**DOE M 470.4-5**

Approved: 08-26-05
Review: 08-26-07

# PERSONNEL SECURITY


## U.S. DEPARTMENT OF ENERGY

**Office of Security and Safety Performance Assurance**

**AVAILABLE ONLINE AT:**
**www.directives.doe.gov**

**INITIATED BY:**
**Office of Security and Safety Performance Assurance**

# PERSONNEL SECURITY

1. PURPOSE. This Manual establishes the overall objectives and requirements for the Personnel Security Program in the U.S. Department of Energy (DOE), including the National Nuclear Security Administration (NNSA).

2. OBJECTIVES.

   a. To effect the policy in DOE P 470.1, *Integrated Safeguards and Security Management Policy (ISSM)*, by integrating personnel security into DOE operations as determined by line management, and according to sound risk management practices. [DOE Policy 470.1, *Integrated Safeguards and Security Management Policy (ISSM)*, is the Department's philosophical approach to the management of the Safeguards & Security (S&S) Program. A principal objective of the ISSM program is to integrate S&S into management and work practices at all levels, based on program line management's risk management-based decisions, so that missions may be accomplished without security events, such as interruption, disruption, or compromise. This approach includes individual responsibility and implementation of the security requirements found in this Manual].

   b. To ensure that individuals are processed for, granted, and allowed to retain an access authorization only when their official duties require access to classified information or matter, or special nuclear material (SNM).

   c. To allow access to DOE classified information or matter, or 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.

   d. To maintain the numbers and types of access authorizations at the minimum levels necessary to ensure the operational efficiency of DOE programs and operations involving classified information or matter, or SNM.

   e. To conduct personnel security activities in a manner that ensures:

      (1) timely and efficient processing of initial access authorization requests and reinvestigations;

      (2) consistent, objective, and fair interpretation and application of criteria and procedures in every access authorization action;

      (3) timely review and adjudication of investigative reports and other information related to an individual's access authorization eligibility; and

(4) maintenance of accurate, complete, and timely access authorization file and record information, the availability of such information to authorized users, and the protection of such information from unauthorized disclosure.

f. To periodically evaluate individuals retaining access authorizations to confirm their continued need for access and access authorization eligibility.

g. To ensure that DOE employees, contractors, and others involved in personnel security activities effectively and efficiently execute their personnel security responsibilities.

h. To prevent the use of personnel security activities for reprisal, discrimination, or any other unauthorized purpose.

i. To promote proactive participation in personnel security activities at the international, national, and interagency levels to ensure the adequate expression and consideration of DOE mission and program interests.

3. PROGRAM INTEGRATION. Personnel Security must be integrated with other programs such as S&S program planning and management, physical protection, protective force, information security, and nuclear material control and accountability. The activities and requirements in the weapons surety, foreign visits and assignments, safety, emergency management, cyber security, intelligence, and counterintelligence programs should be considered in the implementation of this Manual. Additionally, under the Human Reliability Program (HRP), a yearly review of the personnel security files of all individuals occupying HRP positions is conducted by personnel security specialists to ensure that there are no new security issues that would impact the individual's enrollment in the HRP.

4. CANCELLATION. DOE M 472.1-1B, *Personnel Security Program* Manual, dated 7-12-01 is canceled. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual obligation to comply with the directive. Canceled directives that are incorporated by reference in a contract remain in effect until the contract is modified to delete the reference to the requirements in the canceled directives. The publication of this Manual incorporates previous memoranda or letters that were issued by the Office of Security or its predecessor organizations that established policy and/or requirements for this policy.

5. APPLICABILITY.

a. Departmental Elements. Except for the exclusion in 5.c., below, this Manual applies to all Departmental Elements, including NNSA, as indicated on attachment 1. This Manual automatically applies to Departmental Elements created after it is issued. The Administrator of NNSA shall assure that NNSA

employees and contractors comply with their respective responsibilities under this Manual

b. Contractors.

(1) The Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Manual that will apply to site/facility management contracts that include the CRD.

(2) The CRD must be included in the site/facility management contracts that involve classified information or matter, or nuclear materials, and contain DOE Acquisition Regulation (DEAR) clause 952.204-2, *Security Requirements*.

(a) Departmental Elements must notify contracting officers of affected site/facility management contracts to incorporate this directive into those contracts.

(b) Contracting officers are responsible for incorporating this directive into the affected contracts via the "*Laws, Regulations, and DOE Directives*" clause of the contracts.

(3) A violation of the provisions of this directive relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection a. of section 234B of the Atomic Energy Act of 1954 (42 U.S.C. 2282b.). The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations, Part 824, "Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations" (10 CFR part 824).

(4) As stated in DEAR Clause 970.5204-2, *Laws, Regulations, and DOE Directives*, regardless of the performer of the work, site/facility contractors with the CRD incorporated into their contracts are responsible for compliance with the CRD. Affected site/facility management contractors are responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure compliance with the requirements. In doing so, contractors must not unnecessarily or imprudently flow down requirements to subcontracts. That is, contractors must: (1) ensure that they and their subcontractors comply with the requirements of this CRD; and (2) only incur costs that would be incurred by a prudent person in the conduct of competitive business.

(5) This Manual does not automatically apply to other than site/facility management contracts. Application of any of the requirements of this Manual to other than site/facility management contracts will be communicated as follows:

(a) Heads of Field Elements and Headquarters Departmental Elements. Review procurement requests for new non-site/facility management contracts that involve nuclear materials and contain the DEAR Clause 952.204-2, *Security Requirements,* and, if appropriate, ensure that the requirements of the CRD of this directive are included in the contract.

(b) Contracting Officers. Assist originators of procurement requests who want to incorporate the requirements of the CRD of this directive in new non-site/facility management contracts, as appropriate.

c. Exclusion. In accordance with the responsibilities and authorities assigned by Executive Order 12344 and to ensure consistency throughout the joint Navy and DOE organization of the Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors will implement and oversee all requirements and practices pertaining to this Manual for activities under the Deputy Administrator's cognizance.

6. AUTHORITIES. In all matters related to personnel security activities, DOE retains absolute authority. The procedures in this Manual and Title 10, CFR, Part 710 (10 CFR 710) are not subject to collective bargaining.

7. DEVIATIONS. Requests for deviations from requirements in this Manual will be processed in accordance with DOE M 470.4-1, *Safeguards and Security Program Planning and Management*. Deviations from the requirements and procedures in 10 CFR 710 will not be approved. Waivers of pre-appointment investigations will be processed in accordance with 5 CFR 732, 5 CFR 736, and chapter IV, paragraph 3.

8. DEFINITIONS. Terms commonly used in the program are defined in the S&S Glossary located in DOE M 470.4-7, *Safeguards and Security Program References*. In addition to those in the Glossary, the following definitions are provided for use in this Manual.

a. Field Element Manager means the Manager of the Chicago, Idaho, Oak Ridge, Richland, and Savannah River Operations Offices; Manager of the Pittsburgh Naval Reactors Office and the Schenectady Naval Reactors Office; Director of the Service Center, Albuquerque; and for the Washington, D.C. area, the Director, Office of Security.

b. DOE line management refers to DOE and NNSA Federal employees who have been granted the authority to commit resources or direct the allocation of personnel or approve implementation plans and procedures in the accomplishment of specific work activities.

c. Line management refers to DOE and NNSA Federal and contractor employees who have been granted the authority to commit resources or direct the allocation of personnel or approve implementation plans and procedures in the accomplishment of specific work activities.

d. DOE cognizant security authority refers to DOE and NNSA Federal employees who have been granted the authority to commit security resources or direct the allocation of security personnel or approve security implementation plans and procedures in the accomplishment of specific work activities.

e. Cognizant security authority refers to DOE and NNSA Federal and contractor employees who have been granted the authority to commit security resources or direct the allocation of security personnel or approve security implementation plans and procedures in the accomplishment of specific work activities.

f. For the purposes of this Manual, the Office of Security refers to the DOE Office of Security, Office of Security and Safety Performance Assurance.

g. For the purposes of this Manual, the term “access authorization(s)” refers only to DOE access authorizations.

9. CONTACT. Questions should be addressed to the Office of Security and Safety Performance Assurance at (301) 903-4804.

BY ORDER OF THE SECRETARY OF ENERGY:

CLAY SELL
Deputy Secretary

# CONTENTS

# CHAPTER I
# ACCESS AUTHORIZATION REQUESTS

1. DETERMINATION OF NEED FOR ACCESS AUTHORIZATION. A request for an access authorization will be submitted only after a determination has been made that the duties of the position require access to classified information or matter, or SNM. A request for an access authorization will be processed only when the need for access is clearly justified and it is for the type (Q or L) required, to comply with Executive directives and to avoid the unnecessary expenditure of DOE funds and other resources and the unwarranted invasion of an individual's privacy. Access authorizations must not be processed (i.e., requested, granted, continued, reinstated, transferred, or extended) to:

   a. avoid the use of access controls or physical barriers to distinguish perimeters among security areas or between security and open areas;

   b. alleviate responsibilities for escorting uncleared individuals within a security area;

   c. alleviate individual or management responsibilities for properly protecting classified information or controlling dissemination of such classified information on a need-to-know basis;

   d. establish a pool of cleared employees;

   e. accommodate an individual's personal convenience, expedience, gain, or advantage;

   f. anticipate unspecified classified work; or

   g. determine suitability for Federal, contractor, or other employment. For Federal employees, the investigative reports provided to DOE for determining eligibility for an access authorization may also be used to determine suitability for employment; however, an access authorization may not be requested specifically for the purpose of obtaining investigative reports for an employment suitability determination.

2. DETERMINATION OF ACCESS AUTHORIZATION ELIGIBILITY.

   a. DOE has a single access authorization program for DOE contractor and subcontractor employees, consultants, and access permittees. The CRD sets forth Personnel Security Program requirements for DOE contractors (see attachment 2). Statements concerning contractor requirements contained in this Manual are for the purpose of informing Departmental Elements only.

   b. For DOE employees and contractors, access authorizations must be requested only for individuals selected to occupy positions that require the incumbent to have access to classified information or matter, or SNM, in order to perform official work for DOE. Individuals under the age of 18 must not be processed for

or granted an access authorization. Except as authorized in chapter VI, only U.S. citizens are eligible for access authorizations.

c. Except as authorized by the Director, Office of Security, an individual's access authorization eligibility will be based on the review of investigative reports provided to DOE by the Office of Personnel Management (OPM), the Federal Bureau of Investigation (FBI), or another Federal agency authorized to conduct background investigations.

d. All individuals processed for access authorizations must be treated equally, regardless of their employment status, to preclude the appearance, inference, or practice of partiality or favoritism. Any DOE officer or employee who uses personnel security activities to coerce, restrain, threaten, intimidate, or retaliate against individuals for exercising their rights under the Constitution, or under any statute, regulation, or DOE directive, will be subject to appropriate disciplinary action.

e. No individual will be authorized access to classified information or matter, or SNM, until eligibility for such access has been determined in accordance with the procedures in this Manual.

3. DETERMINATION OF ACCESS AUTHORIZATION TYPE. The type of access authorization requested is based on an individual's need for access to the category and level of classified information or matter, or category of SNM, for the performance of official duties. An authorization granted for access to SNM also allows access to the appropriate categories/levels of classified information or matter on a need-to-know basis. To meet the requirements of the National Industrial Security Program Operating Manual (NISPOM), the contractor Facility Security Officer (FSO) and key management personnel must possess access authorizations equivalent to the level of the facility clearance (for information on facility clearances see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*). There are five types of access authorization: Q, L, QX, LX, and QB. Determination of the type of access authorization must be certified in writing by the requester to the Director, Office of Headquarters Security Operations (for Headquarters cases), or to the DOE cognizant security authority.

a. Q and L:

(1) A Q access authorization must be requested when the duties of the position require access to any of the following:

(a) Top Secret or Secret Restricted Data;

(b) Top Secret Formerly Restricted Data;

(c) Top Secret National Security Information;

(d) Classified information or matter designated as "COMSEC," "CRYPTO," "Sensitive Compartmented Information," or Weapon Data, Sigma 14 or Sigma 15;

(e) SNM designated as Category I, and other Categories with Credible Roll-Up to Category I.

**NOTE:** A Q access authorization also authorizes the individual access to the categories/levels of classified information or matter listed in paragraph (2) below.

(2) An L access authorization must 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;

(c) Secret or Confidential National Security Information;

(d) SNM designated as Categories II and III, unless special circumstances determined by a site vulnerability assessment and documented in the Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP) require a Q access authorization.

(3) When it is determined that a Q access authorization is needed but that it would be advantageous to the Department for the individual to be granted an L access authorization if the investigative and adjudicative requirements for an L are completed prior to those for the Q access authorization, then QL processing should be requested. (see Chapter II, 4.b.).

(4) A Q access authorization is required for certification in a position designated under the HRP in accordance with 10 CFR 712.10.

b. QX and LX. QX and LX access authorizations are granted to individuals employed by a DOE access permittee. QX is for access to Secret and/or Confidential Restricted Data, and LX is for access to Confidential Restricted Data. Information regarding the DOE access permit program is found in 10 CFR 725.

c. QB. A QB access authorization is granted by the Director, Office of Security, only to certain Executive, Legislative, and Judicial Branch officials and elected state officials in accordance with section 145b of the Atomic Energy Act of 1954. A QB access authorization allows the individual the same access as a Q access authorization.

