

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

ORDER

DOE 5631.2B

5-18-88

SUBJECT: PERSONNEL SECURITY PROGRAM

-
1. PURPOSE. To establish the policy, responsibilities, and authorities for implementing the Department of Energy (DOE) personnel security program.
 2. CANCELLATION. DOE 5631.2A, PERSONNEL SECURITY PROGRAM, of 12-2-85.
 3. SCOPE. The provisions of this Order apply to all Departmental Elements and contractors performing work for the Department, as provided by law and/or contract and as implemented by the appropriate contracting officer.
 4. APPLICABILITY. The personnel security program of the Department applies to its employees, contractors, subcontractors, and any other individuals who require access to DOE classified information or special nuclear material, as follows:
 - a. The provisions of the Atomic Energy Act of 1954, as amended, Executive Orders 10450 and 12356, and Federal Personnel Manual chapter 732 apply to Departmental employees, applicants for employment, consultants, and employees of other Federal agencies, for employment and/or access to classified information.
 - b. The provisions of the Atomic Energy Act of 1954, as amended, and Executive Orders 10865 and 12356 apply to Departmental contractors, subcontractor employees and consultants, and access permittees.
 - c. The provisions of the Atomic Energy Act of 1954, as amended, apply to any other individual, not falling within the meaning of 4a and b, above, for access to Restricted Data, or special nuclear material under DOE control.
 5. REFERENCES.
 - a. DOE 1700.1, FREEDOM OF INFORMATION PROGRAM, of 11-19-79, which establishes procedures for processing requests made to DOE under the Freedom of Information Act.
 - b. DOE 1800.1A, PRIVACY ACT, of 8-31-84, which establishes Departmental implementation guidelines for the Privacy Act of 1974.

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Safeguards and
Security

- c. DOE 5631.4, CONTROL OF CLASSIFIED VISITS, of 5-25-84, which establishes standards and procedures for controlling visitors to DOE and DOE contractor, subcontractor, and access permittee facilities.
- d. DOE 5632.1A, PROTECTION PROGRAM OPERATIONS, of 2-9-88, which establishes policy, objectives and standards for the physical protection of security interests. This Order series includes clearance requirements for specific categories of special nuclear material.
- e. Title 10 Code of Federal Regulations (CFR) 710, Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Significant Quantities of Special Nuclear Material, which is used in cases in which there are questions of eligibility for DOE access.
- f. Title 48 CFR 970.2201, Basic Labor Policies, which establishes employment standards for management and operating contractors, including preemployment checks.
- g. Atomic Energy Act of 1954, as amended, Section 11, "Definitions"; Section 141, "Policy"; Section 143, "Department of Defense Participation"; Section 145, "Restrictions"; and Section 161.b, "General Provisions"; which provide statutory authority for establishing and implementing a DOE security program for controlling access to Restricted Data and special nuclear material.
- h. Executive Order 10450, "Security Requirements for Government Employees," of 4-29-53, as amended, which establishes the requirement for determining that all Federal employees are loyal, reliable, trustworthy, and of good conduct and character.
- i. Executive Order 10865, "Safeguarding Classified Information Within Industry," of 2-20-60, as amended, which establishes the basis for the industrial security program for civilian personnel.
- j. Executive Order 12356, "National Security Information," of 4-2-82, which establishes controls on access to National Security Information.
- k. Federal Personnel Manual, Chapter 732, "Personnel Security," which implements Executive Order 10450 throughout Federal departments and agencies.
- l. Federal Personnel Manual, Chapter 736, "Personnel Investigations," which deals primarily with National Agency Checks and Inquiries and full field investigations conducted by the Office of Personnel Management (OPM).

- m. Title 5 U.S.C. Section 552a, "Privacy Act of 1974," which establishes the legal requirements for collecting and retaining information on individuals.
 - n. Director of Central Intelligence Directive (DCID) No. 1/14, "Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information," of 11-27-84, which establishes the minimum personnel security standards in procedures governing eligibility for access to sensitive compartmented information.
 - o. "System Reference Manual" for the Central Personnel Clearance Index which details system operation and data input procedures for the Central Personnel Clearance Index.
6. DEFINITIONS. Personnel Security Program definitions are contained in Attachment 1.
7. POLICY AND OBJECTIVES.
- a. It is Departmental policy to grant individuals access to classified information, special nuclear material, or an exclusion area when DOE has determined that such access will not endanger the common defense and security and is clearly consistent with the national interest.
 - b. DOE contractors may not request clearances for the purpose of establishing cleared pools of potential employees or to alleviate responsibilities for escorting uncleared individuals within a security area. A clearance shall be requested only for individuals who have been offered employment or for personnel who are expected to fill projected vacancies or requirements.
 - c. Numbers and levels of security clearances will be kept to the minimum for operational efficiency. As soon as possible, after an individual no longer needs access to classified information or special nuclear material, DOE will terminate an individual's security clearance in accordance with the procedures of this Order. Security clearances will not be continued or kept active merely for an individual's personal convenience.
8. RESPONSIBILITIES AND AUTHORITIES.
- a. Secretary shall:
 - (1) Certify the specific positions of high importance or sensitivity that under section 145f of the Atomic Energy Act of 1954, as amended, are to be the subject of an FBI investigation.
 - (2) Authorize for a limited time, a critical-sensitive position to be occupied within DOE by an individual for whom a preappointment full field investigation has not yet been completed if such action is an emergency and in the national interest under section 3(b) of Executive Order 10450.

