DOE M 472.1-1B

Approved: 7-12-01
Sunset Review: 7-12-03
Expires: 7-12-05

PERSONNEL SECURITY PROGRAM MANUAL

U.S. DEPARTMENT OF ENERGY
Office of Security and Emergency Operations
Office of Security Affairs
Office of Safeguards and Security

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Security and Emergency Operations

PERSONNEL SECURITY PROGRAM MANUAL

1. PURPOSE. This Manual provides detailed requirements and procedures to supplement DOE O 472.1B, *Personnel Security Activities*, which establishes the overall objectives, requirements, and responsibilities for implementation and operation of the Personnel Security Program and the Personnel Security Assurance Program in the Department of Energy (DOE), including the National Nuclear Security Administration (NNSA). This Manual addresses only the Personnel Security Program. It is intended for use by DOE employees responsible for personnel security activities.

2. CANCELLATION. DOE M 472.1-1A, dated 11-16-00, is cancelled.

3. APPLICABILITY.

   a. DOE Elements. This Manual applies to all DOE elements, including NNSA.

   b. Contractors. The Contractor Requirements Document (DOE O 472.1B, Attachment 1) establishes Personnel Security Program requirements for DOE contractors, including NNSA contractors, and stipulates that specific requirements or guidance may also be issued by the cognizant DOE office; that is, the local operations, field, or Naval Reactors Office, or for Headquarters, the Headquarters Operations Division, Office of Safeguards and Security. The Contractor Requirements Document is the DOE equivalent of those portions of the *National Industrial Security Program Operating Manual* (DoD 5220.22M) that address personnel clearances.

4. DEFINITIONS. Definitions of commonly used terms are provided in the Safeguards and Security Glossary of Terms, dated 12-18-95, which is maintained and distributed by the Office of Safeguards and Security.

5. DEVIATIONS. Requests for deviations from requirements in this Manual will be processed in accordance with DOE O 470.1, *Safeguards and Security Program*. Deviations from the requirements and procedures in Title 10, Code of Federal Regulations, Part 710 (10 CFR 710) will not be approved. Waivers of preappointment investigations will be processed in accordance with 5 CFR 732 and 736.

6. REFERENCES.

   a. DOE O 472.1B, *Personnel Security Activities*, dated 3-24-97.

   b. DOE O 470.1, *Safeguards and Security Program*, dated 9-28-95, with change 001, dated 6-21-96.

c. Executive Order 12968, Access to Classified Information, dated 8-2-95.

d. 10 CFR 710, Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material.

e. *National Industrial Security Program Operating Manual* (NISPOM), DoD 5220.22-M, dated 1-95.

7. CONTACT. Questions should be addressed to the DOE Personnel Security Program Manager, 301-903-6637, or the DOE senior personnel security official at the cognizant DOE office.

BY ORDER OF THE SECRETARY OF ENERGY:

FRANCIS S. BLAKE
Deputy Secretary

CONTENTS

CHAPTER III, INVESTIGATIVE RESULTS PROCESS AND ACCESS AUTHORIZATION DETERMINATIONS

CONTENTS (continued)

CONTENTS (continued)

CHAPTER I

ACCESS AUTHORIZATION REQUESTS

1. ACCESS AUTHORIZATION NEED DETERMINATION. 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 matter and/or special nuclear materials (SNM). Access authorizations must not be requested to alleviate individual or management responsibilities for properly protecting classified information or controlling dissemination of such classified information on a need-to-know basis. DOE has a single access authorization program for DOE contractor and subcontractor employees, consultants, and access permittees. The Contractor Requirements Document for DOE O 472.1B, *Personnel Security Activities*, sets forth Personnel Security Program requirements for DOE contractors. Statements concerning contractor requirements contained in this Manual are for the purpose of informing DOE elements only.

2. ACCESS AUTHORIZATION TYPE DETERMINATION. The type of access authorization requested is determined after a review of the type and level of classified matter and/or SNM for which the individual requires access to perform the official duties of his/her assigned position. For additional information regarding access to SNM, refer to DOE O 472.1B, Attachment 3. An authorization granted for access to SNM also allows access to the appropriate categories/levels of classified matter on a need-to-know basis. To meet the requirements of the *National Industrial Security Program Operating Manual* (NISPOM), a contractor Facility Security Officer and key management personnel must possess access authorizations equivalent with the level of the facility clearance (for information on facility clearances see DOE O 470.1, *Safeguards and Security Program*, Chapter V). 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 of Safeguards and Security, SO-21 (for Headquarters cases), or to the appropriate field element manager.

   a. Q and L — The types of access authorizations (Q and L) and the levels of classified matter and categories of SNM for which each type allows access are described in Attachments 2 and 3 of DOE O 472.1B.

   b. QX and LX — Access authorization types QX and LX 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 Title 10, Code of Federal Regulations (CFR) Part 725.

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

3. OTHER FEDERAL DEPARTMENT OR AGENCY EMPLOYEES AND LEGISLATIVE AND JUDICIAL BRANCH EMPLOYEES. Until the Department has determined that such access will not endanger the common defense and security, DOE will withhold access to classified matter or SNM under DOE responsibility from employees of other Federal departments or 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 Office of Personnel Management (OPM), the Federal Bureau of Investigation (FBI), or other Government 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.