4. OTHER FEDERAL DEPARTMENT OR AGENCY EMPLOYEES AND LEGISLATIVE AND JUDICIAL BRANCH EMPLOYEES. Until DOE has determined that such access will not endanger the common defense and security, DOE will withhold access to classified information or matter, or SNM, under DOE responsibility from employees of other Federal agencies and Legislative and Judicial Branch employees. Unless the Secretary or the Secretary's designee authorizes such action as clearly consistent with the national security, this determination will be based on an investigation and report by the OPM, the FBI, or other Federal agency that conducts personnel security investigations. Access to Restricted Data will not be allowed unless an access authorization has been granted to the individual based on the investigation and report. Determinations for access to Restricted Data, pursuant to section 145b of the Atomic Energy Act, will be used only for the President and Vice President; Federal justices, judges, and magistrates; members of Congress; and State governors and lieutenant governors.

5. ACCESS FOR SPECIAL TYPES OF CLASSIFIED INFORMATION. In addition to an access authorization, several types of classified information require approval before access to the information is authorized. They are:

   a. Sensitive Compartmented Information (SCI), CRYPTO, and COMSEC;

      (1) SCI access must be approved by the DOE Senior Intelligence Officer or his/her designated representative within the Office of Intelligence.

      (2) Access to CRYPTO and COMSEC must be approved by the Office of the Chief Information Officer.

      (3) Individuals under DOE cognizance must possess a Q access authorization before being afforded access to any classified information or matter designated as SCI, CRYPTO, or COMSEC. For further information on approval for access to this information, the relevant office should be contacted.

   b. Weapon Data, which requires NNSA approval;

   c. North Atlantic Treaty Organization (NATO) information, which requires NNSA approval.

6. REQUIRED DOCUMENTATION. Each request for an access authorization must include the following information:

   a. the type of access authorization required for the position;

   b. justification for the type of access authorization requested; and

   c. the correct and completed forms as described in this Manual, chapter II, paragraph 1., unless the individual will be processed under the reciprocity process described

in this Manual, chapter II, paragraph 2., or the reinstatement process described in chapter VII, paragraph 3.

# CHAPTER II
# INVESTIGATIVE REQUESTS AND PROCESS, AND PERSONNEL SECURITY FILES

1. FORMS.

   a. Federal Employees. The following forms are required to process a request for an initial access authorization:

      (1) Standard Form 86 (SF 86), *Questionnaire for National Security Positions*, and if necessary, SF 86A, *Questionnaire for National Security Positions Continuation Sheet*;

      (2) SF 87, *Fingerprint Card*, (not required if a previous investigation included a classifiable fingerprint search by the FBI);

      (3) either SF 171, *Application for Federal Employment*; Optional Form 612 (OF 612), *Optional Application for Federal Employment*; or a resumé. If the individual submits an OF 612 or a resumé, an OF 306, *Declaration for Federal Employment*, must also be submitted;

      (4) DOE F 5631.18, *Security Acknowledgment*; and

      (5) DOE F 472.1, *Release (Fair Credit Reporting Act of 1970, as amended).*

   b. Others. All other individuals, including contractors, subcontractors, consultants, and access permittees, will submit an SF 86, an FD 258, *Fingerprint Card*, (not required if a previous investigation included a classifiable fingerprint search by the FBI), DOE F 472.1, and DOE F 5631.18 to apply for an access authorization.

   c. Processing Restrictions. Initial access authorization requests, reinvestigations, or other requests for an access authorization action cannot be processed:

      (1) unless all required forms have been legibly completed, signed (when appropriate), and provided by the applicant, access authorization holder, and/or sponsor;

      (2) if the preprinted content of the forms has been altered; or

      (3) if insufficient, incorrect, or conflicting information is provided.

   d. Additional Forms. As a condition of access authorization approval, individuals may be required to execute forms for investigative agencies to obtain specialized information concerning them. For example, SF 713, *Consent for Access to Records*, allows 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.

2. RECIPROCITY. Whenever possible, access authorizations are granted based on the interagency reciprocity procedures in this Section. Applicants for an access authorization will be processed in accordance with these procedures if they have been cleared or are in the process of being cleared by another Federal agency.

a. Individuals Being Cleared by Another Agency. DOE will not submit a request for investigation to the OPM or the FBI if the individual being processed by DOE is currently being investigated by these or another agency for access authorization or security clearance purposes, unless the type of investigation, when completed, will not be sufficient for DOE's needs. DOE will await the completion of that investigation then act in accordance with the provisions below, as necessary.

b. Individuals Cleared by Another Agency. As a basis for granting an access authorization, DOE will accept verification that the applicant currently has a security clearance, access authorization, or SCI approval granted by another Federal agency, provided the investigative basis meets the standards of investigation required for the DOE access authorization.

(1) Currency of Investigation.

(a) If a Q access authorization is to be granted, the investigation must have been completed or updated by reinvestigation within the past 5 years. If an L access authorization is to be granted, the investigation must have been completed or updated by reinvestigation within the past 10 years.

(b) If the most recent investigation or reinvestigation for an individual with a verified active security clearance, access authorization, or SCI approval at another Federal agency does not meet these time frames, a reciprocal access authorization will not be granted unless approved by the Director, Office of Security. Approval should only be requested when a current SF 86 does not reveal any unresolved security concerns and the requesting organization documents and the Departmental Element (or designee) certifies that the need for a reciprocal access authorization supports an urgent DOE requirement.

(2) Investigative Standards for Initial Investigation. The investigative standard for a Q access authorization is a Single Scope Background Investigation (SSBI). The investigation for an L access authorization processed before October 1997 was a National Agency Check with Credit (NACC). For L access authorization requests initially processed after October 1997, the investigation is a National Agency Check with Law and Credit (NACLC) for non-Federal employees and an Access National Agency Check and Inquiries (ANACI) for Federal employees.

(3) Investigative Standards for Reinvestigation. Until March 1997, the Federal Government did not have a defined investigative standard for reinvestigations, so each Federal agency established its own schedule and investigative standards for periodic reinvestigations. Therefore, if the previous security clearance or SCI approval is based on a reinvestigation, the DOE cognizant security authority must exercise judgment and latitude to determine if the reinvestigation used by the other Federal agency is acceptable.

(4) Determination of Investigation Date and Scope. DOE must accept the other agency's verification of the scope and date of the investigation used as the basis for a security clearance granted by that agency, as set forth in paragraph c.(1) below. DOE must take all reasonable measures to obtain existing investigative reports relied upon by the other agency to complete the personnel security file (PSF).

c. Procedures. The following steps will be taken to grant a reciprocal access authorization.

(1) Verify the date and basis of the security clearance, access authorization, or SCI approval and the individual's date and place of birth and citizenship with the Federal agency that granted it. The verification may be in writing or transmitted electronically.

(2) Obtain either a newly completed SF 86 or a copy of the most recently completed SF 86. A copy of a previously completed questionnaire may be submitted by the individual or the Federal agency that granted the security clearance, access authorization, or SCI approval. If the form does not come directly from the Federal agency where the individual is cleared, the individual must update, re-sign, and re-date it.

(3) Have the individual read and sign DOE F 5631.18, *Security Acknowledgment*.

(4) Grant an access authorization unless the individual is not a U.S. citizen, is a dual citizen, or DOE has an unresolved security concern.

d. Unresolved Issues. Any issues occurring after completion of the last investigation are considered unresolved unless the original agency has provided specific information indicating that such issues were favorably resolved. If security issues develop that require further adjudication, the appropriate action(s) should be initiated. This may involve delaying the access authorization action until receipt of the copy of the previous investigation. If it is clear that the issues of security concern were addressed and resolved by the original agency, those issues should not be adjudicated further.

e. Incomplete Investigative Report. If the investigative report documentation regarding the previously conducted NACC, NACLC, or ANACI does not contain

the actual results of the searches conducted, a new NACLC or ANACI may be requested.

f. Reinvestigation. If the individual's security clearance, access authorization, or SCI approval at the other Federal agency is terminated subsequent to DOE granting a reciprocal access authorization, DOE will assume the responsibility for processing a reinvestigation for the individual. If the individual is reinvestigated by the other agency, DOE will accept the investigative results in determining whether to continue the reciprocal access authorization.

3. ADDITIONAL REQUIREMENTS FOR CONTRACTOR REQUESTS.

a. The DOE contract or subcontract number under which the access authorization is requested must be indicated.

b. Certification of the individual's U.S. citizenship must be provided.

c. Requests for employees of management and operating contractors and other contractors managing DOE-owned facilities must be accompanied by pre-employment checks required by 48 CFR 970.2201(a)(1)(ii).

d. A contractor may submit access authorization requests to DOE for processing while a Foreign Ownership, Control, or Influence (FOCI) determination is pending (see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*). However, a favorable FOCI determination must be rendered by DOE and the facility code must be registered in the Safeguards and Security Information Management System (SSIMS) before an access authorization will be granted, reinstated, continued, extended, or transferred for any of the contractor's employees or applicants for employment.

4. INVESTIGATIVE REQUIREMENTS FOR ACCESS AUTHORIZATIONS. The following types of investigation are required for the type of access authorization shown.

a. Q Designated a "Position of a High Degree of Importance or Sensitivity." An SSBI is conducted by the FBI for the positions listed in appendix 3.

b. Q, QL, and QX. An SSBI is conducted by OPM or the FBI. When a QL is requested, the NAC, credit, and fingerprint portion is usually returned in advance of the background investigation, and an L access authorization can be granted if appropriate, pending completion and review of the SSBI. All of these access authorization types may also be based upon a background investigation by a Federal agency other than the FBI or OPM, provided the investigation meets the scope and extent of the required investigation and the investigation was conducted or updated by reinvestigation within the past 5 years.

c. QB. No investigation is required. The QB access authorization is granted by the Director, Office of Security, pursuant to section 145b of the Atomic Energy Act of 1954 when such action has been determined to be clearly consistent with the

national interest. This authority cannot be re-delegated. A QB access authorization must not be requested when an interim access authorization is appropriate or when an investigative report exists that may be used as a basis for an access authorization.

d. L and LX. For Federal employees, an ANACI; for all other individuals, an NACLC.

5. INVESTIGATIVE COSTS. Except for access permittees who reimburse DOE for investigation costs at rates established by DOE's Chief Financial Officer, DOE assumes security investigation costs associated with processing individuals for initial access authorizations and reinvestigations. DOE's Chief Financial Officer reserves the right to designate specific DOE programs or activities responsible for the reimbursement of such costs.

6. PRESCREENING. Upon receipt, personnel security cases must be prescreened by the processing DOE personnel security office to ensure the following:

a. All information, including proper forms for a full and timely investigation, is made available to the investigative agency. (Alterations to the printed content of the required forms will not be accepted and should be returned to the individual.)

b. Omissions or discrepancies on the SF 86 or other forms have been corrected.

c. The individual has provided the required explanation to any "Yes" answer to items 19 through 30 on the SF 86.

d. The individual has provided a social security number and place of birth for each individual listed in response to question 14 of the SF 86 who is coded "19," as being, "an adult living with you" (i.e., have a spouse-like relationship or similar bond of affection while living with the individual). The information can be written below the individual's name following question 14 or in the continuation space following question 30.

e. The proper justification for the need for an access authorization has been provided by the sponsoring entity.

f. Requests for employees of management and operating contractors and other contractors managing DOE-owned facilities are accompanied by the pre-employment checks required by 48 CFR 970.2201(a)(1)(ii), and all contractor requests are accompanied by a certification of the individual's U.S. citizenship. (See Attachment 2, Contractor Requirements Document.)

g. Any previously granted access authorization that can be reinstated, transferred, or extended is identified.

h. Current investigative reports that DOE can obtain and use as a basis for determining the individual's access authorization eligibility are identified.

i. Any individual concurrently being processed for an access authorization or security clearance by another Federal agency is identified.

j. Foreign national status or dual citizenship requiring approval or waiver from a Departmental Element before processing for investigation is identified (see chapter VI for more detail).

k. Derogatory information on the SF 86 that necessitates a higher level of investigation than would normally be required, is identified.

l. Any citizenship issues that will require additional action prior to submission for investigation are identified.

7. PERSONNEL SECURITY FILE (PSF). DOE must create and maintain a PSF in either paper or electronic form for each individual processed for an access authorization. The processing personnel security office will consecutively assign PSF numbers as individuals are initially processed for any type of access authorization. The PSF number will be used to identify that individual's file, regardless of the location of that PSF.

8. PROCESSING FORMS USED TO REQUEST INVESTIGATIONS.

a. The SF 86 must be used for all investigation requests submitted to OPM or the FBI. A copy of the completed SF 86 must be retained by the processing personnel security office submitting the request. OPM requires that no more than 120 calendar days may elapse between the date of execution of the certification on page 9 of the form and the date the form is received by the investigative agency. Forms older than 120 calendar days, or that would be more than 120 calendar days by the time the form could be transmitted and received by the investigative agency must be returned to the individual for updating and re-signing unless an appropriately executed Federal Investigations Processing Center (FIPC) form FIPC 391, *Certification of Amended Investigation Form*, is completed.

b. The SF 87, *Fingerprint Card*, must be used to process investigations of Federal employees. In all other cases, the FD 258, *Fingerprint Card*, must be used. The DOE PSF number should be inserted in the "Number" space on the FD 258 and below the "Title and Address" section of the SF 87. The type of access authorization requested can be stamped on the block titled "Reason Fingerprinted" or the block titled "Title and Address." "U.S. Department of Energy, Washington, D.C." must be typed in the space titled "ORI" if it is not already printed there.