- (3) Authorize access to National Security Information pursuant to section 4.1(a) of Executive Order 12356 prior to completion of the required investigation when such action has been determined to be in the national interest.
 - (4) Establish written standards and specifications on the scope and extent of investigations under section 145g of the Atomic Energy Act of 1954, as amended.
 - (5) Make determinations required by 10 CFR 710.27(m)(2) and 10 CFR 710.33.
- b. The Assistant Secretary for Defense Programs (DP-1) shall:
- (1) Authorize access to Restricted Data pursuant to section 145b of the Atomic Energy Act of 1954, as amended, prior to, or in lieu of, completion of the required investigation after determining that such action is in the national interest.
 - (2) Act as special designee under 10 CFR 710.27(m)(2) to determine whether statements may be received by a Hearing Officer.
 - (3) Determine whether new evidence may be received in accordance with 10 CFR 710.29(b)(2).
 - (4) Designate the individuals who serve as Personnel Security Review Examiners to offer findings and recommendations in administrative review cases in accordance with 10 CFR 710.31.
 - (5) Submit records in administrative review proceedings to the Personnel Security Review Examiners in accordance with 10 CFR 710.30(d)(2) and (e).
 - (6) Grant, reinstate, continue, deny, or revoke access authorization in accordance with 10 CFR 710.32.
 - (7) Approve reconsideration of access authorization cases in accordance with 10 CFR 710.34.
- c. Deputy Assistant Secretary for Security Affairs (DP-30) shall:
- (1) Issue subpoenas to witnesses in all cases processed in accordance with 10 CFR 710.20 et seq.
 - (2) Determine whether the name of a witness who will testify in a DOE security hearing may be withheld from the individual or his/her

representative if the witness could be subject to intimidation or threats of physical harm, subject to the procedures of 10 CFR 710.27(m) and (n).

d. Heads of Departmental Elements shall:

- (1) Submit requests to the Secretary, through Director of Office of Personnel (MA-20), for waivers of the preappointment full field investigation requirement for candidates under consideration to occupy critical-sensitive positions.
- (2) Through DP-34, submit requests to the Secretary or DP-1 for interim access authorizations.

e. General Counsel (GC-1) shall:

- (1) Approve subpoenas to be issued pursuant to 10 CFR 710.25.
- (2) Review for legal sufficiency all access authorization cases processed under 10 CFR Part 710 prior to action by the Assistant Secretary for Defense Programs.

f. Chief Counsels (and for Headquarters Cases, GC-1) shall:

- (1) Concur in requests for suspensions in cases processed in accordance with 10 CFR 710.21.
- (2) Approve the notification letter to an individual whose eligibility for access authorization is in question in accordance with 10 CFR 710.22.

g. Heads of Headquarters Elements shall:

- (1) Determine the DOE access authorization requirement, if any, for each position under their jurisdiction to be occupied by a DOE employee or applicant for employment, consultant, or assignee; and, at the request of DP-34, verify in writing the individual's continuing need for a DOE access authorization.
- (2) Approve and transmit to the Director of Safeguards and Security requests for access authorization of employees of other Federal departments or agencies who require access to Restricted Data.
- (3) Approve for consideration and transmit to DP-34 applications for access authorizations for foreign nationals.

- (4) Approve and transmit to DP-34 requests for access authorizations to Restricted Data for members of the Armed Forces and civilian employees of the Department of Defense (DOD) and the National Aeronautics and Space Administration (NASA) assigned to duty with Headquarters Elements.
 - (5) Furnish DP-34 with an annual compilation of "positions of a high degree of importance or sensitivity," on March 30 of each year.
 - (6) Advise DP-34 when access authorizations are to be terminated in accordance with Chapter VII, paragraph 2, of this Order.
 - (7) Immediately notify DP-34 when a DOE cleared individual under their cognizance is hospitalized or otherwise treated for a mental illness or other mental condition which may cause a significant defect in judgment or reliability.
 - (8) Notify DP-34 of information of a personnel security interest for individuals under their cognizance who possess or are in process for a DOE access authorization.
- h. Servicing Personnel Offices shall:
- (1) Process and deliver to DP-34 all requests for access authorization for Headquarters employees, applicants for employment, consultants, and assignees under their jurisdiction after the appropriate preemployment processing has been completed. Requests shall include appropriate security forms and, when appropriate, a copy of the individual's most recent SF-171.
 - (2) Determine final action to be taken in those cases where employment suitability information involving a Departmental employee is developed prior to continuance of clearance processing, when applicable.
 - (3) When required, make a determination to continue processing requests for waivers of preappointment full field investigations.
- i. Director of Safeguards and Security (DP-34) shall:
- (1) Develop policy, objectives, standards, guides, and procedures and approve in writing exceptions to established policies for the Personnel Security Program, except those policies and procedures expressly governed by the provisions of 10 CFR 710.
 - (2) Authorize managers of operations offices to initiate security

investigations on foreign nationals who are applicants for security clearance.

- (3) Perform assigned functions and make recommendations to DP-1, as appropriate, on cases processed in accordance with the provisions of 10 CFR 710.
- (4) Process all requests by other Government agencies for verification of an individual's DOE security clearance status.
- (5) Maintain centralized records for all security clearance actions and ensure the accuracy of such records.
- (6) Coordinate requests by the Inspector General (IG-1) for access to personnel security information for investigative purposes.
- (7) Approve review of Headquarters personnel security files by properly identified employees of investigative agencies of the Federal Government and other routine users under the Privacy Act regulations and maintain records of such reviews.
- (8) Recommend to the Controller the amount of funding necessary for conducting personnel security investigations and authorize managers of operations offices to submit specified numbers of requests for investigation on an annual basis to the FBI and OPM, taking into consideration estimates furnished by field elements.
- (9) Maintain liaison with the FBI and OPM as the principal point of contact with these agencies on all personnel security matters.
- (10) Notify the FBI or OPM, as appropriate, of withdrawals of requests for investigation.
- (11) Initiate the following:
 - (a) Investigation of spouses of individuals who marry after having been processed for an access authorization.
 - (b) Appropriate investigation and grant access authorizations for access to Restricted Data for the following people:
 - 1 DOD and NASA personnel assigned for duty with DOE or DOE contractors or with other Federal departments or agencies.
 - 2 Employees of other Federal departments or agencies who require such access.