4. APPROVAL FOR SPECIAL PROGRAMS. Within DOE, several categories of classified information require, in addition to an access authorization, programmatic approval before access to the information is authorized. These categories include the following:

- Sensitive Compartmented Information (SCI), which must be approved by the DOE Senior Intelligence Officer, or his or her designated representative within the Office of Intelligence;
- Weapon Data, which requires approval from the Office of Defense Programs;
- NATO information, which must be approved by the Office of Security Affairs; and
- CRYPTO and COMSEC, which must be approved by the Office of The Chief Information Officer.

For further information regarding these programs, the relevant office should be contacted.

5. 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 2, unless the individual will be processed under the reciprocity process described in this Manual, Chapter II, paragraph 3, or the reinstatement process described in Chapter VII, Section 3.

CHAPTER II

NATIONAL AGENCY CHECK AND BACKGROUND INVESTIGATION REQUESTS AND PROCESS

1. SCOPE. This chapter covers the procedures for initiating and processing requests for National Agency Checks required for L access authorizations and background investigations required for Q access authorizations.

2. FORMS. The following forms are required to process a request for an access authorization.
   a. Federal Employees.
      (1) Standard Form 86 (SF-86), Questionnaire for National Security Positions.
      (2) Standard Form 87 (SF-87), Fingerprint Card.
      (3) Either Standard Form 171 (SF-171), Application for Federal Employment; Optional Form 612 (OF-612), Optional Application for Federal Employment; or a resume. If the individual submits an OF-612 or a resume, an Optional Form 306 (OF-306), Declaration for Federal Employment, must also be submitted.
      (4) DOE F 5631.18, Security Acknowledgment.
      (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, FD-258 (Fingerprint Card), DOE F 472.1, and DOE F 5631.18 to obtain an access authorization.

3. RECIPROCITY. As a basis for granting an access authorization, DOE will accept verification that the applicant currently has a security clearance and/or SCI access approval granted by another Federal agency, provided the investigative basis for the previous security clearance/SCI access approval meets the scope of the investigation required for the DOE access authorization. In addition, if the access authorization to be granted is a Q, the investigation must have been completed or updated by reinvestigation within the past 5 years. If the access authorization to be granted is an L, the investigation must have been completed or updated by reinvestigation within the past 10 years. The scope for a Q access authorization is a Single Scope Background Investigation (SSBI). The scope for an L access authorization is, for cases initially processed prior to October 1997, a National Agency Check with Credit (NACC). For cases initially processed after October 1997, the scope is a National

Agency Check (NACLC) with Law and Credit for non-Federal employees and an Access National Agency Check and Inquiries (ANACI) for Federal employees.

Until March 1997, the Federal Government did not have a defined investigative scope for reinvestigations, so each Federal agency established its own scope for periodic reinvestigations. Therefore, if the previous security clearance/SCI access approval is based on a reinvestigation, the local Personnel Security Program manager must exercise judgment and latitude to determine if the reinvestigation used by the other Federal agency is acceptable.

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

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

(2) Obtain either a newly completed SF-86 or a copy of the most recently completed security questionnaire (SF-86, DD 398, or equivalent). A copy of a previously completed questionnaire may be submitted by the individual or the Federal agency that granted the security clearance and/or SCI approval. If the form does not come directly from the Federal agency where the individual holds a security clearance, the individual must update, re-sign, and redate 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. 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 DOE 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.

b. After a DOE access authorization is granted, a copy of the investigation(s) the original agency used as the basis for granting the security clearance and/or SCI access approval will be obtained. Upon receipt, if action is needed to resolve issues that were not resolved by the original agency, such action will be initiated. If the 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.

c. In instances where the most recent investigation or reinvestigation for an individual with a verified active security clearance at another Federal agency does not meet the time frames required in paragraph 3, an exception may be requested from the Director of Security Affairs. Exceptions should only be requested when a current SF-86 does not reveal any unresolved security concerns and the need for the reciprocal clearance supports an urgent Departmental requirement, certified by the Program Secretarial Officer, or designee, from the organization sponsoring the request. Should the individual's clearance at the other Federal agency be terminated subsequent to DOE granting a reciprocal access authorization, DOE will assume the responsibility for processing a reinvestigation for the individual.

4. 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 (see DOE O 472.1B, Attachment 1, paragraph 3b, for details).

c. Requests for employees of management and operating contractors and other contractors managing DOE-owned facilities must be accompanied by preemployment checks required by 48 CFR 970.2201(b)(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 O 470.1, Chapter VI, "FOCI Program"). However, a favorable FOCI determination must be rendered by DOE and the facility code must be registered on the Safeguards and Security Information Management System (SSIMS) before an access authorization can be granted, reinstated, continued, extended, or transferred for any of the contractor's employees or applicants for employment.

5. 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 conducted by the FBI. A listing of these positions is contained in Attachment 4 to DOE O 472.1B.

b. Q, QL, and QX. An SSBI conducted by OPM or the FBI. When a QL is requested, the NACC 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. These types of access authorizations may also be based upon a background

investigation by a Federal agency other than the FBI or OPM, provided the existing 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 required. The QB access authorization is granted by the Director of Security Affairs, pursuant to Section 145b of the Atomic Energy Act of 1954, as amended, when such action has been determined to be clearly consistent with the national interest. This authority cannot be redelegated. A QB access authorization precludes the need for a background investigation and 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.