(1) It is essential that personnel assigned to take fingerprints be able to recognize unclassifiable prints. If a print may be unclassifiable for obvious reasons (for example, a scar or missing finger), this must be noted on the fingerprint card in the box labeled "scars, marks, or tattoos."

(2) The unclassifiable or illegible fingerprint card submitted for a fingerprint retake must be attached to the newly obtained card. Retakes submitted to OPM must include the OPM serial number indicated on the previously rejected fingerprint card.

(3) Fingerprint retakes for individuals being investigated by OPM will be submitted to the following address:

U.S. Office of Personnel Management
FIPC
P.O. Box 618
1137 Branchton Rd.
Boyers, PA 16018-0618

(4) Fingerprint retakes for individuals being investigated by the FBI will be submitted to the following address:

Federal Bureau of Investigation
U.S. Department of Justice
Washington, D.C. 20535

(5) The access authorization determination may be rendered after the fingerprint retakes are submitted, provided the investigation is otherwise complete. Only one set of fingerprint retakes will be submitted for classification.

c. DOE F 5631.16, *File Summary Sheet*, must be used to record all official access authorization actions and placed in the individual's PSF.

9. OTHER FEDERAL AGENCY REQUESTS FOR ACCESS AUTHORIZATIONS. All requests for access authorizations for employees and contractors of other Federal agencies must be processed through the Director, Office of Security. If such employees are cleared by the other agency and need access to classified information while visiting DOE, they do not need DOE access authorizations if the certification procedures in DOE M 470.4-1, *Safeguards and Security Program Planning Management*, section L, are met. Department of Defense (DoD) and National Aeronautics and Space Administration (NASA) personnel may have access to Restricted Data under these certification procedures except in cases indicated below:

a. DoD and NASA personnel assigned to the DOE require DOE access authorizations and, in their assigned capacities, will be afforded access to Restricted Data on the same basis as DOE employees. When the situation warrants, they may be assigned to work on the basis of appropriate certification of security clearances from their agency, provided the requests for DOE access authorizations have been submitted. Restricted Data received by such personnel during their assignment with DOE must be handled in accordance with DOE security requirements.

b. When DoD and NASA personnel assigned to other Federal agencies require DOE access authorizations, the requests must be initiated by the agency to which they are assigned.

10. DOE AND DOE CONTRACTOR PERSONNEL ASSIGNED TO DoD OR NASA. Any DOE or DOE contractor employee acting as a consultant or member of a DoD or NASA advisory board who, in that capacity, possesses the appropriate DoD or NASA security clearance will, for the purposes of this Manual, be considered a temporary DoD or NASA employee. In this capacity, the individual may communicate Restricted Data to DoD or NASA personnel and their contractors in accordance with the DoD or NASA security requirements. If the DOE employee or contractor does not require an access authorization for DOE work but does require a personnel security clearance for assignment to the other agency, the other agency must request the appropriate investigation, adjudicate the reported information, and grant the appropriate personnel security clearance.

11. ADDITIONAL REQUIREMENTS FOR CASES INVOLVING FOREIGN RESIDENCE, EMPLOYMENT, OR OTHER ACTIVITIES IN A FOREIGN COUNTRY. If upon review of the SF 86, the processing personnel security office finds it unlikely that an adequate investigation is possible because the case involves residence, employment, or other activities in a foreign country, all material pertaining to the case will be forwarded to the Office of Security for coordination with the appropriate investigative agencies. The Office of Security will then advise the processing personnel security office on whether sufficient information can be obtained to determine the individual's eligibility for an access authorization.

12. RECEIPT OF COMPLETED INVESTIGATIVE REPORTS. OPM and the FBI forward reports of investigations directly to the processing personnel security office. Each processing personnel security office must enter both the date the reports were completed and the date the reports were received into the Central Personnel Clearance Index (CPCI) within 2 working days of receipt of the reports.

13. CANCELLATION OF REQUESTS FOR ACCESS AUTHORIZATION OR INVESTIGATION. DOE must request the investigating agency to discontinue its investigation immediately when notified that the individual no longer requires an access authorization. The CPCI must be updated to reflect cancellation of the investigation within 2 working days of receipt of notification. If the access authorization is to be terminated by one DOE processing personnel office because the individual is transferring to another DOE processing personnel security office and will still require an access authorization, the terminating office should not cancel the investigation. When the report of investigation is received, it should be sent to the appropriate DOE personnel security office for adjudication.

14. TYPES OF INVESTIGATIONS. The following are the types of investigations most frequently conducted for the DOE:

a. Single Scope Background Investigation (SSBI). The SSBI is a full-field background investigation covering the most recent 10 years of the individual's life. An NACC, an interview with the individual, and a National Agency Check on the individual's spouse or cohabitant are also conducted.

b. Single Scope Background Investigation - Periodic Reinvestigation (SSBI-PR). The SSBI-PR is a background investigation covering the most recent 5 years of the individual's life. The individual's name is checked with appropriate Federal agencies and a credit search is conducted. This investigation is used for reinvestigations of individuals holding Q access authorizations.

c. National Agency Check with Law and Credit (NACLC). The NACLC is a name check of the individual at appropriate Federal and local law enforcement agencies, a credit search, and a classification of the individual's fingerprints by the FBI. NACLCs are used for the initial investigation of contractor employees who require L access authorizations and for reinvestigations of all individuals holding L access authorizations.

d. Access National Agency Check and Inquiries (ANACI). The ANACI is a name check of the individual at appropriate Federal and local law enforcement agencies, a classification of the individual's fingerprints by the FBI, a credit search, and written inquiries regarding the individual's employment, education, residences, and references. An ANACI is used for the initial investigation of Federal employees requiring L access authorizations.

e. Upgraded Investigation. The type of investigation requested may be upgraded to a more extensive investigation if the case appears to involve significant derogatory issues. OPM can also conduct other investigations of varying scopes to meet the particular needs of a given case for additional cost on a case-by-case basis; for example, a Special Update Investigation to cover the most recent 18 months of the individual's activities.

f. Background Investigations by Other Federal Agencies. Reports of investigation by other Federal agencies (e.g., the Defense Security Service or Department of State) must be accepted in lieu of a new investigation provided that:

(1) the investigation meets the scope and extent of the required investigation; and

(2) the investigation was completed, or updated by reinvestigation, within the most recent 5 years.

15. INCOMPLETE INVESTIGATIONS. In certain situations, OPM will close out a case before the investigation is completed. The outstanding portion of the investigation will be clearly identified by OPM. The processing personnel security office may, when the situation so requires, grant an access authorization provided that as a minimum:

a. a review of the SF 86 and the incomplete investigation is favorable;

b. the incomplete information is documented in the case file; and

c. a further review of the case will be made when the missing information is received from OPM.

16. PROCESSING CLEARED INDIVIDUALS TRANSFERRED TO POSITIONS OF A HIGH DEGREE OF IMPORTANCE OR SENSITIVITY.

The Atomic Energy Act requires that the FBI conduct background investigations on individuals who occupy positions certified by DOE to be of a high degree of importance or sensitivity. When a currently Q-cleared individual is selected for such a position, the field element manager may authorize the transfer to the new position provided:

a. the existing PSF is reviewed by the processing personnel security office before the transfer takes place and this review does not reveal any unresolved derogatory information;

b. the most recently conducted investigation is not more than 5 years old; and

c. the individual must be processed for an FBI reinvestigation when the existing investigation becomes 5 years old.

17. RE-INITIATION OF CASES ADMINISTRATIVELY TERMINATED IN ACCORDANCE WITH 10 CFR 710.6. If an individual fails to comply with a request for information, access authorization processing may be terminated under the procedures in 10 CFR 710.6. If the individual later complies with the request, the process may be reopened and activities resumed at the same point at which the process was terminated. Before the investigation can be reopened, the individual's employer must re-certify the continued need for the individual to have an access authorization and the individual may be required to submit updated security forms.

18. ACCESS AUTHORIZATION DOCUMENTATION. DOE maintains a personnel security automated information system for recording all access authorization transactions. When an access authorization has been granted, the processing personnel security office must make the appropriate entry into the CPCI within 2 working days. The processing personnel security office will also update the File Summary Sheet in the individual's PSF and notify the requesting office.

19. DOE CUSTODY OF PERSONNEL SECURITY FILES. The dissemination of personnel security information and PSF data must be controlled in accordance with the Privacy Act of 1974, as amended, and DOE directives.

a. Because of the privileged nature of the information contained in investigative reports and PSFs, they must be made available within DOE only to individuals who have been the subject of a favorably adjudicated background investigation and are authorized to process or adjudicate an access authorization, determine suitability for Federal employment, certify individuals in the HRP, conduct official investigations into violations of criminal or civil law, or ensure

compliance with DOE requirements. Appropriate handling, transmission, and storage methods must be used to comply with this requirement. Information contained in the PSFs must not be made available to contractor representatives. The term "contractor representatives" does not include those contractor employees who are assigned to DOE personnel security offices for purposes of processing personnel security information. A psychiatrist conducting an evaluation at the request of DOE may be permitted access to the information contained in the background investigation.

b. Reports of investigations of individuals who have been processed for access authorizations may be shown to representatives of other Federal agencies or other entities identified as routine users in the DOE System of Records 43, Personnel Security Files. Such representatives must show that they have an official interest in the investigation. Representatives must not be given copies of an investigation conducted by another Federal agency, but will be advised that the reports may be requested directly from the FBI, OPM, or other Federal investigative agency that originated the report. Authorized representatives may review the contents of the PSF and may be provided copies of information from the PSF (other than the investigative reports).

c. Pursuant to the Privacy Act of 1974, 5 U.S.C. 552a(b)(7), information may be released "to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the U.S. for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the records specifying the particular portion desired and the law enforcement activity for which the record is sought."

d. In accordance with the Privacy Act of 1974, 5 U.S.C. 552a(c)(1) and internal procedures, a record of each disclosure of a PSF as described in paragraphs 19.b. and c. above must be noted in the file as follows:

(1) name of the person to whom the disclosure is made;

(2) agency represented and address;

(3) date;

(4) nature and purpose of the disclosure; and

(5) name of the DOE employee releasing the information.

e. Disclosure of certain information in the background investigation to other DOE employees who need the information to perform official duties connected with the purposes for which the information was collected is permitted by the Privacy Act of 1974, 5 U.S.C. 552a(b)(1).

f. Before the release of a PSF containing classified information, the DOE employee responsible for releasing the file must be assured that the reviewer possesses the appropriate type of access authorization or security clearance and has an official need-to-know.

20. INDIVIDUALS SEEKING ACCESS OR AMENDMENT TO THEIR PERSONNEL SECURITY FILES. PSFs are a system of records under DOE control and are subject to 10 CFR 1008, "Records Maintained on Individuals (Privacy Act)," regarding their release. That regulation establishes the procedures for individuals who wish to review, obtain a copy of, or amend the contents of their PSFs. Specific instructions for submitting a Privacy Act request are in 10 CFR 1008.6, "Procedures for Privacy Act Requests." Further information on how to submit a request for access can be obtained by contacting the cognizant Privacy Act Officer. Individuals must not be given access to investigative reports. Requests for access to these reports must be referred to the agency that conducted the investigation.

21. CONTENTS AND ARRANGEMENT OF DATA IN PERSONNEL SECURITY FILES.

a. The PSF of any individual who is being or has been processed for an access authorization, whether active or terminated, will contain the original or a copy of any document related to an investigation, including an investigative report prepared by a Federal investigative agency or any documents, correspondence, or forms involving the individual subsequent to the initial access authorization action. The PSF will be arranged so that administrative material is fastened to the left side and adjudicative material is fastened to the right side. Material on each side of the folder will be arranged chronologically with the oldest on the bottom progressing to the newest on the top.

b. Administrative materials are memorandums and other correspondence relating to administration of the case including requests for access authorizations; prescreening forms; notes to the file (except notes containing investigative or adjudicative data); requests to other offices for interviews; security advisory letters; suspension correspondence, notification letters, and responses thereto; correspondence relating to special access authorizations; security badge and briefing forms; and similar data. A File Summary Sheet (DOE F 5631.16 or equivalent) must be placed on top of all other material on the left side of the PSF.

c. Adjudicative materials are all investigative materials relating to the access authorization determination, including the questionnaire completed by the individual, fingerprint cards, release forms, and security acknowledgment; reports of investigation from any Federal agency or local law enforcement activity, the Office of the Inspector General, or contractor security personnel; documentation regarding security infractions; letters, memorandums, or notes to file containing investigative data; summaries of investigation; incident reports, reports of hospitalization for a mental illness, treatment for drug abuse, or treatment for alcohol abuse; interview transcripts or summaries; letters of interrogatory to the individual and responses thereto; correspondence and reports relating to

psychiatric and/or psychological evaluations; case evaluations; and any other material relating to the adjudication of the individual's eligibility for an access authorization.