- (12) Accept properly executed certifications for DOD and NASA personnel assigned for duty with DOE and who require access to Restricted Data.
- (13) Concur on requests to the Secretary for waivers of preappointment full field investigation requirements for candidates under consideration to occupy critical-sensitive positions.
- (14) Accept properly executed requests for interim access authorizations, conduct appropriate index checks (such as name checks with other Government agencies), and forward such requests to DP-1 with appropriate recommendations.
- (15) Perform the following functions for Headquarters, energy technology centers, and power marketing administrations:
 - (a) Implement the personnel security program consistent with the policy, standards, guides, and procedures stated in this Order and in Title 10 CFR 710.
 - (b) Perform functions outlined below in subparagraphs 8j(2) through 8j(8), and 8j(13).
 - (c) Perform functions outlined below in subparagraphs 8j(16)(a) through 8j(16)(f) and 8j(16)(h) through 8i(16)(q).
 - (d) Make an annual compilation of positions of a high degree of importance or sensitivity for certification.
 - (e) Process DOE F 5631.34, "Data Report on Spouse."
 - (f) Process cases of DOE or DOE contractor personnel who are hospitalized or otherwise treated for a mental illness that may cause a defect in judgment or reliability.
 - (g) Determine the access authorization requirements and type of investigation to be conducted for applicants for DOE access authorization.
- (16) Approve all forms used in carrying out the DOE Personnel Security Program upon review by the Office of General Counsel for legal sufficiency.
- (17) Provide specialized training for DOE personnel security specialists.
- (18) Conduct periodic personnel security program reviews at Headquarters

and field organizations to ensure proper implementation of the provisions of this Order.

- (19) Determine, after discussion with the investigative agencies as appropriate, whether sufficient information can be obtained to determine the individual's eligibility for access authorization.
- (20) Process and transmit to DP-1 requests for access to Restricted Data which are to be granted pursuant to section 145b of the Atomic Energy Act of 1954, as amended.

j. Managers of Operations Offices shall:

- (1) Implement the personnel security program consistent with the policy, standards, guides, and procedures stated in this Order and in 10 CFR 710 for individuals employed in programs under their jurisdiction.
- (2) Authorize suspension of access authorization in accordance with 10 CFR Part 710.21.
- (3) Initiate requests for investigations and reinvestigations directly to the FBI or OPM.
- (4) Determine the access authorization requirements and type of investigation to be conducted prior to requesting investigations for DOE employees or applicants for employment, consultants, and assignees.
- (5) Determine the access requirements and type of investigation to be conducted prior to requesting investigations for DOE contractor or subcontractor employees, consultants, or access permittees and assure that management and operating contractors have completed the required preemployment checks in compliance with 48 CFR 970.2201.
- (6) Implement procedures requiring DOE supervisors and contractor organizations to report verified information when an individual under their jurisdiction who possesses an active access authorization is hospitalized or otherwise being treated for a mental or emotional condition that causes or may cause a significant defect in judgment or reliability; enter the appropriate remark on the Central Personnel Clearance Index; and remove this remark when the employee has recovered from the condition.
- (7) Arrange for a psychiatrist to conduct an evaluation when professional assistance is needed to determine whether an

individual has a mental illness or condition that causes or may cause a significant defect in the individual's judgment or reliability within the meaning of 10 CFR 710.

- (8) Implement procedures to ensure that DOE supervisors and contractor organizations are aware that:
 - (a) Information concerning an individual possessing an active DOE access authorization (or in process for same) that is a matter of personnel security interest, such as an arrest or an observation of illegal drug use, should be reported to a DOE security official; and
 - (b) Established reporting channels should be used in communicating a matter of personnel security concern to the appropriate DOE security official.
- (9) Request approval of DP-34 to initiate security investigations on foreign nationals.
- (10) Refer to DP-34 requests for access authorization for employees of other Federal departments and agencies.
- (11) Furnish DP-34 with the following:
 - (a) Written notifications of withdrawals of requests for access authorization;
 - (b) An annual compilation of positions of a high degree of importance or sensitivity on March 30 of each year;
 - (c) DOE F 5631.34, "Data Report on Spouse", for personnel under their jurisdiction who marry after being processed for an access authorization; and,
 - (d) DOE F 5631.3, "Estimates of Requests for Investigations for Security Clearance," on a quarterly basis.
- (12) Accept for access to Confidential or Secret National Security Information or Formerly Restricted Data involved in DOE contracts and subcontracts written assurances that personnel of the facility engaged in DOE work possess final DOD or NASA clearances for access to National Security Information and the type of investigation by which such clearances were granted. The written assurance shall be indicated on a DOE F 5631.20, "Request for Visit or Access Approval"; for NASA-cleared individuals a NASA Form 405 may be

substituted. Clearances granted by DOD contractors and interim Confidential or Secret clearances are not acceptable. Appropriate records of accepted clearances shall be maintained by the field element.

- (13) For the purpose of granting access to Confidential Restricted Data involved in DOE contracts and subcontracts, accept written assurances that personnel of the facility engaged in DOE work possess final DOD or NASA clearance for access to National Security Information. Such written assurances shall be indicated on a DOE F 5631.20; for NASA-cleared individuals, a NASA Form 405 may be substituted. The following conditions must also be met for access to Restricted Data:
 - (a) The individual must be a U.S. citizen.
 - (b) The individual must complete security forms including SF-86, "Questionnaire for Sensitive Positions," and DOE F 5631.18, "Security Acknowledgement."
 - (c) The DOD/NASA clearance must be based on an investigation completed within the past 5 years.
 - (d) The access is for a temporary period not to exceed 12 months.
 - (e) DOE reserves the right to submit security forms for investigation if a review of the forms indicates a security concern.
- (14) Send requests to the Secretary or DP-1, through DP-34, for interim access authorizations, and certify the requisite conditions therefor.
- (15) Send requests to the Secretary, through MA-20, for waivers of the preappointment full field investigation requirement for candidates under consideration to occupy critical-sensitive positions, and certify the requisite conditions therefor.
- (16) In addition to the above, managers of operations offices shall:
 - (a) Grant access authorization in all cases except those requiring processing for a hearing before a Hearing Officer.
 - (b) Have individuals interviewed, as appropriate, when the reported information falls within the criteria of 10 CFR 710 or Executive Order 10450.