6. PRESCREENING. Each personnel security case 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 after Question 14 of the SF-86 who is coded "19," as being, "an adult living with you."

e. The proper justification for the need for 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 preemployment checks required by 48 CFR 970.2201(b)(1)(ii), and all contractor requests are accompanied by a certification of the individual's U.S. citizenship. (See DOE O 472.1B, Attachment 1, Contractor Requirements Document.)

g. An individual previously granted a DOE 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. An individual concurrently being processed for access authorization or security clearance by another Federal agency is identified.

j. A foreign national or dual citizen requiring Secretarial Officer approval prior to processing for investigation is identified. (See Chapter VI.)

k. An individual for whom the SF-86 discloses derogatory information, necessitating a higher level of investigation than would normally be required, is identified.

l. An individual for whom citizenship issues are raised that will require additional action prior to submission for investigation is identified.

7. PERSONNEL SECURITY FILE (PSF) NUMBERS. The appropriate security office will consecutively assign PSF numbers as individuals are initially processed for any type of DOE 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 will be retained by the DOE security office submitting the request. No more than 120 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 that are more than 120 days old, or that would exceed 120 days by the time the form can be transmitted and received by the investigative agency, must be returned to the individual for updating and re-signing unless an appropriately executed FIPC 391, Certification of Amended Investigated Form, is completed. (FIPC stands for Federal Investigations Processing Center.)

b. The SF-87, Fingerprint Card, will be used to process investigations of Federal employees. In all other cases, the FD-258, Fingerprint Card, will 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 not already printed there.

(1) It is essential that personnel assigned to take fingerprints be adequately trained to recognize unclassifiable prints. If there is an obvious reason why a print will be

unclassifiable (for example, a scar or missing finger), this should be noted on the fingerprint card in the box labeled "scars, marks, or tattoos." Fingerprint cards that cannot be classified by the FBI cause undue delay in the access authorization determination process. Particular care should be taken whenever retakes are necessary.

(2) The unclassifiable or illegible fingerprint card submitted for a fingerprint retake should be attached to the newly obtained card with a cover letter indicating the type of investigation and access authorization requested for the individual. 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 should be submitted to the following address:

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

(4) Fingerprint retakes for individuals being investigated by the FBI should 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. Normally, only one set of fingerprint retakes will be submitted for classification.

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

9. OTHER FEDERAL AGENCY REQUESTS FOR DOE ACCESS AUTHORIZATIONS. All requests for DOE access authorization for Federal employees and contractors must be processed through the Director of Safeguards and Security. DoD and NASA personnel may have access to Restricted Data under the certification procedures outlined in Chapter VIII of DOE O 470.1, *Safeguards and Security Program*, except in cases indicated below.

a. DoD and NASA Personnel Assigned to the Department. These individuals require DOE access authorization 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 clearance from their agency, providing the processing for DOE access authorization has been initiated. Restricted Data received by such personnel during their assignment with DOE must be handled in accordance with DOE security requirements.

b. DoD and NASA Personnel Assigned to Other Federal Agencies. When these individuals 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 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 security clearance for assignment to the other agency, the other agency must request the appropriate investigation, adjudicate the reported information, and grant the appropriate clearance.

11. ADDITIONAL REQUIREMENTS FOR CASES INVOLVING FOREIGN RESIDENCE, EMPLOYMENT, OR OTHER ACTIVITIES IN A FOREIGN COUNTRY.

a. When an individual has lived, worked, attended school, or had any other activity outside the United States, it frequently takes additional time to complete an investigation. If the individual's activities outside the United States can be verified by individuals currently in the United States, the investigation can be completed more quickly than through investigation conducted outside the United States Individuals who have resided, worked, attended school, or had any other activity outside the United States during the period of time covered by their investigation should complete the Office of Personnel Management "Attachment for Individuals Who Have Resided or Worked Outside the United States." A copy of this attachment can be printed from the OPM Web site at the following address:

http://www.opm.gov/extra/investigate/fin0006.htm

This address will bring you to the OPM Federal Investigations Notice of this subject and by clicking on Optional Attachment at the end of the Notice, you can access the attachment. The completed attachment will be submitted to the investigative agency with the completed SF-86 to assist in developing adequate coverage to complete the investigation.

b. If, upon review of the SF-86, and the attachment described above, the DOE security office finds it unlikely that an adequate investigation is possible, all material pertaining to the case will be forwarded to the Office of Safeguards and Security for coordination with the appropriate investigative agencies. The Office of Safeguards and Security will then advise the requesting DOE security office on whether sufficient information can be obtained to determine the individual's eligibility for access authorization.

12. TRANSMITTAL OF COMPLETED INVESTIGATIVE REPORTS. OPM and the FBI forward reports of investigations directly to the requesting security office. Each DOE field element 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 the receipt of the reports.

13. CANCELLATION OF REQUESTS FOR ACCESS AUTHORIZATION OR INVESTIGATION. DOE must request the investigating agency to discontinue its investigation immediately upon receipt of notification 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 a field element because the individual is transferring to another field element and will still require access authorization, the terminating office should not cancel the investigation. Upon receipt of the investigation report, it should be sent to the appropriate DOE personnel security office for adjudication.

14. TYPES OF INVESTIGATIONS. The following investigations are those most frequently conducted for DOE.

a. Single Scope Background Investigation. 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. 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. 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 with 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. The ANACI is a name check of the individual at appropriate Federal and local law enforcement agencies, a classification of the individual's fingerprints with the FBI, a credit search, and written inquiries regarding the individual's employers, education, residences, and references. An ANACI is used for the initial investigation of Federal employees requiring L access authorization.

e. Upgrading an 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) should 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 prior to completion of the investigation. The outstanding portion of the investigation will be clearly identified by OPM. The local DOE 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 is to be made when the missing information is received from OPM.