22. RETENTION OF PERSONNEL SECURITY FILES. PSFs must be retained and disposed of in accordance with the approved National Archives and Records Administration (NARA)/DOE Records Schedules. The schedule for these records calls for personnel security files to be destroyed 10 years after the termination, discontinuance, or cancellation of an access authorization.

# CHAPTER III
# INVESTIGATIVE RESULTS PROCESS AND ACCESS AUTHORIZATION DETERMINATIONS

1. SCREENING. When an investigative report is received, a personnel security specialist must review it to ensure that the required DOE scope of investigation for the particular type of access authorization has been met and that all derogatory and mitigating information has been identified.

   a. Background Investigations (Initial Investigations or Reinvestigations).

      (1) The report must be reviewed to ensure that thorough information is provided on the individual's residence, employment, education, and military service, and that checks of references, credit, and law enforcement have been completed.

      (2) All derogatory and mitigating information, as well as any missing elements of investigative coverage, must be documented with the date and signature of the reviewer. Under certain circumstances (chapter II, paragraph 15.), it is appropriate to proceed with adjudication even if information is missing. The individual's employer, as listed on the SF 86, must be checked against the employer as reported in the investigation to ensure they are identical; if not identical, a check will be conducted to determine if the reported employer (i.e., the current employer) has submitted a request for access authorization and if it has been approved for the same type of access authorization.

      (3) Cases for which the investigation is complete and no derogatory information has been reported must be appropriately documented. If the reviewer has been delegated authority in writing to grant an access authorization, the granting must be so noted in the file. At least 5 percent of such cases must be reviewed by a senior personnel security specialist to ensure the investigation is, in fact, complete and contains no derogatory information. Such verification of review will be documented by the date and signature of the reviewer on the File Summary Sheet (DOE F 5631.16) or equivalent.

   b. National Agency Checks. Individuals screening these investigations must determine whether all items have been covered. Derogatory and mitigating information must be listed and documented with the date and signature of the screener. If there is no derogatory information, the procedures listed in paragraph 1.a.(3) above should be followed.

2. ANALYSIS. Only DOE employees who are so authorized in writing may 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 information or matter, or SNM, before notifying the DOE cognizant security authority.] DOE employees authorized to render access authorization eligibility determinations must receive training in the DOE personnel security process prior to actually rendering such determinations.

a. Favorable and unfavorable investigative information must be analyzed according to the criteria found in 10 CFR 710.8. Frequently, the reported derogatory information alone raises a security concern but may be resolved when considered with other reported mitigating information.

b. When information contained in investigative reports or the receipt of other reliable information raises a question concerning an individual's eligibility for an access authorization, additional actions may be authorized for collecting relevant information pertaining to the eligibility determination. If the question is favorably resolved, the access authorization may be granted, continued, or reinstated. If the question cannot be favorably resolved, the individual's access authorization eligibility must be determined under 10 CFR 710. Additional actions, such as those described in paragraphs 4. through 7. below, may be required to adjudicate a case. If one of these actions is necessary, the approval for such action must be by a senior personnel security specialist other than the specialist making the recommendation.

c. If an investigation is complete, the authorized DOE employee (as defined in paragraph 2. above) may grant or continue an access authorization based on the existing record if:

(1) the file is clear of derogatory information;

(2) the post-investigative record fully mitigates any derogatory information; or

(3) an interview and/or other supplementary fact-finding effort has resolved all security concerns documented in the record.

d. DOE's final determination regarding the eligibility for an access authorization will be provided in writing or electronically to the employer or prospective employer who initiated the request. This information may also be furnished to representatives of DOE contractors or to Federal agencies having an official interest in the individual. If there is reason to notify the individual in writing of the final determination, such as at the completion of the administrative review process, as defined in 10 CFR 710, or the granting of an interim access authorization in accordance with chapter IV, 2.g. of this Manual, the notification will be in the form of a letter or memorandum, but no official DOE form reflecting the granting of an access authorization will be enclosed.

e. If it is determined by the DOE cognizant security authority that reported information falls within one or more of the categories in 10 CFR 710.8 and the case cannot be resolved locally, then the access authorization must be suspended

or recommended for denial. A duplicate of the PSF, a summary statement, and a request for authority to initiate administrative review processing under 10 CFR 710 must be transmitted to the Director, Office of Security. The individual's employer, any other Departmental Element having an access authorization interest in the individual, and any other Federal agency for which the individual holds an access authorization, security clearance, or SCI approval, or to which DOE has certified the individual's access authorization, must be notified immediately of the suspension action. The CPCI must also be immediately updated and the individual's badging office notified.

f. Any case may be referred to the Director, Office of Security, for review and advice. Any case referred must reflect the rationale and recommendations for further action.

3. ACTIONS AUTHORIZED BY THE DOE OFFICE OF SECURITY. The Director, Office of Security, must review all cases referred under 10 CFR 710.10 and may:

a. direct specific additional actions to be taken in the case, such as an interview, additional investigation, or psychiatric evaluation;

b. authorize the granting or reinstatement of an access authorization; or

c. authorize an administrative review (10 CFR 710.20, et seq.).

4. PERSONNEL SECURITY INTERVIEWS. Personnel security interviews (PSIs) must be conducted only by personnel security specialists appropriately trained and cognizant of all the questions or items of information to be explored. DOE F 5631.5, *The Conduct of Personnel Security Interviews Under DOE Security Regulation*, and DOE F 5631.7, *Privacy Act Statement for Personnel Security Interviews and Release Forms Related Thereto*, must be properly executed for all PSIs. All PSIs will be audio or audio/video recorded. The PSI will then be transcribed or summarized. If a transcript is not prepared, the recorded PSI must be retained and protected in the same manner as the PSF.

5. LETTERS OF INTERROGATORY. An alternative to a PSI is the letter of interrogatory, which may be sent to an individual if the derogatory information requires clarification, or if the geographic location of the individual would make it extremely difficult to arrange a PSI. Letters of interrogatory must include a deadline for the individual to provide the response. The individual's response will be evaluated to determine whether the security concern that prompted the letter has been resolved.

If the individual's response does not favorably resolve the security concern, further adjudicative action must be taken.

6. ADDITIONAL INVESTIGATION. When an additional investigation is required to expand, resolve, or corroborate information, the processing personnel security office will submit a request for such investigation to either the OPM or the FBI, as appropriate.

7. DRUG CERTIFICATIONS. If information indicates that the individual has illegally used or trafficked in a controlled substance as defined in the Controlled Substances Act of 1970 (21 U.S.C. 812), that information, including the extent and duration of such drug involvement and the individual's intentions for future involvement, must be evaluated. The individual may be given an opportunity to certify in writing on a DOE F 5631.9, *Drug Certification*, that he or she will no longer engage in such activity. If, after being granted an access authorization (or having an access authorization continued), the individual who signed a DOE F 5631.9 violates its terms, an immediate evaluation of the circumstances of that violation must be conducted.

8. CASES INVOLVING MENTAL ILLNESS OR MENTAL CONDITION. To assist in determining whether reported information about a mental illness or condition falls within 10 CFR 710.8, the following procedures will be implemented:

   a. A DOE or contractor supervisor must report to the processing personnel security office when an individual under their cognizance, who holds an access authorization, is hospitalized for mental illness or receives other treatment for a condition that, in the supervisor's opinion, may cause a significant defect in the individual's judgment or reliability. Verbal notification must be made within 8 working hours, and written confirmation within the next 10 working days. The individual's access authorization will be continued unless the processing personnel security office finds convincing evidence that there is a significant defect in the individual's judgment or reliability as described in 10 CFR 710.8(h).

   b. To aid in determining the individual's judgment or reliability, the processing personnel security office may accept previously rendered competent medical advice or records that are in the possession of DOE or a DOE contractor. The processing personnel security office may also have a board-certified psychiatrist or a licensed clinical psychologist designated by DOE conduct a mental evaluation. Any referral to a DOE-designated psychiatrist or psychologist must be approved by the head of the processing personnel security office. In such a case, the individual will be requested to submit to an examination and to execute a consent form (DOE F 5631.10, *Waiver*) for the examination.

      (1) The examining psychiatrist or psychologist must submit to the processing personnel security office a written report containing an opinion on whether the individual suffers from a mental illness or condition that causes or may cause a significant defect in judgment or reliability.

      (2) If the individual refuses to submit to an examination, the individual's access authorization may be terminated in accordance with 10 CFR 710.6.

   c. If a psychiatric or psychological examination is conducted as described in paragraph 8.b. above, the DOE-designated examiner must be notified that they may be called upon to testify before a hearing officer. Only psychiatrists or psychologists consenting to testify should be designated for examining purposes.

9. UPDATED SECURITY FORMS. The processing personnel security office may request updated security forms at any time when there is probable cause to believe that the individual may have engaged in an activity or been subject to circumstances that may affect continued access authorization eligibility.

10. TIME ELEMENTS IN PROCESSING ACCESS AUTHORIZATIONS.

a. Cases not containing derogatory information. Initial screening and either granting or continuing (after a reinvestigation) of an access authorization will be accomplished within 7 working days of the receipt of a completed investigation or reinvestigation that has been evaluated and found not to contain derogatory information.

b. Cases involving derogatory information. Within 30 working days of the receipt of a completed investigation that has been evaluated as containing derogatory information, one of the following actions must take place.

(1) Access authorization will be granted or continued.

(2) Additional investigation will be requested.

(3) A PSI will be scheduled with the individual.

(4) A letter of interrogatory will be sent to the individual.

(5) The case will be referred to the Director, Office of Security, with a request for authority to initiate administrative review processing under 10 CFR 710.

(6) The case will be referred to the Director, Office of Security, for review and advice.

(7) Cases involving DOE employees that contain information relevant to suitability determinations will be referred to the servicing personnel office as described in item 12 below.

c. Time elements for processing cases that are in administrative review are in 10 CFR 710.

11. EMPLOYER INQUIRIES. Once an individual is notified of the opportunity to request a hearing before a hearing officer, the individual's employer may, upon inquiry, be informed of the status of the case but not of the information requiring initiation of administrative review processing.

12. SUITABILITY DETERMINATIONS FOR FEDERAL EMPLOYEES AND REFERRALS TO SERVICING PERSONNEL OFFICES.

a. DOE Employees and Applicants for DOE Employment. Derogatory or discrepant information developed as part of the personnel security process may be relevant to the suitability for Federal employment of a DOE employee or an applicant for DOE employment or may require disciplinary action by the servicing personnel office. Each processing personnel security office must establish procedures with the servicing personnel office(s) for the DOE employees under their jurisdiction for the referral of such information so the servicing personnel office can take appropriate action regarding the individual's employment status. Ordinarily, any adverse action proceedings of the servicing personnel office must be completed before initiation of administrative review processing of the individual's eligibility for an access authorization. However, a referral to the servicing personnel office does not preclude suspension of the individual's access authorization.

b. Other Federal Agency Employees and Consultants. In cases where employment suitability information is developed on an employee or consultant of another Federal agency, the report of investigation will first be reviewed by the hiring agency or official. A non-DOE Federal official must notify DOE Headquarters Personnel Security within 30 working days if action will be taken against the individual. Unless DOE security officials consider it necessary for security reasons to proceed with the access authorization eligibility determination before a determination of employment eligibility, the employment decision must be rendered first.

# CHAPTER IV
# INTERIM ACCESS AUTHORIZATIONS AND WAIVERS OF PRE-APPOINTMENT INVESTIGATIONS

1. GENERAL. Only under exceptional circumstances and when such action is clearly consistent with the national interest will an individual, before completion of the appropriate investigation, be permitted to have access to classified information or matter, or SNM, or be allowed to occupy a Federal position designated by the cognizant personnel office as Critical-Sensitive. In all such cases, Interim Access Authorizations (IAAs) to Restricted Data, National Security Information, or SNM, or waivers of pre-appointment investigations, must be considered temporary measures pending completion of the investigation, which must be in process. The use of IAAs must be kept to the absolute minimum and considered only when properly requested in accordance with procedures in this Manual. An IAA to Restricted Data, National Security Information, or SNM must be approved by the Director, Office of Security. A waiver of a pre-appointment investigation must be approved by the Secretary. Individuals who are dual citzens or non-U.S. citizens must not be processed for IAAs.