- (c) Inform individuals whose DOE access eligibility has been approved after a personnel security interview using a security advisory letter.
- (d) Perform functions assigned to the manager of the operations office under 10 CFR 710.
- (e) Extend, accept for transfer, reinstate, and terminate access authorizations as appropriate.
- (f) Authorize transfer of contractor personnel whose access authorizations are based on investigations by the OPM or other Government agencies to positions of a high degree of importance or sensitivity prior to receipt of FBI reports.
- (g) Furnish DP-34 with appropriate notifications of all access authorization actions.
- (h) Approve and maintain records of review of personnel security files by properly identified employees of investigative agencies of the Federal Government and other routine users under Privacy Act regulations.
- (i) Accept investigations and reports on the character, associations, and loyalty of individuals made by the OPM, FBI, or another Government agency which conducts personnel security investigations, provided that a security clearance has been granted to such individuals by another Government agency based on such investigations and reports conducted within the last 10 years and updated with, at a minimum, a National Agency Check within the last 5 years.
- (j) Maintain personnel security files, as appropriate, containing copies of investigative reports and other pertinent data on individuals granted a DOE security clearance by that office.
- (k) Ensure that the information reflected on standard employment forms completed by DOE employees, applicants for employment, consultants, and assignees is consistent with the information reflected on prior security forms prior to forwarding the new security forms to the appropriate investigative agency.
- (l) Evaluate all applicable reports of investigations on DOE employees and applicants for employment under their jurisdiction for suitability and notify the cognizant office of the results of each investigation for appropriate action.

- (m) Arrange with other managers of operations offices to perform administrative services, under the provisions of this Order, when the location of a facility or individual justifies such an arrangement as a matter of convenience or economy.
- (n) Ensure proper redelegation in writing of DOE personnel security responsibilities and authorities when appropriate.
- (o) Request DP-34 approval for locally generated forms used in the DOE Personnel Security Program.
- (p) Ensure that proper notifications are made (such as cancellation of continuing classified visits) when DOE security clearances are terminated for individuals under the cognizance of that office.
- (q) Request the approval of DP-34 for exceptions to the provisions of this Order.

k. Individuals Applying for or Holding DOE Access Authorization shall:

- (1) Provide full, frank, and truthful answers to relevant and material questions and when appropriate furnish or authorize others to furnish information during the course of an initial personnel security background investigation or reinvestigation, a personnel security interview, in response to a letter of interrogatory, an examination, or hearing related to the determination of the individual's eligibility for DOE access authorization. The individual may elect on constitutional or other grounds not to comply; however, such refusal or failure to furnish or authorize others to furnish relevant and material information may prevent the Department from reaching an affirmative finding required for granting or continuing access authorization. In this event, any security clearance then in effect may be suspended and processed in accordance with 10 CFR 710, or, for applicants, further processing may be terminated.
- (2) An individual who holds a DOE clearance or who has completed a Personnel Security Questionnaire (DP-1), or SF-86 must notify the Department within 5 working days of all arrests, charges (including charges that are dismissed), or detentions by Federal, State, or other law enforcement authorities for any violations, other than traffic violations for which a fine of \$100 or less was imposed.
- (3) Furnish DOE F 5631.34, "Data Report on Spouse," to the appropriate DOE security office, in accordance with the provisions of Chapter V of this Order.

BY ORDER OF THE SECRETARY OF ENERGY:



LAWRENCE F. DAVENPORT
Assistant Secretary
Management and Administration

DEFINITIONS

1. Access refers to the following:
 - a. The knowledge, use, or possession of classified information required by an individual to perform his/her official duties and which is provided to the individual on a need-to-know basis.
 - b. Situations that may provide an individual proximity to or control over special nuclear material in quantities defined in the DOE 5632 Order series.
2. Access Authorization or Security Clearance is an administrative determination that an individual is eligible for access to classified information or special nuclear material. Clearances granted by the Department are designated Q, L, Top Secret or Secret.
 - a. Q Access Authorizations or Clearances are based on full field investigations conducted by the Federal Bureau of Investigation (FBI), OPM, or another Government agency that conducts personnel security investigations. Q clearances permit an individual to have access, on a need-to-know basis, to Top Secret, Secret, and Confidential levels of Restricted Data, Formerly Restricted Data, National Security Information, or special nuclear material as required in the performance of duties. When Q access authorizations or clearances are granted to employees of access permit holders the clearances are identified as Q(X) access authorizations or clearances and permit access only to the type of Secret or Confidential Restricted Data specified in the permit.
 - b. Top Secret Access Authorizations or Clearances are based on full field investigations conducted by OPM or another Government agency which conducts personnel security investigations. Top Secret clearances permit an individual to have access, on a need-to-know basis, to Top Secret, Secret, and Confidential levels of National Security Information and Formerly Restricted Data as required in the performance of duties.
 - c. L Access Authorizations or Clearances are based on National Agency Check and Inquiries with Credit for Federal employees, or National Agency Check with Credit for non-Federal employees, conducted by the OPM. L clearances permit an individual access, on a need-to-know basis, to Confidential Restricted Data; Secret and Confidential Formerly Restricted Data;

Secret and Confidential National Security Information provided such information is not designated classified cryptographic information (CRYPTO), other classified communications security (COMSEC) information, or Sensitive Compartmented Information; and special nuclear material in quantities described in the DOE 5632 Order series, as required in the performance of official duties. When L access authorizations or clearances are granted to employees of access permit holders, they are identified as L(X) access authorization or clearances and permit access only to the type of Confidential Restricted Data specified in the access permit. Additionally, the Manager of the Operations Office may grant an "L" access authorization or clearance to craft or manual workers, community management and service personnel, nurses, medical technicians, cafeteria workers, health and safety workers, purchasing and accounting groups, and others who are employed in classified construction or operation areas, provided the work of such individuals does not afford them:

- (1) More than visual access to buildings and equipment classified no higher than Secret Restricted Data; or
 - (2) Access to information classified higher than Confidential Restricted Data concerning plant operating characteristics, process data, weapons, or weapons components.
- d. Secret Access Authorizations or Clearances are based on National Agency Checks and Inquiries with Credit for Federal employees, or National Agency Checks with Credit for non-Federal employees, conducted by OPM. Secret clearances permit an individual access, on a need-to-know basis, to Secret and Confidential National Security Information and Formerly Restricted Data as required in the performance of duties.
3. Access Permittee designates an individual or organization who has been issued a permit by the Department, providing access to Restricted Data applicable to civilian uses of atomic energy in accordance with the terms and conditions stated on the permit and in accordance with applicable security regulations.
 4. Classified Information is Restricted Data, Formerly Restricted Data, or National Security Information, which requires safeguarding in the interest of national security.

5. Derogatory Information refers to unfavorable information on an individual which brings into question the individual's eligibility or continued eligibility for access authorization or suitability for Federal employment. Specific types of derogatory information are listed in 10 CFR 710 and Executive Order 10450.
6. Drug Certification is a written assurance signed by an individual stating the person will refrain from using or being involved with illegal drugs while employed in a position requiring DOE access authorization.
7. Exclusion Area is a security area for the protection of classified matter where mere access to the area would result in access to classified matter.
8. Formerly Restricted Data is classified information jointly determined by the Department (or its predecessors, the Atomic Energy Commission and the Energy Research and Development Administration) and the Department of Defense (DOD) to be related primarily to the military use of atomic weapons and removed by DOE from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.
9. Hearing Counsel is the DOE attorney assigned to prepare and conduct a personnel security hearing before a Hearing Officer.
10. Hearing Officer is an individual appointed by the manager of an operations office who, upon considering the evidence at a hearing, makes specific findings as to the truth of the derogatory information, and determines whether to recommend the granting, continuation, revocation, or denial of an individual's access authorization. Hearing Officers shall be U.S. citizens and have a DOE Q access authorization.
11. Interim Access Authorization is a determination by the Secretary, for access to National Security Information or Formerly Restricted Data, or by the Assistant Secretary for Defense Programs (DP-1), for access to Restricted Data or special nuclear material, that it is clearly consistent with the national interest for the Department to permit an individual interim access authorization prior to receipt of full field reports of investigation. Interim access authorizations are not processed for access permittees or for individuals whose accesses will require an L or Secret clearance.
12. Managers of Operations Offices means the manager of a DOE operations office, the Manager of Pittsburgh Naval Reactors Office, the Manager of Schenectady Naval Reactors Office, and at Headquarters, the Director of Safeguards and Security (DP-34).

13. National Security Information designates information which requires protection in the interest of national defense or foreign relations of the United States, that is, classified in accordance with Executive Order 12356 and does not fall within the definition of Restricted Data or Formerly Restricted Data.
14. Need-to-Know is a determination by persons having responsibility for classified information or matter, that a proposed recipient's access to such classified information or matter is necessary in the performance of official or contractual duties of employment under the cognizance of the Department of Energy.
15. Personnel Security Interview is a meeting held with an individual to discuss areas of security concern.
16. Personnel Security Review Examiners are persons appointed by Assistant Secretary for Defense Programs (DP-1) who are designated to review questions concerning the eligibility or continued eligibility of individuals described in 10 CFR 710.20. Examiners shall be U.S. citizens and have a DOE Q access authorization.
17. Restricted Data is defined in section 11y of the Atomic Energy Act of 1954, as amended, as "...all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy; but shall not include data declassified or removed from the Restricted Data category pursuant to section 142."
18. Security Advisory Letter is a written notification to an individual following the favorable resolution of the individual's eligibility for access authorization after a security interview. The letter shall advise the individual that further involvement in the activity that prompted the interview could result in review of eligibility for access authorization under the terms of 10 CFR 710.
19. Security Area is a physically defined space containing a Departmental security interest and subject to physical protection and personnel access controls.
20. Special Nuclear Material, as defined in Section 11 of the Atomic Energy Act of 1954, as amended, means (1) plutonium, uranium enriched in the isotope 233 or in the isotope 235, and any other material which is determined to be SNM, pursuant to section 51 of the Atomic Energy Act of 1954, but does not include source material; or (2) any material artificially enriched by any of the foregoing, but does not include source material.

TABLE OF CONTENTS

	<u>Page</u>
<u>CHAPTER I - GENERAL GUIDELINES FOR DETERMINING LEVEL OF ACCESS AUTHORIZATION AND INVESTIGATIVE REQUIREMENTS</u>	
1. General	I-1
2. Determining Investigative Requirements	I-2
a. Criteria That Determine Investigative Requirements for DOE Employees, Consultants, and Assignees	I-2
b. Criteria For Determining Investigative Requirements for DOE Contractor and Subcontractor Employees, Consultants, and Access Permittees	I-3
c. Other Federal Department or Agency Employees and Legislative and Judicial Branch Employees	I-4
3. Sensitive Compartmented Information	I-4
4. Attachment I-1--Access to Classified Information Allowed by Clearance Types	I-5
<u>CHAPTER II - PROCESSING PERSONNEL SECURITY CASES</u>	
1. General	II-1
2. Preparing the Request	II-1
3. Investigative Requirements for Access Authorizations	II-1
4. Prescreening of Personnel Security Cases	II-2
5. Personnel Security File Numbers	II-3
6. Processing the Forms Used to Request Investigations	II-3
7. Access Authorization for Other Federal Agency Employees	II-5
8. DOE and DOE Contractor Personnel Assigned to DOD or NASA	II-5
9. Additional Requirements for Investigating Naturalized U.S. Citizens and Individuals Who Have Resided in Foreign Countries	II-6
10. Transmittal of Investigative Reports Upon Completion	II-6
11. Cancellation of Requests for Access Authorization or Investigation	II-6
12. Requests for Copies of Missing Reports	II-7
13. Types of Investigations	II-7
a. Federal Bureau of Investigation	II-7
b. Office of Personnel Management	II-8
c. Background Investigations by Other Federal Agencies	II-9
d. Incomplete National Agency Checks	II-9
e. Requests for Full Field Investigations When the National Agency Checks Reveal Derogatory Information	II-10
14. Requesting FBI Investigation for Individuals Transferred to Posi- tions of a High Degree of Importance or Sensitivity	II-10
15. Requesting Expedited Investigations	II-11
16. Documentation Required in Granting Access Authorizations	II-11
17. Reopening of Cases in Which Requests for Access Authorization Were Cancelled	II-11