16. INVESTIGATION REQUESTS FOR INDIVIDUALS TRANSFERRED TO POSITIONS OF A HIGH DEGREE OF IMPORTANCE OR SENSITIVITY.

a. The Atomic Energy Act of 1954, as amended, 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. (See Chapter I.) When a currently cleared individual is selected for such a position, the manager may authorize the transfer to the new position provided—

(1) the existing PSF is reviewed by a personnel security specialist before the transfer takes place and this review has not revealed any unresolved derogatory information, and

(2) the most recently conducted investigation is not more than 5 years old.

b. In such cases, the individual must be processed for an FBI reinvestigation when the existing investigation becomes 5 years old.

c. The manager may also authorize the transfer to a new position prior to the receipt of a completed FBI investigation provided a review of the existing PSF has been conducted and there is no security objection to such action.

17. ACCESS AUTHORIZATION DOCUMENTATION. When access authorization has been granted, the field element must make the appropriate entry to the CPCI within 2 working days. The field element will also update the File Summary Sheet in the individual's PSF and notify the requesting office.

18. REINITIATION OF CASES ADMINISTRATIVELY TERMINATED UNDER 10 CFR 710.6. If an individual fails to comply with a request for information, his/her case may be terminated under the procedures described 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 recertify the continued need for the individual to have an access authorization.

19. DOE CUSTODY OF PERSONNEL SECURITY FILES.

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, investigate a criminal violation, or ensure compliance with DOE requirements. Appropriate handling, transmission, and storage methods must be used to comply with this requirement. Reports of investigation or information contained in the PSFs must not be made available to contractor representatives.

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 United States 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, a record of each disclosure of a PSF as described in paragraph 19b or 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 information in the background investigation to other DOE employees who need the information to perform official duties is permitted by the Privacy Act of 1974, 5 U.S.C. 552a(b)(1). A psychiatrist conducting an evaluation at the request of DOE may be permitted access to the information contained in the background investigation.

f. Prior to 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 level 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 Part 1008, Records Maintained on Individuals (Privacy Act), regarding their release. That regulation describes 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 contained in 10 CFR 1008.6, Requests for Access or Amendment. Further information on how to submit a request for access can be obtained by contacting the local Privacy Act Officer.

21. NOTIFICATION OF ACCESS AUTHORIZATION DETERMINATION. 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. Notification of final determination will not be given in writing to the individual except when the determination is made as a result of the completion of the DOE administrative review process as specified in 10 CFR 710, or when the individual is also the designated official in the agency, firm, or organization to whom written notifications are normally forwarded.

22. 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 from bottom to 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; Personnel Security Assurance Program-related documents; and similar data. A File Summary Sheet (DOE F 5631.16 or equivalent) will 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 or treatment for mental illness, substance abuse, or alcohol abuse; interview transcripts or summaries; letters of interrogatory to the individual and responses thereto; correspondence and reports relating to psychiatric and/or psychological evaluations; case evaluations; and any other material relating to the adjudication of the individual's eligibility for access authorization.

23. RETENTION OF PERSONNEL SECURITY FILES. PSFs should be retained and disposed of in accordance with the approved National Archives and Records Administration (NARA)/DOE Record Schedule. The NARA approved schedule for these records calls for

personnel security clearance files to be destroyed 10 years after the termination, discontinuance, or cancellation of a clearance or access authorization.

CHAPTER III

INVESTIGATIVE RESULTS PROCESS AND ACCESS AUTHORIZATION DETERMINATIONS

1. SCREENING. Upon receipt of an investigative report, the individual assigned must screen it to ensure that the required DOE scope of investigation for the particular type of access authorization has been met.

   a. Background Investigations (Initial Investigations or Reinvestigations).

      (1) The report must be reviewed by the screener to ensure that thorough information is provided on the individual's residence, employment, education, and military service, and 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, should be checked against the employer as reported in the investigation to ensure that they are identical.

      (3) Those cases in which the investigation is complete and no derogatory information has been reported must be appropriately documented. If the individual assigned to the function 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 analyst to ensure that the investigation is in fact complete and that no derogatory information is present. 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 reviewer. The procedures listed under paragraph 1a(3) above should be followed.

2. ANALYSIS.

   a. Favorable and unfavorable investigative information must be analyzed in relation to the "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or SNM, Subpart A" (10 CFR 710, hereafter referred to as "criteria") and to determine whether the reported information raises substantial doubt concerning such eligibility.

Frequently, the reported derogatory information alone would raise such a concern but may be resolved when considered with other reported mitigating information.

b. Additional actions, such as those described in paragraphs 5 through 8 below, are frequently required to adjudicate a case. If one of these actions is necessary, the approval for such action (including a personnel security interview, letter of interrogatory, or additional investigation) must be by a senior personnel security specialist other than the analyst making the recommendation.

c. If an investigation is complete, the field element manager, or an individual who has been delegated written adjudication authority, 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. If the field element manager has determined that reported information falls within one or more of the categories in the criteria and the case cannot be resolved locally, the manager must suspend any access authorization currently in effect and transmit to the Director of Safeguards and Security a duplicate of the PSF, a summary statement, and a request for authority to initiate administrative review processing under 10 CFR 710. The individual's employer, any other field 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 access 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 updated and the individual's badging office notified.

3. REFERRAL OF CASE FOR REVIEW AND ADVICE. Field element managers may refer any case to the Director of Safeguards and Security for review and advice. Any case referred should reflect the manager's opinions and recommendations for further action.