2. INTERIM ACCESS AUTHORIZATION TO CLASSIFIED INFORMATION OR MATTER OR SNM.

   a. A written request for an IAA will be submitted to the Director, Office of Security, and must be supported by a certification that:

      (1) serious delay of, or interference in, an operation or project essential to a DOE program will occur unless the named individual is granted access to Restricted Data, National Security Information, or SNM before completion of the access authorization procedures; and

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

   b. If an investigation was not requested before the request for an IAA, the investigation request accompanied by the forms required for the access authorization must be submitted concurrently with the request for an IAA. Expedited service for the background investigation must be requested from OPM or the FBI.

   c. When the request for an IAA and the appropriate DOE security forms are received, the Office of Security will review the forms and conduct other agency indices checks as appropriate.

   d. Individuals who require an IAA in connection with a Q access authorization may be offered the opportunity to voluntarily participate in the DOE Accelerated Access Authorization Program (AAAP), which involves completion of an NACC, psychological assessment, drug testing, and counterintelligence scope polygraph examination at the DOE Test Centers, Albuquerque, New Mexico, or Oak Ridge,

Tennessee. Transportation and per diem costs for such processing are the responsibility of the individual's program office or employer. Additional information concerning the AAAP is available from the processing personnel security office. AAAP information brochures may be requested by calling the Albuquerque Test Center at (505) 346-7752 or the Oak Ridge Test Center at (865) 576-2446.

e. For an L access authorization, the SF 86 will be coded to request advance NAC and fingerprint reports by entering Extra Coverage Code '3' in block B and Special Coverage Code 'R' in the Codes block of part 1. The interim L will be granted if the results of both the NAC and fingerprint check are favorable.

f. Any derogatory information developed as part of these checks must be documented by the Office of Security and provided to the official determining eligibility for the IAA or granting the waiver of the pre-appointment investigation.

g. The requester must be notified of the determination to grant or deny an IAA in accordance with chapter III, paragraph 2.d., and if an IAA is granted, the individual must be notified in writing that:

(1) access is granted only to identified categories of classified information or matter, or SNM, necessary to perform specified duties;

(2) the IAA is valid until the investigation and adjudication processes are completed and may be canceled by the Director, Office of Security, at any time based on unfavorable information;

(3) cancellation cannot be appealed and adjudication of the individual's eligibility for access authorization will continue upon receipt of the completed investigation; and

(4) cancellation denies access to classified information or matter, or SNM, and assignment to any position requiring such access.

h. An individual with an IAA may be certified for a classified visit outside the DOE complex, provided that the receiving agency is furnished, and acknowledges understanding of, information regarding the IAA's investigative basis.

i. If DOE cancels an individual's IAA, the processing personnel security office must notify the individual's employer in writing. The individual's employer must then ensure that the individual is precluded from access to classified information or matter, or SNM.

j. When DOE grants, denies, or stops processing the access authorization, the IAA must be canceled. The CPCI must be updated to reflect this action within 2 working days.

3. WAIVER OF PRE-APPOINTMENT INVESTIGATION. DOE will process requests for waivers of pre-appointment investigations in accordance with the procedures established by OPM in 5 CFR 732 and 736. The pre-appointment investigation requirement may not be waived for appointment to positions designated Special-Sensitive. Guidelines for determining position sensitivity are in 5 CFR 732. The pre-appointment investigation requirement for persons entering Critical-Sensitive positions may be waived only for a limited period and only if the Secretary finds that such action is necessary and in the national interest and such finding is made a part of DOE records.

# CHAPTER V
# INDIVIDUAL RESPONSIBILITIES AND REPORTING REQUIREMENTS

1. GENERAL. An individual applying for or granted a DOE access authorization must report truthfully all information requested for personnel security purposes and must authorize others to report such information. The individual has a specific obligation to report certain personnel security-related matters as they occur.

2. RESPONSIBILITIES.

   a. Access authorization applicants and holders must provide full, frank, and truthful answers to relevant and material questions.

   b. When requested, access authorization applicants and holders must furnish or authorize others to furnish information that DOE deems pertinent to the access authorization eligibility process.

   c. These responsibilities apply when completing security forms, during the course of an initial background 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 an access authorization. In this event, any access authorization in effect may be terminated or, for applicants, further processing may be suspended (refer to 10 CFR 710.6[a]).

3. SPECIFIC REPORTING REQUIREMENTS.

   a. Legal, Employment, and Medical Information. Access authorization applicants and holders must provide direct notification to the cognizant DOE personnel security office of the following (NOTE: Verbal notification is required within 2 working days followed by written confirmation within the next 3 working days):

      (1) any arrests, criminal charges (including charges that are dismissed), or detentions by Federal, State, or other law enforcement authorities for violations of law within or outside of the U.S. Traffic violations for which a fine of up to $250 was imposed need not be reported, unless the violation was alcohol or drug related;

      (2) personal or business-related filing for bankruptcy;

      (3) garnishment of wages;

      (4) legal action effected for a name change;

      (5) change in citizenship;

(6) employment by, representation of, or other business-related association with a foreign or foreign-owned interest or foreign national; or

(7) hospitalization for a mental illness; treatment for drug abuse; or treatment for alcohol abuse.

b. Spouse/Cohabitant Information. Access authorization applicants and holders must provide two completed copies of DOE F 5631.34, *Data Report on Spouse/Cohabitant*, directly to the processing personnel security office, within 45 working days, of marriage or cohabitation. NOTE: A cohabitant is a person who lives with the individual in a spouse-like relationship or with a similar bond of affection, but is not the individual's legal spouse, child, or other relative (in-laws, mother, father, brother, sister, etc.).

(1) For an individual holding or applying for a Q access authorization whose new spouse or cohabitant is either a foreign national or a dual citizen, an Office of Personnel Management (OPM) National Agency Check (without fingerprint cards) will be requested on the new spouse or cohabitant by submitting two copies of the DOE F 5631.34 and a completed OFI 86C, *Special Agreement Checks*. The OFI 86C should be overprinted with the current agency agreement number and "S" should be entered in box 7 of the form.

(2) For an individual holding or applying for an L access authorization whose new spouse or cohabitant is either a foreign national or a dual citizen, the DOE F 5631.34 should be forwarded to the Office of Security, which will arrange for the appropriate indices check.

c. Information on Unauthorized Access Attempts. Access authorization applicants and holders must notify the processing DOE personnel security office or the facility security officer, as appropriate, immediately after any approach or contact by any individual seeking unauthorized access to classified information or matter, or SNM. If such an approach or contact is made while on foreign travel, the notification must be made to Department of State official at the local United States Embassy or Consulate with a request that the Department of State report the incident to the Director, Office of Security at DOE Headquarters. These requirements are in addition to any similar reporting requirements implemented under other DOE directives.

# CHAPTER VI
# ACCESS AUTHORIZATIONS FOR FOREIGN NATIONALS AND DUAL CITIZENS

1. REQUIREMENTS. Where there are compelling reasons in furthering the DOE mission, foreign nationals (to include immigrant aliens) with a special expertise that is not possessed to a comparable degree by an available U.S. citizen may be granted access authorization only for specific programs, projects, contracts, licenses, certificates, or grants for which the individual needs access to classified information or matter, or SNM. Such individuals will not be eligible for access to any greater level of classified information than the U.S. Government has determined may be releasable to the country of which the individual is currently a citizen, and such limited access may be approved only if the prior 10 years of the individual's life can be appropriately investigated. Additional lawful investigative procedures must be fully pursued to allay any doubts concerning the granting of access. A request to process a foreign national for an access authorization must be approved by the Departmental Element with jurisdiction over the program where the individual will be employed, the Office of General Counsel, and the Office of Security, before submission for investigation. A foreign national granted an access authorization must not receive access to the following types of classified information or matter:

   a. Top Secret, CRYPTO, or COMSEC information, except classified keys used to operate secure telephone units (STU IIIs);

   b. Intelligence or Special Access Program (SAP) information;

   c. information that has not been determined to be releasable by a U.S. Government Designated Disclosure Authority to the country of which the individual is a citizen;

   d. NATO Information, although a foreign national of a NATO member nation may be authorized access to NATO Information provided that:

      (1) a NATO Security Clearance Certificate is obtained by DOE from the individual's home country; and

      (2) NATO Information access is limited to performance on a specific NATO contract.

   e. information for which foreign disclosure has been prohibited in whole or in part (identified as NOFORN); and

   f. classified information furnished by a third-party government, and information provided to the U.S. Government in confidence by a third-party government (identified as FGI).

2. FOREIGN NATIONALS.

   a. The DOE cognizant security authority must:

(1) receive and consider requests for access authorizations for foreign nationals under their jurisdiction. Requests may be disapproved by the DOE cognizant security authority if the requirements of paragraph 1. above have not been met;

(2) interview the foreign national to determine steps taken by the individual to become a U.S. citizen; previous civilian or military service with a foreign government; family or other relatives abroad; family, legal, and financial ties abroad; and employment of relatives by a foreign government;

(3) evaluate the risk arising from foreign national status, considering the following factors:

(a) the nationality of the foreign national,

(b) whether a sufficient security investigation can be conducted,

(c) length of stay in the U.S.,

(d) family, legal, and financial ties abroad, and

(e) whether and in what manner the foreign national has shown the intent to become a U.S. citizen;

(4) transmit the request to the Director, Office of Security, if it is determined that an adequate investigation can be conducted and the evaluation of risks described in subparagraph (3) above is favorable. The DOE cognizant security authority must include the following with the request:

(a) a duplicate PSF, including the paperwork completed by the individual and a transcript of the interview;

(b) a statement concerning the program for which the foreign national has been recruited and the specific access to classified information or matter, or SNM, to be afforded; and

(c) a statement that a favorable risk evaluation has been completed based upon the factors described in subparagraph (3) above.

b. The Director, Office of Security, must:

(1) coordinate the following reviews/determinations:

(a) The Departmental Element with programmatic authority for the relevant project must review the request for a foreign national's access authorization and determine whether the individual in question possesses special expertise necessary to a DOE program;

(b) The review of the request for a foreign national access authorization to determine compliance with the requirements of the Atomic Energy Act concerning the release of Restricted Data to the government of the country where the foreign national holds citizenship. (NOTE: Release of Restricted Data to a foreign national is considered as release to that individual's country of citizenship.)

(2) evaluate the security risk arising from foreign national status, taking into consideration those factors in paragraph 2.a.(3) above, and determine whether the potential contribution of the individual outweighs the security risk arising from foreign national status; and

(3) notify the processing personnel security office that the case has been approved for processing and may now be submitted for investigation if favorable determinations have been made as a result of the reviews described in paragraphs 2.b.(1) and (2) above.

c. For foreign nationals, an SSBI is required for any type of access authorization.

d. The determination to grant an access authorization to a foreign national can only be made by the DOE cognizant security authority or, in Headquarters, by the Director, Office of Security, without power of redelegation.

e. An access authorization for a foreign national may only be extended, reinstated, or accepted for transfer with the concurrence of the Departmental Element having functional interest in the work to be done and after a new review as described in paragraph 2.b.(1)(b) above.

f. The Office of Security must maintain duplicate PSFs on all foreign nationals holding access authorizations. The processing personnel security office must provide copies of any additions to the PSFs on these individuals. Change of the individual's citizenship status must be reported to the Office of Security.

3. DUAL CITIZENS. Individuals who possess a dual citizenship (i.e., who are simultaneously a citizen of the U.S. and another country) and who have exercised citizenship rights in the foreign country, or have represented themselves as citizens of the foreign country, or who have intentions to do so in the future, must meet the requirements for foreign nationals in paragraphs 1. and 2. above. There are two alternatives to being processed as foreign nationals, as described below:

a. Renunciation of the Citizenship in the Other Country. If the individual is willing to renounce citizenship in the other country, the individual must provide a notarized statement attesting to the fact that the non-U.S. citizenship has been formally renounced, and if available, evidence that the renunciation has been formally accepted by an official representative of the other country's government. Copies of documents completed by the individual to formally renounce non-U.S. citizenship must accompany the notarized statement. An individual's statement

of renunciation must be considered invalid if the individual continues to exercise citizenship rights in a foreign country.

b. Waiver. The DOE cognizant security authority, or the Director, Office of Security, for Headquarters cases, may waive the requirement to renounce the non-U.S. citizenship if it is determined that it would be detrimental to the individual or to DOE security objectives, or that the risk associated with the individual maintaining the non-U.S. citizenship status has been adequately mitigated. A copy of the security evaluation documenting this waiver must be maintained in the individual's PSF.

# CHAPTER VII
# EXTENSIONS, TRANSFERS, TERMINATIONS, AND REINSTATEMENTS OF ACCESS AUTHORIZATION

1. EXTENSIONS AND TRANSFERS.

a. Extensions. 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 Departmental Elements, two or more employers, or one employer under two or more contract numbers.

(1) A Q access authorization can be extended as either a Q or an L access authorization, but an L access authorization can be extended only as an L access authorization. An access authorization must not be extended to a Departmental Element where the individual is not employed or does not perform contractual duties.

(2) QX and LX access authorizations cannot be extended as they are granted for limited access as specified in an access permit.

(3) When derogatory information develops after an access authorization has been extended, the processing personnel security office in possession of the new information must notify all offices having an access authorization interest in the individual.

(4) In extensions, the processing personnel security office that granted the oldest active access authorization must be indicated on the CPCI as being the PSF location and will be responsible for the reinvestigation. The only exception is when the subsequent access authorization extension results in a higher type of access authorization. In such cases, the processing personnel security office granting the higher type of access authorization will be indicated as the PSF location and must implement the reinvestigation requirements.

(5) If the processing personnel security office that originated the access authorization terminates the access authorization, the PSF must be sent to the processing personnel security office to which the access authorization had been extended as described in paragraph 4 below.

b. Transfers. Transfer of an access authorization requires a personnel security office to accept the active access authorization granted by another personnel security office simultaneously with the termination of that access authorization by the latter.

(1) In transfer cases, the PSF must be sent to the processing personnel security office to which the access authorization has been transferred as described in paragraph 4 below. The PSF must be reviewed and documented upon receipt.