18.	Departmental Custody of Investigative Reports	II-12
19.	Release of Contents of Personnel Security Files.....	II-14
20.	Notification of Access Authorization Determination	II-14
21.	Contents of and Arrangement of Data in Personnel Security Files	II-15
	Attachment II-1 -- Forms Required for Security Investigations	II-17
	Attachment II-2 -- Additional Information to be Obtained for Investigation of Naturalized U.S. Citizens or Individuals Who Have Resided in Foreign Countries	II-19

CHAPTER III - SCREENING AND ANALYSIS OF PERSONNEL SECURITY CASES AND
METHODS FOR DETERMINING ACCESS AUTHORIZATION ELIGIBILITY

1.	Screening	III-1
2.	Analysis	III-2
3.	Referral of Cases for Review and Advice	III-2
4.	Actions Authorized by the Office of Safeguards and Security	III-2
5.	Interviews	III-3
6.	Security Advisory Letters	III-3
7.	Interrogatories	III-4
8.	Additional Investigations	III-4
9.	Special Updates	III-4
10.	Drug Certificates.....	III-4
11.	Administrative Review Procedures	III-4
12.	Persons Treated for Mental Illness or Mental Conditions	III-4
13.	Disclosure of Reported Information	III-5
14.	Time Element in Processing Cases	III-6
15.	Referral for Suitability Determination.....	III-7

CHAPTER IV - INTERIM ACCESS AUTHORIZATIONS AND WAIVERS OF PREAPPOINTMENT
FULL FIELD INVESTIGATIONS

1.	General	IV-1
2.	Interim Access Authorization to Restricted Data	IV-1
3.	Interim Access Authorization to National Security Information	IV-1
4.	Waiver of Preappointment Full Field Investigation	IV-2
5.	Standards and Procedures	IV-3

CHAPTER V - DATA ON SPOUSES

1.	General	V-1
2.	Procedures	V-1
3.	Additional Requirements	V-2

CHAPTER VI - ACCESS AUTHORIZATIONS FOR FOREIGN NATIONALS, INDIVIDUALS
POSSESSING DUAL CITIZENSHIP, AND NATURALIZED U.S. CITIZENS

1. Requirements	VI-1
2. Standards and Procedures for Processing Foreign Nationals	VI-1
3. Dual Citizenship	VI-4
4. Naturalized U.S. Citizens.....	VI-4

CHAPTER VII - EXTENSIONS, TRANSFERS, TERMINATIONS AND REINSTATEMENTS
OF ACCESS AUTHORIZATIONS

1. Extensions and Transfers	VII-1
2. Terminations	VII-3
3. Reinstatements	VII-4
4. Transmittal of Personnel Security Files	VII-5

CHAPTER VIII - REINVESTIGATION PROGRAM

1. General Information	VIII-1
2. Reevaluation	VIII-1
3. Determining the Type of Reinvestigation To Be Conducted	VIII-1
4. Scheduling Reinvestigations	VIII-2
5. Evaluation Procedures	VIII-2

CHAPTER IX - ESTIMATES OF REQUESTS FOR SECURITY INVESTIGATIONS

1. General	IX-1
2. Procedures	IX-1
3. Records	IX-1

CHAPTER I

GENERAL GUIDELINES FOR DETERMINING LEVEL OF
ACCESS AUTHORIZATION AND INVESTIGATIVE REQUIREMENTS

1. GENERAL. Requests for investigation shall be submitted only after a determination has been made that the duties of a position require access to classified information or special nuclear material in quantities defined in the DOE 5632 Order series, or access to an exclusion area. Security clearances are not to be requested to alleviate individual or management responsibilities for properly safeguarding classified information or controlling dissemination of such classified information on a need-to-know basis, or to preclude the use of access controls or physical barriers to distinguish between classified and unclassified areas or facilities, or to determine suitability for Government employment. It is Departmental policy that clearances shall be granted only when absolutely required and at the level of access required to avoid the unnecessary expenditure of Departmental funds and resources or the unwarranted invasion of an individual's right to privacy.
 - a. Except as authorized by the Secretary (for National Security Information and Formerly Restricted Data) or the Assistant Secretary for Defense Programs (for Restricted Data or Special Nuclear Material), the determination to grant access authorization shall be based on an investigation and report by OPM or the FBI. The determination may also be based on an investigation conducted by another Government agency that conducts personnel security investigations, provided (in instances involving access to Restricted Data) that a security clearance was granted to such individuals by another Government agency based on the investigation and report. Moreover, the investigation must be comparable in scope to the investigation DOE would ordinarily request for that position, cannot be more than 10 years old, and must have been updated with at least a National Agency Check within the most recent 5 years. The determination made by the Assistant Secretary for Defense Programs for access to Restricted Data or special nuclear material also permits an individual to have access to the other types of classified data reflected in Attachment I-1.
 - b. DOE will take all reasonable measures to obtain existing investigative reports that may fulfill Departmental standards and specifications for the scope and extent of investigations, as established by the Secretary.
 - c. Requests for clearances shall not be processed: (1) unless all required security forms are completed and signed (when appropriate) by the applicant and/or sponsor; (2) if the printed content of the security forms has been altered; (3) if insufficient, incorrect, or conflicting information is provided or (4) if the forms are illegible.