4. ACTIONS AUTHORIZED BY THE OFFICE OF SAFEGUARDS AND SECURITY. The Director of Safeguards and 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 restoration of an access authorization; or

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

5. PERSONNEL SECURITY INTERVIEWS. Conducting personnel security interviews (PSIs) is a critical function of a personnel security official. 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 tape 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.

6. LETTERS OF INTERROGATORY. An alternative to a PSI is the letter of interrogatory, which may be sent to an individual if the information required is not of a serious nature, which may include minor drug use that ended more than 5 years ago, 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 resolve the security concern, a PSI must be scheduled to further explore the concern.

7. ADDITIONAL INVESTIGATION. When an additional investigation is required to expand, resolve, or corroborate information, the field element will submit a request for such investigation to either the OPM or the FBI, as appropriate.

8. 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 future intentions for such 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/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 Drug Certification violates its terms, an immediate evaluation of the circumstances of that violation must be conducted.

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

a. When a DOE or contractor employee or a consultant who has an access authorization is hospitalized or otherwise treated for a mental illness or mental condition, the DOE supervisor or a responsible DOE contractor official must report this information to the cognizant field element manager, or for Headquarters cases, to the Director of Safeguards and Security. Upon determination by the employer that the individual is able to perform

his/her regular duties, the individual's access authorization may be continued unless the field element manager or the Director of Safeguards and Security 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 manager or the Director of Safeguards and Security may accept previously rendered competent medical advice or records that are in the possession of DOE or a DOE contractor. The field element manager or Director of Safeguards and Security 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 cognizant Personnel Security Program manager. 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 field element manager or the Director of Safeguards and Security a written report containing his/her professional 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, his/her 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 9b above, the DOE-designated examiner must be notified that he/she may be called upon to testify before a hearing officer. Only psychiatrists or psychologists consenting to testify should be designated for examining purposes.

10. TIME ELEMENTS IN PROCESSING CASES. The following schedules should be observed in processing cases. (All time frames are in work days, unless otherwise indicated.)

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

b. Within 30 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 reaffirmed.

(2) Additional investigation will be requested.

(3) A Personnel Security Interview with the individual will be scheduled.

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

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

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

(7) Cases involving a DOE employee will be referred to the servicing personnel office as described in item 12 below.

c. After a field element manager or the Director of a Headquarters Operations Division requests approval to proceed with administrative review processing, the following time frames should be used in the various processing steps.

(1) The Office of Safeguards and Security will render a determination on the request for the initiation of administrative review processing within 30 days of receipt of the request.

(2) Within 30 calendar days of receiving administrative review authorization from the Office of Safeguards and Security, the field element manager (or for Headquarters cases, the Personnel Security Program Manager) will prepare and deliver a notification letter to the individual. Notification letters for Headquarters cases must be signed by the Director of Safeguards and Security. This notification letter constitutes the "Notice to the Individual" described in 10 CFR 710.21.

(3) The individual must respond to the notification letter within 20 calendar days of receipt of the notification letter.

(4) Should the individual fail to respond to the notification letter within 20 calendar days, he/she will be contacted again within 3 days to determine whether he/she intends to request a hearing. Unsuccessful attempts to locate an individual who has failed to respond should be documented.

(5) If the individual does not request a hearing, the case must be forwarded to the field element manager, or for Headquarters cases, the Director of Safeguards and Security, within 7 days of notice from the individual that a hearing is not requested, or within 7 days of the unsuccessful attempt to recontact the individual. In such cases, the manager or, for Headquarters cases, the Director of Safeguards and Security, will

be provided with the individual's PSF, and will issue a final determination within 30 days of receipt of the case.

(6) If the individual requests a hearing, the field element manager must assign an attorney to serve as DOE counsel and transmit the request to the Director, Office of Hearings and Appeals, within 15 days of receipt of the individual's request for a hearing. For Headquarters cases, the Director of Safeguards and Security must request the Office of General Counsel to assign an attorney to serve as DOE counsel and transmit the individual's request for a hearing to the Director, Office of Hearings and Appeals.

(7) Hearings must commence within 90 calendar days of receipt by DOE of the individual's request for a hearing.

(8) The court reporter must return the transcript of the hearing to the appropriate field element manager or, for Headquarters cases, the Director of Safeguards and Security, within 30 days of the completion of the hearing or closing of the record.

(9) The field element manager or, for Headquarters cases, the Director of Safeguards and Security, must transmit the completed hearing transcript to the hearing officer within 5 days of receipt from the court reporter.

(10) The hearing officer must issue an opinion within 30 calendar days of receiving the hearing transcript or closing of the record, whichever is later.

(11) Either the individual or the Office of Security Affairs may submit to the Director, Office of Hearings and Appeals, a request for review of the hearing officer's opinion within 30 calendar days of receipt of the opinion.

(12) Within 15 calendar days after filing a request for review, the party seeking the review (either the individual or the Office of Security Affairs) must file a statement identifying the issues on which it wishes the Director, Office of Hearings and Appeals, to focus. The other party has 20 calendar days (starting from the date of receipt of the statement identifying the issues for review) in which to file a response with the Director, Office of Hearings and Appeals.

(13) The Director, Office of Hearings and Appeals, must issue an opinion within 45 days of the closing of the record. Refer to 10 CFR 710.28 for further details on this process.

(14) Personnel Security Policy, Office of Safeguards and Security, must prepare a consolidation package within 30 calendar days of receipt of the completed record from the Office of Hearings and Appeals.

(15) The Director, Policy, Standards and Analysis Division, Office of Safeguards and Security, must make a determination on the recommended action within 5 days of receipt of the case from Personnel Security Policy.