(2) When supplemental investigation is deemed appropriate, a request for such an investigation must be submitted to the appropriate investigative agency by the processing personnel security office to which the access authorization has been transferred.

c. Requesting extensions and transfers. A request for extension or transfer of an access authorization must contain the full name of the individual, date of birth, social security number, and DOE file number to establish positive identification.

d. Identifiers. The Departmental Element having custody of the individual's PSF must inform the personnel security office accepting the extension or transfer of the following:

(1) the individual's date of birth;

(2) the individual's access authorization status;

(3) the type of investigation upon which the access authorization was based;

(4) if reinvestigated, the date and action taken; and

(5) whether the PSF contains unresolved derogatory information.

e. Accepting extensions and transfers. After positive identification has been established, and based on the information received, the individual's access authorization must be extended or accepted for transfer within 2 working days of receipt of all necessary information, unless the PSF contains unresolved derogatory information. The processing personnel security office having knowledge of unresolved derogatory information must notify all other offices having an access authorization interest in the individual of the details of the derogatory information.

f. Positions of a high degree of importance or sensitivity. If an access authorization is extended or transferred to a position certified as being "of a high degree of importance or sensitivity" and the previous investigation was not conducted by the FBI, the request for the new investigation, accompanied by a new SF 86, must be forwarded to the FBI.

g. CPCI. The personnel security office extending the access authorization and the personnel security office accepting the transfer of an access authorization must update the CPCI accordingly.

h. Interim access authorizations. IAAs may be extended or transferred among processing personnel security offices.

2. TERMINATIONS. Within 2 working days of receipt of notification that an individual no longer requires access to classified information or matter, or SNM, DOE must terminate the individual's access authorization.

a. Causes.

(1) An access authorization must be terminated when there is termination of employment or change of official duties so that the position no longer requires access to classified information or matter, or SNM. Continuation may be authorized by the processing personnel security office when the employer has certified that the individual will be reemployed or reassigned to a position that requires an access authorization within 3 months and that DOE will be kept informed of the individual's status. If an individual is cleared for more than one contract, each access authorization requires a separate termination action.

(2) The access authorization must be terminated if the holder is on leave of absence or extended leave and will not require access for at least 90 working days. (This includes leave for foreign travel, employment, or education, not involving official U.S. Government business.) This 90-day period may be adjusted at the discretion of the DOE cognizant security authority or the Director, Office of Security.

b. Procedures.

(1) When an individual no longer requires an access authorization, or when an access authorization is administratively terminated, the processing personnel security office must be notified electronically or verbally within 2 working days to be followed by a completed DOE F 5631.29, *Security Termination Statement*. Every practical effort should be made to obtain an executed DOE F 5631.29 from individuals, since the form explains their continuing security responsibilities after they no longer hold access authorizations. In cases in which it is not possible to obtain the individual's signature, the completed but unsigned DOE F 5631.29 must still be submitted, along with a written explanation of the circumstances surrounding the termination and why the signature could not be obtained.

(2) Within 2 working days of receipt of a DOE F 5631.29 or written notice of termination, the processing personnel security office must note in the individual's PSF the date the access authorization was actually terminated and must enter the appropriate information in the CPCI. A signed DOE F 5631.29 is not needed to effect a termination action.

(3) When an access authorization is to be terminated as required in paragraph 2.a.(2) above, due to foreign travel not involving official U.S. Government business, the individual must be advised that the access authorization is being terminated, the reason, and that it may be reinstated when the individual resumes work requiring it. The reinstatement procedure may require new security forms and/or an updated investigation as noted in paragraph 3. below.

c. Transfer of Terminated Personnel Security Files. When the PSF of an individual whose access authorization has been terminated at one processing personnel security office is transferred to another office, the transferring office must enter the new file location on the CPCI.

3. REINSTATEMENTS.

a. A new or updated and recertified SF 86 must be obtained if more than 6 months have elapsed since termination of the access authorization and more than 1 year has elapsed since the date of the previous form, or when any significant changes are known to have occurred since that date. When an SF 86 is not required, a request for reinstatement must contain the date of birth of the individual to establish positive identification. A new DOE F 5631.18 must be obtained in all cases.

b. The individual's PSF must be reviewed against the new or updated SF 86 and identifiers such as full name, social security number, and date of birth compared to ensure that the individual being reinstated is the same person whose file is being reviewed.

c. Supplemental investigation must be requested before, or concurrent with, reinstatement when any of the following conditions exist:

(1) the most recent investigation is more than 5 years old;

(2) the previous access authorization has been terminated for more than 24 months (unless the individual has been continuously employed by the same employer where access authorization was held, in which case the access authorization can be reinstated for up to 5 years from termination);

(3) new derogatory information has been found and has not been resolved following the initial granting of the access authorization; or

(4) the reason for the termination concerned eligibility for an access authorization.

d. If conditions described in paragraphs .c.(3) or (4) above exist and there is sufficient available information to proceed directly to administrative review processing, it is not necessary to schedule supplemental investigations.

e. Supplemental investigation must be completed and adjudicated before reinstatement in any instance when more than 10 years have elapsed since the previous investigation.

f. In requesting supplemental investigation, a completed SF 86 must be forwarded to the appropriate investigative agency. If a fingerprint card has been previously classified by the FBI, it is not necessary to submit a new fingerprint card.

g. Where the reinstatement involves assignment of an individual to a "position of a high degree of importance or sensitivity," and the previous investigation was not conducted by the FBI, a new SF 86 must be forwarded to the FBI for investigation. The DOE cognizant security authority or the Director, Office of Security, for Headquarters, may authorize the reinstatement of an access authorization before receipt of the new investigative report from the FBI, provided the circumstances listed in subparagraph d. above do not apply.

4. TRANSMITTAL OF PERSONNEL SECURITY FILES. Unclassified PSFs must be sent by first class mail or by other means approved for the transmittal of classified information. Classified PSFs must be sent by authorized means (See DOE M 470.4-4, *Information Security*). This applies to active or inactive PSFs and the mailing of investigative reports to the investigative agencies or processing personnel security offices. A memorandum or other transmittal form must be used to ensure that a record of the location of PSFs and reports is maintained. PSFs must be transmitted in double envelopes, the inner envelope marked "Security Mail—To Be Opened By Addressee Only," in addition to any classification markings required. Files containing classified information must be mailed only to the approved classified mailing address. Additional information concerning the transmission of classified information including other approved methods is contained in the Classified Matter Protection and Control chapter of DOE M 470.4-4, *Information Security*.

# CHAPTER VIII
# REINVESTIGATIONS

1. GENERAL. Except as authorized by the Director, Office of Security, individuals with access authorizations must be periodically reinvestigated. Reinvestigations are designed to ensure that individuals with access authorizations are periodically reevaluated to determine their continued need for such access authorizations and reinvestigated to determine their continued eligibility. A reevaluation and reinvestigation must be completed every 5 years for individuals holding Q access authorizations and every 10 years for individuals holding L access authorizations. This Chapter applies to all individuals with active access authorizations.

2. REEVALUATION. In conjunction with reinvestigation, the individual's sponsor must review the individual's need to hold an access authorization of the existing type. The sponsor must certify to DOE that the individual requires continuation of the access authorization and indicate the category and level of classified information or category(ies) of SNM to which the individual requires access to perform the official duties of the position. If access authorization has been approved under section 145b of the Atomic Energy Act, the Director, Office of Security, or designee, must ensure annually that the individual continues to require access to classified information or matter to perform the official duties of the position. Completion of security forms and the scheduling of a reinvestigation will normally not be required for such individuals unless the need to do so is approved by the Director, Office of Security.

3. INDIVIDUAL COMPLIANCE. If an individual's need to hold an access authorization is recertified, the individual must be provided the required security forms by the cognizant DOE or contractor security authority. The individual must be notified in writing that failure to provide updated security forms to the DOE cognizant security authority within 30 calendar days of the formal notification of the requirement for reinvestigation may result in administrative termination of the access authorization. Individuals who fail to submit completed security forms within the 30-day period will be contacted by the processing personnel security office to verify that they did receive the security forms and are aware of the administrative action that will be taken if they fail to return the forms. The personnel security representative making this contact must document the PSF with the date and time of contact. The individual's sponsor must be notified in writing when an individual's access authorization is administratively terminated. The decision to effect an administrative termination under these circumstances must be made by the head of the processing personnel security office. Individuals whose access authorizations are administratively terminated for failure to complete reinvestigation security forms must receive a termination briefing and execute a DOE F 5631.29, Security Termination Statement. Termination procedures in chapter VII, 2.b. should be followed.

4. REINVESTIGATION.

   a. Review of Continued Eligibility. A review of the individual's eligibility for continuation of the access authorization must be based upon evaluation of:

(1) the individual's updated security forms;

(2) the individual's PSF;

(3) the completed investigation as described below; and,

(4) any additional data resulting from required further investigative or administrative effort (e.g., personnel security interview, psychiatric evaluation, letter of interrogatory, and/or specialized indices checks).

b. Types of Reinvestigation. The type of reinvestigation to be conducted is determined by the type of access authorization held by the individual and the certification by the individual's sponsor of the individual's continued need for access. If an individual's SF 86 or PSF reflects new and/or unresolved derogatory information, the type of reinvestigation may be upgraded to resolve issues. Fingerprint cards are required only if there has not been a previously valid technical check by the FBI. Other reinvestigation requirements are listed below.

(1) Q Access Authorization. At each 5-year interval following completion of the previous investigation or reinvestigation, an SSBI-PR must be conducted. The investigation may be expanded or upgraded to resolve issues.

(2) L Access Authorization. At each 10-year interval following completion of the previous investigation or reinvestigation, an NACLC must be conducted. The investigation may be expanded or upgraded to resolve issues.

c. Scheduling Reinvestigations. The processing personnel security office must establish a schedule for submitting requests for reinvestigations for cases within their cognizance. The PSF location, as shown in the CPCI, indicates the processing personnel security office responsible for the reinvestigation. Reinvestigations should be submitted to the investigative agency at even intervals throughout the year. A reinvestigation may be scheduled whenever there is evidence that the individual has engaged in an activity or has been subject to circumstances that cause a security concern within the meaning of 10 CFR 710 or as a follow-up to previously adjudicated derogatory issues.

d. Security Forms. Processing personnel security offices are authorized to request updated security forms to process a periodic reinvestigation or at any time there is probable cause to believe that the individual may have engaged in an activity, or been subject to circumstances, that affect continued eligibility for access authorization.

e. Evaluation Procedures. The results of the reinvestigation must be reviewed and adjudicated following the procedures in chapter III for initial investigations. When a reinvestigation report contains derogatory information and the individual

has an active access authorization, the case must receive priority processing to resolve the derogatory information as quickly as possible or to determine whether the individual's case warrants processing under administrative review procedures. The results of the evaluation must be entered into the CPCI. If an access authorization has been extended, the processing personnel security office must immediately notify any other DOE personnel security office or Federal agency where the individual holds an access authorization or security clearance of any unresolved derogatory information.

**APPENDIX**
**POSITIONS OF A HIGH DEGREE OF IMPORTANCE OR SENSITIVITY**

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

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

A. DOE HEADQUARTERS

Secretary of Energy

Deputy Secretary of Energy

Under Secretary of Energy for Energy, Science and Environment

Under Secretary for Nuclear Security/Administrator for the National Nuclear Security Administration (NNSA)

Principal Deputy Administrator for National Nuclear Security, NNSA

Chief, Office of Defense Nuclear Counterintelligence, NNSA

Associate Administrator for Defense Nuclear Security

Deputy Administrator, Defense Programs, NNSA

Deputy Administrator, Defense Nuclear Nonproliferation, NNSA

Deputy Administrator, Naval Reactors, NNSA

Director, Office of Emergency Operations, NNSA

Assistant Secretary for Congressional and Intergovernmental Affairs

Director, Office of Counterintelligence

Assistant Secretary for Environment, Safety and Health

Assistant Secretary for Environmental Management

General Counsel

Director, Office of Hearings and Appeals

Inspector General

Director, Office of Intelligence

Director, Office of Nuclear Energy, Science and Technology

Director, Office of Independent Oversight and Performance Assurance

Assistant Secretary for Policy and International Affairs

Director, Office of Science

Director, Office of Security and Safety Performance Assurance

Director, Office of Security

Director, Office of Security Technology and Assistance Support

Director, Office of Safeguards and Security Policy and Classification Management

Director, Office of Headquarters Security Operations

B. DOE FIELD ELEMENTS

Manager, Chicago Operations Office

Manager, Idaho Operations Office

Manager, Oak Ridge Operations Office

Manager, Ohio Field Office

Manager, Pittsburgh Naval Reactors Office

Manager, Richland Operations Office

Manager, Savannah River Operations Office

Manager, Schenectady Naval Reactors Office

Director, NNSA Service Center, Albuquerque

Manager, Kansas City Site Office, NNSA

Assistant Manager for Safety and Security, Kansas City Site Office, NNSA

Manager, Livermore Site Office, NNSA

Assistant Manager for Safeguards and Security, Livermore Site Office, NNSA

Manager, Los Alamos Site Office, NNSA

Assistant Manager for Security Management, Los Alamos Site Office, NNSA

Manager, Nevada Site Office, NNSA

Assistant Manager for Safeguards and Security, Nevada Site Office, NNSA

Manager, Pantex Site Office, NNSA

Assistant Manager for Safeguards, Security, and Emergency Management, Pantex Site Office, NNSA

Manager, Sandia Site Office, NNSA

Assistant Manager for Safeguards and Security, Sandia Site Office, NNSA

Manager, Savannah River Site Office, NNSA

Manager, Y-12 Site Office, NNSA

Assistant Manager for Safeguards and Security, Y-12 Site Office, NNSA

**DEPARTMENTAL ELEMENTS TO WHICH**
**DOE M 470.4-5, *Personnel Security*, IS APPLICABLE**

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

# CONTRACTOR REQUIREMENTS DOCUMENT (CRD)

This Contractor Requirements Document (CRD) (which is equivalent to the National Industrial Security Program Operating Manual, Chapter 2, Section 2, "Personnel Clearances") prescribes requirements and procedures necessary for DOE and National Nuclear Security Administration (NNSA) contractors to:

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

Regardless of the performer of the work, the contractor is responsible for compliance with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontracts at any tier to the extent necessary to ensure the contractor's compliance with the requirements. In doing so, the contractor shall not unnecessarily or imprudently flow down requirements to subcontracts. That is, the contractor shall (1) ensure that it and its subcontractors comply with the requirements of this CRD to the extent necessary to ensure the contractor's compliance and (2) only incur costs that would be incurred by a prudent person in the conduct of competitive business.