- d. The use of interim access authorizations shall be kept to the absolute minimum and considered only when properly requested in accordance with the requirements of Chapter IV.
 - e. Determinations for access to Restricted Data pursuant to section 145b, Atomic Energy Act of 1954, as amended, normally will be used only for the President and Vice-President, Federal judges and justices, members of Congress, and governors and lieutenant governors.
 - f. Updated security forms may be requested by DOE security officials in the course of the Reinvestigation Program, or at any time when there is probable cause that the individual has engaged in activity that may affect continued eligibility for access authorization.
 - g. Except where otherwise specified in this Order or other DOE Orders, individuals requiring access to classified data under DOE control in order to perform work for the DOE, must possess an active DOE access authorization prior to being afforded such access.
 - h. Individuals under DOE cognizance must possess an active DOE Q or Top Secret access authorization, as appropriate, for access to any level of classified data designated as "CRYPTO," "COMSEC," or "Sensitive Compartmented Information."
2. DETERMINING INVESTIGATIVE REQUIREMENTS. To ensure that investigative coverage is appropriate for the access required for a position, a determination shall be made on what type of classified information, special nuclear material, or exclusion areas are required by each position. This determination shall be certified in writing to DP-34 or to the appropriate official of a field organization.
- a. Criteria that Determine Investigative Requirements for DOE Employees, Consultants, and Assignees.
 - (1) Q Sensitive. A position involving the following responsibilities should be designated a "position of a high degree of importance or sensitivity" (Q sensitive access authorization) within the meaning of section 145f of the Atomic Energy Act of 1954, as amended, and requires an investigation by the FBI.
 - (a) Access to Top Secret Restricted Data.
 - (b) Access to any Restricted Data involving broad policy or program direction when the duties of the position affect such policy or program direction in any of the following areas:
 - 1 Research and development programs pertaining to nuclear or thermonuclear weapons or special nuclear material production;

- 2 Production or stockpile of nuclear or thermonuclear weapons or special nuclear material;
- 3 Research, development, or production in the laser fusion or laser isotope programs; or
- 4 The naval nuclear propulsion program including broad policy or program direction and fuel manufacturing technology.

(c) Any other position so designated by the Secretary.

- (2) Q Nonsensitive is designated if the incumbent in a position requires access to Secret Restricted Data or access to special nuclear material in quantities described in the DOE 5632 Order series.
- (3) Top Secret. The presence of the following criteria indicates that the incumbent in a position requires a Top Secret access authorization:
 - (a) Access to Top Secret National Security Information; or
 - (b) Access to and development of war plans, particulars of future or major or special operations of war, or critical or extremely important items of war.
- (4) L is designated if the incumbent in a position requires access to Confidential Restricted Data or access to special nuclear material in quantities described in the DOE 5632 Order series.
- (5) Secret is designated if the incumbent in a position requires access to Secret or Confidential National Security Information or Formerly Restricted Data.

b. Criteria for Determining Investigative Requirements for DOE Contractor and Subcontractor Employees, Consultants, and Access Permittees.

- (1) To ensure that investigative coverage is appropriate, the individual's type of access (Restricted Data, National Security Information, or special nuclear material) and level of access (Top Secret, Secret, or Confidential) shall be determined, using the criteria listed on page I-2, paragraph 2a, before a request for investigation is made by the appropriate DOE official. Additionally, a DOE contractor or subcontractor employee or consultant position shall be designated as a "position of a high degree of importance or sensitivity" within the meaning of section 145f of the Atomic Energy Act of 1954, as amended, when the duties of that position fall within the scope of paragraph 2a(1) of this chapter.

- (2) It is Departmental policy not to establish a separate clearance program for DOE contractor and subcontractor employees and consultants and access permittees for positions associated with unclassified Federal computer systems. Rather, the contractor, subcontractor, consultant, or access permittee is responsible for maintaining satisfactory standards of employees' qualifications, performance, conduct, and business ethics under its own personnel policies (Department of Energy Acquisition Regulation, Subpart 970.22, "Application of Labor Policies").

c. Other Federal Department or Agency Employees and Legislative and Judicial Branch Employees

- (1) DOE will withhold access to Restricted Data, Formerly Restricted Data, or National Security Information under DOE responsibility and access to quantities of special nuclear material to other Federal department or agency employees and Legislative and Judicial Branch employees until the Department has determined that such access shall not endanger the common defense and security. Except as authorized by the Secretary or the Secretary's designee that such action is clearly consistent with the national security, this determination shall be based on an investigation and report by the Office of Personnel Management (OPM), FBI, or another Government agency that conducts personnel security investigations, provided (in instances involving access to Restricted Data) that a security clearance has been granted to the individual based on the investigation and report.
- (2) Additionally, a position within other Federal agencies (exclusive of DOD and NASA personnel, who do not require DOE security clearance by virtue of section 143 of the Atomic Energy Act of 1954, as amended, or section 304(b) of the National Aeronautics and Space Act of 1958) shall be designated as a "position of a high degree of importance or sensitivity" within the meaning of section 145f of the Atomic Energy Act of 1954, as amended, when the duties of that position fall within the scope of paragraph 2a(1) of this chapter.

3. SENSITIVE COMPARTMENTED INFORMATION. Within the Department, determination of individual's eligibility for access to Sensitive Compartmented Information (SCI) is the responsibility of the DOE Senior Official of the Intelligence Community and his or her designated representative(s). The granting of access to SCI shall be controlled under the strictest application of the "need-to-know" principle under procedures prescribed in Director of Central Intelligence Directive (DCID) No. 1/14, which requires a 15-year background investigation. The Senior Official of the Intelligence Community will approve only DOE and DOE contractor employees for access to SCI.