(16) The Director, Office of Safeguards and Security, must make a determination on the recommended action within 5 days of receipt of the case from the Director, Policy, Standards and Analysis Division.

(17) The Director, Office of Security Affairs, must make a final determination within 30 days of receipt of the case.

(18) The Director, Office of Safeguards and Security, or the field element manager must notify the individual of the final determination within 10 days of the final determination.

11. EMPLOYER INQUIRIES. Once an individual is notified of his/her 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 that is developed as part of the Personnel Security Program 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 local Personnel Security office should establish procedures with the servicing personnel office(s) for the DOE employees under their jurisdiction for the referral of such information so that 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 prior to initiation of administrative review processing of the individual's eligibility for access authorization. However, a referral to the servicing personnel office does not preclude a manager from suspending 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 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 determination prior to a determination of employment eligibility, the employment decision must be rendered first.

CHAPTER IV

INTERIM ACCESS AUTHORIZATIONS AND WAIVERS OF PREAPPOINTMENT BACKGROUND INVESTIGATIONS

1. GENERAL. Only under exceptional circumstances and when such action is clearly consistent with the national interest will an individual, prior to completion of the appropriate investigation, be permitted to have access to classified matter or SNM or be allowed to occupy a position designated by the cognizant personnel office as Critical Sensitive. In all such cases, Interim Access Authorizations (IAAs) to either Restricted Data, National Security Information, SNM, or waivers of preappointment investigations must be considered temporary measures pending completion of the investigation, which must be in process. An IAA to Restricted Data, National Security Information, and SNM must be approved by the Director, Office of Security Affairs. A waiver of preappointment investigation must be approved only by the Secretary. Requests for IAAs must be made only for individuals required to have Q access authorizations. Individuals who require L access authorization must not be processed for IAAs.

2. INTERIM ACCESS AUTHORIZATION TO CLASSIFIED MATTER OR SNM.

   a. A written request for an IAA will be submitted to the Director, Office of Safeguards and 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 prior to completion of the access authorization procedures; and

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

   b. If an investigation was not requested prior to the request for IAA, the investigation request accompanied by the forms required for a Q access authorization must be submitted concurrently with the request for an IAA.

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

   d. Individuals who require an IAA 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 psychophysiological detection of deception testing at the DOE Test Center, Albuquerque,

New Mexico. 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 cognizant DOE personnel security office. AAAP information brochures may be requested from the Test Center by calling 505-346-7755.

e. IAAs are valid until the completion of the investigation and adjudication process and may be canceled by the Director of Security Affairs at any time based on unfavorable information. Such withdrawal of an IAA is not appealable during this stage of the processing. If such is the case, adjudication of the individual's eligibility for access authorization will continue upon receipt of the completed investigation.

f. If DOE withdraws an individual's IAA, the cognizant DOE 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 matter and SNM.

g. IAAs must not be processed for individuals who are dual citizens or are not United States citizens.

h. When DOE grants final Q access authorization, the IAA must be terminated. The CPCI should be updated to reflect this action within 2 working days of the final Q grant.

3. WAIVERS OF PREAPPOINTMENT INVESTIGATION. DOE will process requests for waivers of preappointment investigations in accordance with the procedures established by OPM in 5 CFR 732 and 736. The preappointment investigation requirement may not be waived for appointment to positions designated Special-Sensitive. DOE will not process waivers for non-sensitive positions. Guidelines for determining position sensitivity are contained in 5 CFR 732. The preappointment 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.

4. STANDARDS AND PROCEDURES.

a. The Office of Safeguards and Security must ensure that the following checks have been completed and reviewed with favorable results:

(1) review of an SF-86 signed by the individual;

(2) a credit search;

(3) check of the security files at any current or former place of Federal employment;

(4) the results of the individual's name being checked at the following locations:

(a) CPCI,
(b) FBI criminal history and investigative records,
(c) OPM Security/Suitability Index (SII),
(d) Defense Clearance and Investigations Index (DCII),
(e) Central Intelligence Agency Security and Operations Offices, and
(f) National Criminal Information Center (NCIC).

b. Expedited service for the access authorization investigation must be requested from OPM or the FBI.

c. Any derogatory information developed as part of these checks will be documented by the Office of Safeguards and Security and will be provided to the official determining eligibility for the IAA or the waiver of the preappointment investigation.

CHAPTER V

DATA ON SPOUSES AND COHABITANTS

1. GENERAL. To implement Section 145a of the Atomic Energy Act of 1954, as amended, and Executive Orders 12968 and 10450, which require an investigation and report on an individual's character, associations, and loyalty, DOE needs information on spouses and cohabitants of individuals seeking or holding access authorization. A cohabitant is a person who lives with the individual who requires access authorization. A cohabitant is a person other than a legal spouse, child, or other relative (in-laws, mother, father, brother, sister, etc.) and with whom the individual has a spouse-like relationship or similar bond of affection. In carrying out investigations of applicants and reinvestigations on incumbents, inquiries and record checks are made on spouses and cohabitants named on the SF-86. Therefore, individuals who marry or cohabitate after being granted an access authorization must complete a DOE F 5631.34, Data Report on Spouse/Cohabitant, if their spouse/ cohabitant has never held a DOE access authorization.

2. PROCEDURES.

   a. Cleared Individuals Who Marry or Cohabitate.

      (1) Within 45 days of marriage or cohabitation with an individual who has never held a DOE access authorization, an individual who has been granted access authorization must submit two copies of DOE F 5631.34 to the appropriate field element manager.