A violation of the provisions of this CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to Subsection a. of Section 234B. of the Atomic Energy Act of 1954 (42 U.S.C. 2282b.). The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations, Part 824, "Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations" (10 CFR part 824).

The Atomic Energy Act provides the statutory basis for DOE's Personnel Security Program, which encompasses sets of activities for determining an individual's eligibility for access to Restricted Data and SNM. Both the DOE and the Nuclear Regulatory Commission (NRC) grant Q and L access authorizations. The term "access authorization(s)" in this document refers only to DOE access authorizations.

While Executive Orders (EOs) do not apply to contractors directly, the contractor must meet the requirements stated in the EOs to enable DOE to meet its requirements under the EOs. EOs 10865, 12829, 12958, as amended, and 12968 state requirements for DOE to determine an individual's eligibility for access to classified information or matter and to protect classified information or matter.

1. GENERAL REQUIREMENTS FOR ACCESS AUTHORIZATIONS.

   a. Requests for access authorizations must not be submitted until the contractor has been awarded a DOE contract and has submitted to DOE the required

paperwork for a Foreign Ownership, Control, or Influence (FOCI) determination.

b. Access authorization requests may be submitted to DOE pending completion of the FOCI determination; however, a favorable FOCI determination must be rendered by DOE before an access authorization will be granted, reinstated, continued, extended, or transferred for the contractor's applicant for employment (hereafter referred to as "applicant") or employee.

c. An access authorization request must be submitted to DOE only after the contractor's determination that the access authorization is essential for the individual to perform tasks or services stipulated in contract provisions (i.e., for an applicant or employee selected to occupy a position that requires the incumbent to access classified information or matter, or SNM, to perform work under the contract).

d. An access authorization must not be requested or continued to:

(1) allow the dissemination of classified information or matter on other than a need-to-know basis;

(2) avoid 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) alleviate responsibilities for properly protecting or disseminating classified information

(6) establish a pool of cleared employees;

(7) accommodate an individual's personal convenience, expedience, gain, advantage; or

(8) anticipate unspecified classified work.

e. An access authorization must be requested (or recertified as continuing to be needed) only when required, and only for the type (Q or L, see paragraph 2. below) required, to avoid the unnecessary expenditure of DOE resources and the unwarranted invasion of an individual's privacy.

f. Individual access to classified information or matter, or SNM, must not be permitted until notification has been received from DOE that an access authorization has been granted, reinstated, extended, or transferred. Verbal

notification from the processing personnel security office may be accepted, to be followed by written confirmation of the action.

g. Except as authorized by DOE in paragraph 6. below, access authorizations must be requested only for individuals who are U.S. citizens and over 18 years old.

h. Only authorized DOE employees can render a formal access authorization determination (such as eligibility and termination); however, contractors are authorized to effect actions that affect an individual's access, such as restricting access to classified information or matter, or SNM, when access eligibility terminates, or obtaining a DOE F. 5631.29, *Security Termination Statement* prior to the individual's departure.

i. Logistical assistance must be provided to DOE and investigative agencies, as reflected in paragraph 4. below, for conducting initial investigations and periodic reinvestigations, and for reinvestigations conducted when DOE determines that an employee may have been engaged in an activity or subjected to circumstances that affect continued access authorization eligibility.

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

k. An individual's active access authorization status must 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 must not be used by contractor management or other employees to coerce, restrain, threaten, intimidate, or retaliate against individuals for exercising their rights under the Constitution or under any statute, regulation, or DOE directive.

m. Unless otherwise stipulated, the contractor will not be required to reimburse DOE for DOE costs associated with processing the contractor's applicants or employees for investigations or other actions related to access authorizations.

n. Access authorizations must be requested and maintained at the minimum number necessary to ensure operational efficiency, and must be terminated as required in paragraph 7. below.

2. DETERMINATION OF ACCESS AUTHORIZATION TYPES. When the duties of a position will require the incumbent to access DOE classified information or matter, or SNM, the contractor must process the selectee for either a Q or L access authorization if the selectee does not already possess the appropriate type of 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 information or matter, or category of SNM (I, II, III, or IV) to which the incumbent will require access.

a. For Access to Classified Information or Matter.

(1) A Q access authorization must be requested when the duties of the position require access to any of the following:

(a) Top Secret or Secret Restricted Data;

(b) Top Secret Formerly Restricted Data;

(c) Top Secret National Security Information; or

(d) Classified information or matter designated as "COMSEC," "CRYPTO," "Sensitive Compartmented Information," or Weapon Data, Sigma 14 or Sigma 15.

**NOTE:** A Q access authorization also authorizes the individual access to the categories/levels of classified information or matter listed in paragraph 2.a.(2) below.

(2) An L access authorization must 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.

(1) Category I and other Categories with Credible Roll-Up to Category I. Q access authorization is required.

(2) Categories II and III. An L access authorization is required unless special circumstances determined by a site vulnerability assessment, and documented in the Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP), require a Q access authorization.

(3) Category IV. No access authorization is required, unless special circumstances determined by a site vulnerability assessment and documented in the SSSP or SSP require an access authorization to minimize risk.

c. For the Human Reliability Program (HRP). A Q access authorization is required for certification in a position designated under the HRP in accordance with 10 CFR 712.10.

3. PRE-EMPLOYMENT AND PRE-PROCESSING REQUIREMENTS.

a. The following statement must 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 information or matter." The statement may be modified, as appropriate, to reflect that access to SNM may require additional reviews and/or testing procedures.

b. The contractor must require applicants and employees selected for positions requiring access authorizations to provide evidence of U.S. citizenship and must verify such evidence to DOE when requesting that the individuals be processed for access authorizations. (See paragraph 4.a.(2) below.) Acceptable evidence of U.S. citizenship consists of the following:

(1) For an individual born in the U.S., a birth certificate is the primary and preferred means of citizenship verification. Acceptable birth certificates must show that the record was filed shortly after birth and must be certified with the registrar's signature. The birth certificate must bear the raised, impressed, or multi-colored seal of the registrar's office. The only exception is if a state or other jurisdiction does not issue such seals as a matter of policy. Uncertified copies of birth certificates are not acceptable. A delayed birth certificate (one created when a record was filed more than 1 year after the date of birth) is acceptable if it shows that the report of birth was supported by acceptable secondary evidence of birth. Secondary evidence may include baptismal or circumcision certificates, hospital birth records, or affidavits of persons having personal knowledge about the facts of the birth. Other documentary evidence can be early census, school, or family records; newspaper files; or insurance papers. All documents submitted as evidence must be original or certified.

(2) For an individual claiming citizenship by naturalization, a certificate of naturalization showing the individual's name is required.

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

(a) a Certificate of Citizenship issued by the Immigration and Naturalization Service;

(b) a Report of Birth Abroad of a Citizen of the U.S. of America (Form FS 240); or

(c) a Certificate of Birth (Form FS 545 or DS 1350).

(4) A U.S. passport, current or expired.

(5) *A Record of Military Processing-Armed Forces of the U.S.* (DD Form 1966), provided it reflects that the individual is a U.S. citizen.

c. When an access authorization will be required for an applicant or employee, the contractor must conduct the following checks, as appropriate, to establish the individual's job qualifications and suitability before submitting the access authorization request to DOE:

(1) a credit check;

(2) verification of a high school degree or diploma or a degree or diploma granted by an institution of higher learning within the past 5 years;

(3) contacts with listed references;

(4) contacts with listed employers for the past 3 years (excluding employment of less than 60 working days duration, part-time employment, and craft/union employment); and

(5) local law enforcement checks when such checks are not prohibited by state or local law, statute, or regulation, and when the individual has resided in the jurisdiction where the contractor is located.

d. An applicant hired specifically for a position that will require an access authorization must not be placed in that position until the access authorization has been granted by DOE unless an exception has been obtained from the head of the DOE contracting activity or designee.

e. The contractor is not required to conduct the checks or provide verifications to DOE stipulated in paragraphs 3.b and 3.c. for:

(1) individuals who hold an access authorization/security clearance granted by another Federal agency;

(2) Federal employees (including members of the Armed Forces) detailed or assigned to the contractor; or

(3) an employee who previously held an access authorization if the individual has been continuously employed by the contractor, provided that the access authorization was not terminated for cause.

f. The contractor must not concurrently submit an applicant or employee for a DOE 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 must first be submitted to DOE. After DOE has granted a Q access authorization, the contractor should then request the other agency reciprocal 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. The same procedure must 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 processing personnel security office.

4. PROCESSING ACCESS AUTHORIZATION REQUESTS TO DOE.

a. Access authorization requests must be forwarded through established channels to the DOE processing personnel security office. Requests must include the following documentation (additional documentation may be required by the DOE processing personnel security office):

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

General statements such as "An access authorization is required to perform contractual duties," or "An 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. 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 U.S. citizenship.

(3) Required security forms, usually a Standard Form 86, fingerprint cards, DOE credit release, and a DOE Security Acknowledgment. [NOTE: Security forms and instructions must 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 information or matter designated as "Sensitive Compartmented Information," "CRYPTO," or "Weapon Data," the individual may be required to file financial disclosure reports. Copies of the form will be provided by the cognizant DOE office.]

(4) Verification that pre-processing checks have been conducted as indicated in paragraph 3.c. above.

(5) The DOE contract or subcontract number under which access authorization is being requested.

b. The contractor must advise employees and applicants for employment that their completed security forms will be reviewed by designated contractor employees for completeness before they are submitted to DOE. The contractor may elect to maintain copies of the individual's security forms in paper or electronic format. If the contractor elects to maintain copies of the individual's security forms, the individual must be informed of the contractor's policy concerning copies of the security forms, the contractor's procedures for protecting the information from unauthorized disclosure, and the procedures by which the individual may obtain access to, or copies of, the security forms maintained by the contractor. The contractor should recommend to the individual that they maintain copies of the completed security forms for personal records.

c. Written procedures must be established for the protection of access authorization request information, including the procedures for:

(1) designating the employees responsible and trained in the procedures for reviewing the individual's completed security forms before their submission to DOE; and

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

d. Deficient access authorization requests will be returned to the contractor by the DOE processing personnel security office with an indication of the deficiency(ies). The contractor must ensure that the request is corrected and returned to the DOE processing personnel security office.

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

g. The contractor must ensure that the individual being processed for an access authorization is not provided access to classified information or matter, or SNM, until the DOE processing personnel security office notifies the contractor that an access authorization has been granted, reinstated, extended or transferred. Verbal notification of the access authorization action from the DOE processing personnel security office will be confirmed by a written notification from DOE.

5. INTERIM ACCESS AUTHORIZATION (IAA) REQUEST.

a. The contractor may request that an individual being processed for an access authorization also be processed for an IAA based on the following circumstances:

(1) serious delay or disruption of a DOE program may be experienced unless the named individual is granted an access authorization before the completion of full access authorization procedures; and

(2) the services of a qualified person with an active access authorization cannot be obtained.

**NOTE:** Specific information substantiating the justification must be provided.

b. The contractor must not request an IAA for dual citizens or foreign nationals.

c. The IAA request must accompany the required documentation in paragraph 4.a. above.

d. Individuals processed for an IAA at the Q level may be asked to voluntarily participate in the DOE Accelerated Access Authorization Program (AAAP), which involves psychological, drug, and counterintelligence polygraph testing at the DOE Test Centers, Albuquerque, New Mexico, or Oak Ridge, Tennessee. Transportation and per diem costs for such processing are the contractor's responsibility. Additional information concerning the AAAP is available from the DOE processing personnel security office.

e. The contractor may provide the individual access to classified information or matter, or SNM, upon receipt of written notification from the DOE processing personnel security office that the IAA has been approved. DOE must also notify the contractor if the IAA is not approved. Non-approval of an IAA is not a denial

of an access authorization and is not appealable. DOE full access authorization procedures will continue in either case.

f. If DOE withdraws an individual's IAA approval, the contractor must, upon receipt of verbal notification from the DOE processing personnel security office, ensure that the individual is precluded from access to classified information or matter, or SNM. DOE must confirm the verbal notification in writing. Withdrawal of an individual's IAA approval by DOE is not a denial or revocation of an access authorization and is not appealable. Withdrawal of an individual's IAA approval does not halt the processing of the access authorization request.

g. If DOE grants a final access authorization, the individual's IAA approval will be withdrawn and the contractor will be notified in writing.

