Director of Energy Intelligence	NN-30
Director of Security Affairs	NN-50

Assistant Secretary for Policy

PO-1

B. DOE FIELD ELEMENTS

1. Manager, Albuquerque Operations Office
 - a. Assistant Manager, Office of National Defense Programs
 - b. Director, Amarillo Area Office
 - c. Director, Kansas City Area Office
 - d. Director, Kirtland Area Office
 - e. Director, Los Alamos Area Office
2. Manager, Chicago Operations Office
3. Manager, Idaho Operations Office
4. Manager, Nevada Operations Office
5. Manager, Oakland Operations Office
6.
 - a. Manager, Oak Ridge Operations Office
 - b. Assistant Manager for Defense Programs
7. Manager, Ohio Field Office
8. Manager, Pittsburgh Naval Reactors Office
9. Manager, Richland Operations Office
10. Manager, Rocky Flats Field Office
11. Manager, Savannah River Operations Office
12. Manager, Schenectady Naval Reactors Office

REFERENCES

1. Title 5, United States Code, 552a, "Privacy Act of 1974," 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, 732, "Personnel Security," which implements Executive Order 10450 throughout the Federal agencies and departments.
5. Title 5, Code of Federal Regulations, 736, "Personnel Investigations," which deals primarily with the conduct of investigations by the Office of Personnel Management.
6. Title 10, Code of Federal Regulations, 707, "Substance Abuse Programs at DOE Sites," which establishes procedures for drug testing in DOE.
7. Title 10, Code of Federal Regulations, 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 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, 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, 1008, Subpart B, Privacy Act, "Records Maintained on Individuals," which establishes the procedures to implement the provisions of the Privacy Act of 1974 within DOE.
10. Title 10, Code of Federal Regulations, 1016, "Safeguarding of Restricted Data," which establishes requirements for the safeguarding of 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 preemployment check requirements.

12. Title 53, Code of Federal Regulations, 11970, "Department of Health and Human Services: Mandatory Guidelines for Federal Workplace Drug Testing Programs," of 4-11-88, which contains requirements for conducting drug testing.
13. Executive Order 10450, "Security Requirements for Government Employees," of 4-29-53, as amended, which establishes the requirement for determining that all Federal employees be loyal, reliable, trustworthy, and of good conduct and character.
14. Executive Order 10865, "Safeguarding Classified Information Within Industry," of 2-20-65, as amended, which establishes the basis for the industrial security program for civilian personnel.
15. Executive Order 12564, "Drug-Free Federal Workplace," of 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," of 1-6-93, which establishes a program to safeguard Federal Government classified information released to its contractors, licensees, and grantees.
17. Executive Order 12958, "Classified National Security Information," of 4-17-95 which establishes a uniform system for safeguarding National Security Information.
18. Executive Order 12968, "Access to Classified Information," of 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. National Security Directive 63, "Single Scope Background Investigations," of 10-21-91, which establishes the scope and extent of the investigation used as a basis in the Federal Government to determine an individual's eligibility for a Top Secret security clearance and/or eligibility for access to Sensitive Compartmented Information.
20. Director of Central Intelligence Directive (DCID) No. 1/14, "Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information," of 11-27-84, which establishes the minimum personnel security standards and procedures governing eligibility for access to Sensitive Compartmented Information.
21. Department of Defense "National Industrial Security Program Operating Manual (NISPOM)," of October 1994, issued pursuant to Executive Order 12829, which establishes minimum security requirements for the protection of classified matter by

- Government contractors. This document replaces the Department of Defense "Industrial Security Manual for Safeguarding Classified Information," of January 1991.
22. Department of Energy Delegation Order No. 0204-139, of 12-20-91, which authorizes the Director of Security Affairs to make determinations of eligibility (in accordance with section 4.2[a][1] of Executive Order 12356, which has been superseded by Executive Order 12958), prescribe such regulations or Orders as deemed necessary to protect Restricted Data, and make determinations pursuant to section 145b of the Atomic Energy Act of 1954, as amended.
 23. DOE 1700.1, FREEDOM OF INFORMATION PROGRAM, of 11-19-79, which establishes procedures for processing requests made to DOE under the Freedom of Information Act.
 24. DOE 1800.1A, PRIVACY ACT, of 8-31-84, which establishes DOE implementation guidelines for the Privacy Act of 1974.
 25. DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM, of 9-28-95, which establishes the policy and responsibilities for the DOE Safeguards and Security Program, and the accompanying Manual, DOE M 5632.1C-1, SAFEGUARDS AND SECURITY PROGRAM MANUAL, of 7-15-94, which establish the policies, requirements, and procedures 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 special nuclear material.
 26. DOE Integrated Security System (DISS) "User System Reference Manual," of November 1994, which establishes for system users the system requirements, operations, and data input procedures for the Central Personnel Clearance Index (CPCI) and other system components.
 27. Office of Safeguards and Security "Adjudicative Guidelines for Determining Eligibility for Access to Classified Matter and/or Special Nuclear Material," of April 1994, which establishes guidelines for DOE personnel security officials in evaluating information of security concern in personnel security cases.
 28. Office of Safeguards and Security "Implementation Guidance for Title 10, Code of Federal Regulations, Part 710, Subpart A (10 CFR 710)," of September 1994, which provides supplemental instructions and guidance for DOE personnel security officials in the processing of personnel security cases under DOE Administrative Review procedures.