      (2) For individuals holding "Q" access authorization whose new spouse or cohabitant is either a foreign national or maintains dual citizenship an OPM National Agency Check (without fingerprint cards) will be requested on the new spouse or cohabitant by submitting the DOE F 5631.34 and a completed OFI 86C, Special Agreement Checks, to OPM. The OFI 86C should be overprinted with the appropriate agency agreement number (98-01) and an "S" should be entered in box 7 of the form.

      (3) For individuals holding "L" access authorization whose new spouse or cohabitant is either a foreign national or maintains dual citizenship, the DOE F 5631.34 should be forwarded to Personnel Security Policy, SO-211.2, who will arrange for the appropriate indices checks to be conducted.

   b. Name Changes. Whenever a DOE-cleared individual has a name change, the individual must notify the appropriate DOE security office so that the appropriate name change can be made on the CPCI.

CHAPTER VI

ACCESS AUTHORIZATIONS FOR FOREIGN NATIONALS AND DUAL CITIZENS

1. REQUIREMENTS. Where there are compelling reasons in the furtherance of the DOE mission, immigrant aliens and foreign nationals 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 matter and/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 Headquarters element with jurisdiction over the program where the individual will be employed, the Office of General Counsel, and the Office of Safeguards and Security prior to submission for investigation. A foreign national granted an access authorization must not receive access to the following types of classified matter.

   a. Top Secret, CRYPTO, or COMSEC information.

   b. Intelligence 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.

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

2. FOREIGN NATIONALS.

a. Field Elements must accomplish the following.

(1) Receive and consider requests for access authorizations for foreign nationals originated by DOE elements and contractors under their jurisdiction. Requests may be disapproved by the local Director of Security if the requirements of paragraph 1 above have not been met.

(2) Interview all foreign nationals seeking access authorizations to develop the detailed information described in Attachment II-1. The interview should address 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 United States;

(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 of Safeguards and Security if it is determined that an adequate investigation can be conducted and the evaluation of risks described in subparagraph (3) above is favorable. Include the following information and documents with the request:

(a) a duplicate PSF, including the paperwork completed by the individual and a transcript of the interview that has been conducted with the individual;

(b) a statement concerning the program for which the foreign national has been recruited and specific access to classified information and/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. Director of Safeguards and Security must accomplish the following.

(1) Coordinate the following reviews/determinations.

(a) Heads of Headquarters elements 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) A review of each request for a foreign national's access authorization to determine compliance with requirements of the Atomic Energy Act of 1954, as amended, regarding the release of Restricted Data to the government involved (and thereby the citizens of that government).

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

(3) Notify the concerned field element that the case has been approved for processing and may now be submitted for investigation in cases where favorable determinations have been made as a result of the reviews described in paragraphs 2b(1) and (2) above.

c. An SSBI is required for all types of access authorization for foreign nationals. If the individual has resided in or has relatives living in a country where the language is written in a non-Latin alphabet (e.g., Hebrew, Arabic, Chinese, Japanese, Russian), the individual may be required to translate the information on overseas addresses and relatives into the Latin alphabet.

d. The determination to grant an access authorization for a foreign national must be made by the field element manager and, in Headquarters, by the Director of Safeguards and 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 Headquarters element having functional interest in the work to be done and after a new review as described in paragraph b(1)(b) above.

f. The Office of Safeguards and Security will maintain duplicate PSFs on all foreign nationals holding access authorizations. The field element must provide copies of any additions to the

PSFs on these individuals. If the individual's citizenship status changes substantially, this information must be reported to the Office of Safeguards and Security.

3. DUAL CITIZENS. Individuals who possess a dual citizenship (i.e., who are simultaneously a citizen of the United States 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 his/her citizenship in the other country, he/she must provide a notarized statement attesting to the fact that the non-U.S. citizenship has been formally renounced, and if documentation is available, evidence that the renunciation has been formally accepted by an official representative of the other country's government. Copies of any documents completed by the individual to formally renounce his/her non-U.S. citizenship should accompany the notarized statement. An individual's statement of renunciation must be considered invalid if the individual continues to exercise his/her citizenship rights in a foreign country.

   b. Waiver. The cognizant field element manager, or the Director of Safeguards and Security for Headquarters cases, may waive the requirement to renounce the alternate 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. Extension of an access authorization is the process that allows an individual to hold concurrent active access authorizations under the cognizance of two or more DOE offices, two or more employers, or for one employer under two or more contract numbers. A Q access authorization can be extended as either a Q or an L access authorization, but an L access authorization can be extended only as an L access authorization. An access authorization may not be extended to a DOE element where the individual is not employed or does not perform contractual duties. QX and LX access authorizations cannot be extended because these access authorizations are granted for the limited access specified in an access permit.

   b. Transfer of an access authorization requires a DOE element to accept the active access authorization granted by another DOE element simultaneously with the termination of that access authorization by the latter.

   c. A request for extension or transfer of an access authorization must contain the full name of the individual and his/her date of birth, Social Security number, and DOE file number (if known) to establish positive identification.

   d. The DOE element having custody of the individual's PSF must inform the DOE element extending the access authorization or accepting it for 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. 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. An 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. In case of transfer, the PSF must be reviewed upon receipt and a note must be made to document the review before it is filed.

g. When supplemental investigation is deemed appropriate, requests for such an investigation must be submitted directly to the appropriate investigative agency.

h. 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.

i. When derogatory information develops after an access authorization has been granted or extended, the office in possession of the new information must notify all offices having an access authorization interest in the individual.

j. In extension cases, the DOE element that granted the original access authorization (or oldest active access authorization if the original has been terminated) must be indicated on the CPCI as being the PSF location and will be responsible for the Reinvestigation Program requirements in Chapter VIII of this Manual. The only exception is when the subsequent access authorization extension or action results in a higher type of access authorization. In such cases, the DOE element granting the higher type of access authorization will be indicated as the PSF location and must implement the Reinvestigation Program requirements.

k. The DOE element extending the access authorization and the DOE element accepting the transfer of an access authorization must update the CPCI accordingly.

l. IAAs may be extended or transferred among DOE offices. 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.

m. If the DOE element that originated the access authorization terminates the access authorization, the PSF must be sent to the office to which the access authorization had been extended as described in paragraph 2c below.