6. ACCESS AUTHORIZATION REQUESTS FOR FOREIGN NATIONALS AND DUAL CITIZENS.

a. Foreign Nationals.

(1) The contractor must process a request for an access authorization for a foreign national in accordance with the guidance provided by the DOE processing personnel security office.

(2) The request must be made only when the contractor can provide clear evidence that the individual has skills essential to the DOE's mission that are not possessed to a comparable degree by an available U.S. citizen.

(3) The request will not be processed by DOE if sufficient information cannot be obtained by an investigation to determine the individual's access authorization eligibility.

(4) The contractor must not provide access to the following types of classified information or matter to a foreign national granted an access authorization:

(a) Top Secret, CRYPTO, or COMSEC information except classified keys used to operate secure telephone units (e.g., STU IIIs).

(b) Intelligence or Special Access Program (SAP) information.

(c) Information that has not been determined releasable by a U.S. Government Designated Disclosure Authority to the country of which the individual is a citizen.

(d) NATO Information; however, a foreign national of a NATO member nation may be authorized access to NATO Information provided that:

1 a NATO Security Clearance Certificate is obtained by DOE from the individual's home country; and

2 NATO Information access is limited to performance on a specific NATO contract.

(e) Information for which foreign disclosure has been prohibited in whole or in part (NOFORN).

(f) Information provided to the U.S. Government in confidence by a third party government (FGI) and classified information furnished by a third-party government.

b. Dual Citizens. Individuals who possess a dual citizenship (i.e., who are simultaneously a citizen of the U.S. and another country) and who have exercised citizenship rights in the foreign country, or have represented themselves as citizens of the foreign country, or who have intentions to do so in the future, must meet the requirements for foreign nationals in paragraphs 1. and 2. above. There are two alternatives to being processed as foreign nationals, as described below:

(1) Renunciation of the Citizenship in the Other Country. If the individual is willing to renounce citizenship in the other country, the individual must provide a notarized statement attesting to the fact that the non-U.S. citizenship has been formally renounced, and if available, evidence that the renunciation has been formally accepted by an official representative of the other country's government. Copies of documents completed by the individual to formally renounce non-U.S. citizenship must accompany the notarized statement. An individual's statement of renunciation must be considered invalid if the individual continues to exercise citizenship rights in a foreign country.

(2) Waiver. The DOE cognizant security authority, or the Director, Office of Security, for Headquarters cases, may waive the requirement to renounce the non-U.S. citizenship if it is determined that it would be detrimental to the individual or to DOE security objectives, or that the risk associated with the individual maintaining the non-U.S. citizenship status has been adequately mitigated. A copy of the security evaluation documenting this waiver must be maintained in the individual's PSF.

7. REPORTING AND OTHER REQUIREMENTS.

a. Contractor Reporting Requirements. Except for item (3) below, contractors must notify, within 2 working days followed by written confirmation within the next 10 working days, the DOE processing personnel security office of the following conditions affecting the status of an applicant's or employee's access authorization:

(1) when an applicant declines the offer of employment or fails to report for duty;

(2) for any reason in paragraph 7.c. below;

(3) when an individual under their cognizance who holds an access authorization is hospitalized for mental illness or has received other treatment for a condition that in the supervisor's opinion may cause a significant defect in the individual's judgment or reliability, verbal notification must be made within 8 working hours and written confirmation within the next 10 working days;

(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 U.S. citizen through naturalization or effects any other change in their citizenship status; or

(6) when the contractor restricts or withdraws an employee's access to classified information or matter, or SNM, without DOE direction.

b. Individual Reporting Requirements. The contractor must inform employees and applicants who are applying for or granted access authorization that they must:

(1) Provide full, frank, and truthful answers to questions and, when requested, furnish or authorize others to furnish information that DOE deems pertinent to the access authorization eligibility process. This applies when completing security forms, during the course of an initial investigation and reinvestigations, and at any stage of access authorization processing including, but not limited to, letters of interrogatory, personnel security interviews, DOE-sponsored mental evaluations, and other authorized DOE investigative activities. An individual may elect not to cooperate; however, such refusal may prevent DOE from granting or continuing access authorization. In this event, any access authorization then in effect may be terminated or further processing may be suspended.

(2) Provide direct notification to the DOE processing personnel security office of the following (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 U.S., unless the traffic violations were drug or alcohol related;

(b) personal or business-related filing for bankruptcy;

(c) garnishment of wages;

(d) legal action effected for name change;

(e) change in citizenship;

(f) employment by, representation of, or other business-related association with a foreign or foreign-owned interest, or foreign national; and

(g) hospitalization for a mental illness; treatment of drug abuse; or treatment for alcohol abuse.

(3) Provide notification to the DOE processing personnel security office or the FSO, as appropriate, immediately after any approach or contact by any individual seeking unauthorized access to classified information or matter, or SNM. If such an approach or contact is made while on foreign travel, individuals should notify a Department of State official at the local U.S. Embassy or Consulate with a request that the Department of State report the incident to the Director, Office of Security, at DOE Headquarters. This requirement is in addition to any similar reporting requirements implemented under DOE directives or regulations.

(4) Provide a completed DOE F 5631.34, *Data Report on Spouse/Cohabitant*, directly to the DOE processing personnel security office within 45 working days of marriage or cohabitation. These forms must be obtained from the cognizant personnel security office.

c. Access Authorization Termination Requests. The contractor must request that the DOE processing personnel security office(s) terminate an employee's access authorization and must provide a DOE F 5631.29, *Security Termination Statement*, completed by the employee whenever any of the following occur:

(1) employment by the contractor is terminated;

(2) an access authorization is no longer required;

(3) the individual is on a leave of absence or on extended leave and will not require access to classified information or matter, or SNM, for 90 consecutive working days. Upon request, this interval may be adjusted at the discretion of the DOE processing personnel security office;

(4) access to classified information or matter, or SNM, is no longer required due to transfer to a position not requiring such access; or

(5) the individual leaves for foreign travel, employment, assignment, education, or residence of more than 3 months duration, not involving official U.S. Government business. This requirement applies even if the individual remains employed by the contractor.

[NOTE: The purpose of the DOE F 5631.29 is to ensure that the individual is aware of the continuing responsibility to protect classified information or matter after termination of an access authorization. The DOE processing personnel security office must be requested to terminate an employee's access authorization even though a completed DOE F 5631.29 cannot be immediately provided. In cases in which it is not possible to obtain the individual's signature, the completed but unsigned DOE F 5631.29 must still be submitted. In addition, the contractor will provide an explanation to the DOE processing personnel security office of the circumstances surrounding the termination and why the signature could not be obtained.]

d. Access Authorization Pending Reemployment/Reassignment. The DOE processing personnel security office may approve a contractor request for an individual to retain an access authorization when the contractor verifies that the individual will be reemployed or reassigned by the contractor within the next 3 months in a position that will require an access authorization. The contractor must inform the DOE processing personnel security office of the individual's employment status at the end of the 3-month interval.

e. Access Authorization Reinstatement Requests. The contractor must request that the DOE processing personnel security office reinstate the access authorization for an applicant or employee when the contractor is aware that the individual previously was granted an access authorization. The DOE processing personnel security office will advise the contractor whether the individual must complete a new set of security forms or update information previously provided.

f. Access Authorization Upgrade Requests. The contractor must request that the DOE processing personnel security office upgrade an employee's access authorization from L to Q in accordance with the new access requirements associated with the duties of the position (reference paragraph 2. above). The request must be accompanied by appropriate security forms and a revised access authorization justification statement, as directed by the DOE processing personnel security office.

g. Access Authorization Downgrade Requests. The contractor must request that the DOE processing personnel security office downgrade an employee's access authorization from Q to L in accordance with the new access requirements associated with the duties of the position (reference paragraph 2. above). The request must be accompanied by a revised access authorization justification statement.

h. Access Authorization Extension Requests. Extension of an access authorization is the process that allows an individual to hold concurrent access authorizations under the cognizance of two or more DOE personnel security offices, under two or more employers, or for one employer under two or more contracts. A Q access authorization can be extended as either a Q or L access authorization; however, an L access authorization can only be extended as an L access authorization. The contractor must request an access authorization extension under the following circumstances:

(1) for an applicant who has an access authorization granted by DOE at the request of another employer and who must retain that access authorization in connection with that other employment; or

(2) for an employee when the individual will be assigned to perform classified work under more than one DOE contract and must retain the original access authorization in connection with their continued work under the first DOE contract.

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

i. 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., from Q to Q, or from L to L). The contractor must request an access authorization transfer under the following circumstances:

(1) for an applicant when the individual has an access authorization granted by DOE at the request of the current employer that will be terminated when the individual leaves that employment [NOTE: this action involves a change of employers for the individual]; or

(2) for an employee when they will be assigned to perform classified work under a different contract than the one for which an access authorization was originally granted, and will no longer require access to classified information or matter, or SNM, associated with the original contract [NOTE: this action involves a change of contracts for the individual under one employer].

The contractor's request for an access authorization transfer must be accompanied by a written access authorization justification statement and must reference the individual's full name, social security number, and, if known, DOE personnel security file number and type/date of the access authorization. The DOE processing personnel security office must advise the contractor if additional security forms are required to affect the transfer. The contractor must ensure the individual is precluded from access to classified information or matter, or SNM, until notified by the DOE processing personnel security office that the transfer request has been approved. When applicable, the DOE personnel security office processing the transfer request is responsible for notifying the DOE personnel security office that originally granted the access authorization to terminate the individual's access authorization associated with the previous employment.

j. Access Authorization Suspension, Revocation, and Denial.

(1) Upon receipt of notification by the DOE processing personnel security office of an employee's access authorization suspension, or denial of final access authorization after previous approval of an IAA, the contractor must ensure that the employee is precluded from access to classified information or matter, or categories of SNM, requiring an access authorization. When the security issue(s) concerning the employee's access authorization status has been resolved, the contractor will be notified in writing by the DOE processing personnel security office of whether the employee's access authorization has been reinstated, revoked, or denied.

(2) 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.

k. Records Maintenance.

(1) The contractor must maintain current records which reflect by contract numbers all employees granted access authorizations. The listing must include the employee's name, DOE file number, and the date the contractor was notified by DOE that the employee's access authorization was granted, reinstated, extended, or transferred.

(2) Copies of correspondence to and from the DOE processing personnel security office(s) that reflect access authorization matters for each

applicant and employee must be maintained, including: the request for an access authorization, notification that access authorization action was effected, and access authorization termination action. Such copies must be maintained while the individual holds an access authorization at the contractor's request and for a period of 2 years after the date the individual's access authorization is terminated, at which time they may be destroyed.

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

l. Recertifications and Reinvestigations.

(1) The contractor must comply with periodic DOE requests to re-certify its employees' access authorization status. Usually, the DOE processing personnel security office will furnish the contractor a listing of its applicants and employees who hold, or are being processed for, access authorizations and request that the contractor annotate the listing with any corrections or adjustments and return the listing in a timely manner. Recertification or an examination of access authorization records also may be requested during the conduct of a DOE security survey. Specific recertification guidance will be provided by the DOE processing personnel security office.

(2) The contractor must assist DOE in the conduct of periodic reinvestigations in accordance with guidance provided by the DOE processing personnel security office (reference paragraph 4.e. above).

8. DEFINITIONS. Terms commonly used in the program are defined in the S&S Glossary located in DOE M 470.4-7, *Safeguards and Security Program References*. In addition to those in the Glossary, the following definitions are provided for use in this Manual.

a. Field Element Manager means the Manager of the Chicago, Idaho, Oak Ridge, Richland, and Savannah River Operations Offices; Manager of the Pittsburgh Naval Reactors Office and the Schenectady Naval Reactors Office; Director of the Service Center, Albuquerque; and for the Washington, D.C. area, the Director, Office of Security.

b. DOE line management refers to DOE and NNSA Federal employees who have been granted the authority to commit resources or direct the allocation of

personnel or approve implementation plans and procedures in the accomplishment of specific work activities.

c. Line management refers to DOE and NNSA Federal and contractor employees who have been granted the authority to commit resources or direct the allocation of personnel or approve implementation plans and procedures in the accomplishment of specific work activities.

d. DOE cognizant security authority refers to DOE and NNSA Federal employees who have been granted the authority to commit security resources or direct the allocation of security personnel or approve security implementation plans and procedures in the accomplishment of specific work activities.

e. Cognizant security authority refers to DOE and NNSA Federal and contractor employees who have been granted the authority to commit security resources or direct the allocation of security personnel or approve security implementation plans and procedures in the accomplishment of specific work activities.

f. For the purposes of this Manual, the Office of Security refers to the DOE Office of Security.

g. For the purposes of this Manual, the term “access authorization(s)” refers only to DOE access authorizations.