2. TERMINATIONS. Termination is the discontinuance of an individual's authorization to have access to classified matter or SNM. (For the purposes of this paragraph, terminations do not include suspensions or revocations.)

a. Causes.

(1) An access authorization is no longer required due to termination of employment or change of official duties so that the position no longer requires access to classified matter or SNM. Continuation may be authorized upon certification by the employer 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 is terminated if the holder is on leave of absence or extended leave and will not require access for at least 90 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 field element manager or the Director of Safeguards and Security.

b. Procedures.

(1) When an individual no longer requires an access authorization, the cognizant DOE 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 a DOE F 5631.29 from individuals since the form explains to the individuals their continuing security responsibilities after they no longer hold DOE access authorizations. When the DOE F 5631.29 cannot be provided, the reasons must be explained in a written notice, which also must include the reason for the termination.

(2) Within 2 working days of receipt of a DOE F 5631.29 or written notice, the cognizant DOE security office must note in the individual's PSF the date the access authorization was actually terminated and must enter the appropriate information to the CPCI.

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

c. Transfer of Personnel Security Files of Terminated Cases. When the PSF of an individual whose access authorization has been terminated at one field element is transferred to

another field element where the individual continues to require access authorization for retention, the transferring element must enter the new file location on the CPCI.

3. REINSTATEMENTS.

a. A new or updated and/or 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 received, a request for reinstatement should 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 to ensure that the individual being reinstated is the same person whose file is being reviewed.

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

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

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

(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 3c(3) or (4) 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 prior to reinstatement in any case 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 DOE has documentation that 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. Field elements may authorize the reinstatement of an access authorization prior to receipt of the new investigation by the FBI, provided the circumstances listed in subparagraph (d) above do not apply.

4. TRANSMITTAL OF PERSONNEL SECURITY FILES. Unclassified PSFs being transferred by mail must be sent by First Class mail or by other means approved for the transmittal of classified information. PSFs that are classified must be sent by authorized means. (See DOE M 471.2-1C, *Manual for Classified Matter Protection and Control*.) This applies to active or inactive PSFs and the mailing of one or more investigative reports to the investigative agencies or DOE elements. 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 DOE M 471.2-1C.

CHAPTER VIII

REINVESTIGATION PROGRAM

1. DESCRIPTION. The Reinvestigation Program is 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 will 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 at the existing level. The sponsor must certify to DOE that the individual requires continuation of the access authorization and indicate the level of classified information or category(ies) of SNM to which the individual requires access in order to perform the official duties of the position.

   If access authorization has been approved under Section 145b of the Atomic Energy Act of 1954, as amended, the Director of Safeguards and Security, or designee, must ensure annually that the individual continues to require access to classified material in order 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 of Security Affairs.

3. INDIVIDUAL COMPLIANCE. If an individual is recertified, he/she must be provided the required security forms by the cognizant DOE or contractor security office. The individual must be notified in writing that failure to provide updated security forms to the cognizant DOE security office within 30 calendar days of the formal notification of the requirement for reinvestigation may result in administrative termination of his/her access authorization. Individuals who fail to submit completed security forms within the 30-day period will be recontacted by the cognizant DOE 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 cognizant chief of personnel security. Individuals whose access authorizations are administratively terminated must receive a DOE Security Termination Statement to complete and return to the cognizant DOE security office. However, the signed DOE Security Termination Statement is not needed to effect the administrative termination action.

4. REINVESTIGATION.

a. Review of Continued Eligibility. A review of the individual's eligibility for continuation of the access authorization will be based upon reevaluation 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. Type of Reinvestigation. The type of reinvestigation to be conducted is determined by the type of access authorization held by the individual and the recertification 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. 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 will be conducted. The investigation may be expanded or upgraded to resolve issues. Fingerprint cards are required only if there has not been a previously valid technical check by the FBI.

(2) L Access Authorization. At each 10-year interval following completion of the previous investigation or reinvestigation, an NACLC will be conducted. The investigation may be expanded or upgraded to resolve issues. Fingerprint cards are required only if there has not been a previous valid technical check by the FBI.

c. Scheduling Reinvestigations. The manager of the DOE element must establish a schedule for submitting requests for reinvestigations for cases under his/her jurisdiction. The PSF location, as designated on the CPCI, will indicate the field element jurisdiction responsible for processing the reinvestigation. Reinvestigations must be submitted to the investigative agency as evenly throughout the year as possible. In addition, a reinvestigation must be scheduled whenever there is substantiated probable cause to believe 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. Evaluation Procedures. The results of the reinvestigation must be reviewed and adjudicated following the procedures described in Chapter III for initial investigations. When reinvestigation reports contain derogatory information and the individual has an active access authorization, the case must receive priority processing in order 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 office reviewing the reinvestigation reports must notify the cognizant field element of any unresolved derogatory information, including suspension of the access authorization.