ACCESS TO CLASSIFIED INFORMATION
ALLOWED BY CLEARANCE TYPES

	<u>RESTRICTED DATA</u>	<u>FORMERLY RESTRICTED DATA</u>	<u>NATIONAL SECURITY INFORMATION</u>
Q SENSITIVE	TOP SECRET SECRET CONFIDENTIAL	TOP SECRET SECRET CONFIDENTIAL	TOP SECRET SECRET CONFIDENTIAL
Q NONSENSITIVE	----- SECRET CONFIDENTIAL	TOP SECRET SECRET CONFIDENTIAL	TOP SECRET SECRET CONFIDENTIAL
TOP SECRET	----- ----- -----	TOP SECRET SECRET CONFIDENTIAL	TOP SECRET SECRET CONFIDENTIAL
L	----- ----- CONFIDENTIAL	----- SECRET CONFIDENTIAL	----- SECRET CONFIDENTIAL
SECRET	----- ----- -----	----- SECRET CONFIDENTIAL	----- SECRET CONFIDENTIAL

CHAPTER II

PROCESSING PERSONNEL SECURITY CASES

1. GENERAL. This chapter covers the procedures for initiating and processing requests for full field investigations, National Agency Checks and Inquiries with Credit, and National Agency Checks with Credit, required for access authorizations.
2. PREPARING THE REQUEST.
 - a. Before a request for investigation or access authorization is submitted, the following determinations should be made:
 - (1) The access authorization required (guidelines contained in Chapter I).
 - (2) Whether the individual has previously been granted access authorization that can be reinstated, transferred, or extended.
 - (3) Whether the individual has been granted a security clearance by another Government agency, and if so, all available information relating to such clearance (date, place, level, whether active or terminated, and so forth).
 - (4) Whether the individual is a foreign national or dual citizen requiring Headquarters approval prior to processing for investigation (see Chapter VI).
 - b. Types of access authorizations and forms required to process each are indicated on Attachment II-1.
3. INVESTIGATIVE REQUIREMENTS FOR ACCESS AUTHORIZATIONS. Investigations are required for access authorization as indicated below:
 - a. Q Sensitive - Access authorization for a "position of a high degree of importance or sensitivity," requires a full field investigation that covers at least the most recent 15 years. The investigation is conducted by the FBI. Persons under 18 years of age may not be processed for an FBI full field investigation, but should be submitted for background investigation by OPM.
 - b. Q Nonsensitive, QL, Top Secret, and QX require an OPM full field background investigation. When a QL is requested, the National Agency Check portion of the investigation is usually returned in advance of the full field investigation, and an L access authorization can be granted if appropriate,

pending completion and review of the full field investigation. These levels of access authorization may also be based on full field investigation by a Government agency other than the FBI or OPM which conducts personnel security investigations, provided that a security clearance has been granted to the individual by that agency based on a full field investigation and report and that the investigation was conducted within the last 5 years.

- c. L, Secret, and LX require the OPM National Agency Check and Inquiry with a credit check for Federal employees, or the OPM National Agency Check with credit check for non-Federal employees.
 - d. QB requires no investigation. This is an access authorization granted by the Assistant Secretary for Defense Programs, 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 normally will be processed only for the President and Vice-President, members of Congress, Federal justices and judges, and governors and lieutenant governors. A QB access authorization precludes the conduct of a background investigation, and, therefore, shall not be requested when an interim access authorization is appropriate, or when an investigation report exists which may be used as a basis for an access authorization.
4. PRESCREENING OF PERSONNEL SECURITY CASES. Personnel security cases shall be prescreened by the requesting Departmental security office to ensure that:
- a. All information, including the proper forms for a full and timely investigation, is made available to the investigative agency;
 - b. Omissions or discrepancies on the SF-86 or SF-171 have been corrected;
 - c. The individual has provided the required explanation to any "YES" answers to items 21 through 30 on the SF-86;
 - d. A proper justification for the need for clearance has been provided by the sponsoring entity; and,
 - e. If the request is submitted by either a DOE personnel office for a Federal employee, or by a management and operating contractor who is subject to compliance with 48 CFR 970.22, that preemployment checks have been completed with favorable results.
5. PERSONNEL SECURITY FILE NUMBERS will be assigned consecutively by the appropriate security office, as individuals are initially processed for any

type of DOE access authorization. A DOE personnel security file number shall continue to be used for identifying that individual's file, regardless of the element location of that file. The symbol of the submitting office shall be used as a suffix if it differs from the original DOE file number.

6. PROCESSING THE FORMS USED TO REQUEST INVESTIGATIONS.

- a. SF-86 will be used in requesting National Agency Checks with Credit, National Agency Checks and Inquiries with Credit, and full field investigations, or in initiating reinvestigations or reinstatements. The form submitted should be legible, completely filled out, and based on information furnished by the individual. A copy of the completely executed SF-86 shall be retained by the security office submitting the request. The original and one copy of the SF-86 shall be submitted to the investigative agency. No more than 60 days shall elapse between the date of execution of the SF-86 and its submission to the investigative agency. Forms that are more than 60 days old shall be returned to the individual for updating and resigning.
- b. Fingerprint Cards, SF-87, shall be used in cases involving Federal employees being processed for OPM investigations. In all other cases, the FD-258 will be used. The DOE Security File number should be inserted in the "Number" space on the FD-258 and listed on the bottom of the "Title and Address" section of the SF-87. The type of access authorization requested can be stamped on the block entitled "Reason Fingerprinted" or the block entitled "Title and Address." "U.S. Department of Energy, Washington, DC," will be typed in the block entitled "ORI" where this has not already been overprinted.
 - (1) It is essential that the personnel assigned to take fingerprints be adequately trained to recognize unclassifiable prints and to ensure that such prints are not submitted. Fingerprint cards that cannot be classified by the FBI cause undue delay in the clearance determination process. Should fingerprints be returned by the FBI as "unclassifiable," it is important to take particular care in making retakes to ensure that the resubmissions are classifiable.
 - (2) When submitting fingerprint retakes, the unclassifiable or illegible fingerprint card should be attached to the new card with a cover letter indicating the type of investigation and access

authorization requested for the individual. When submitting retakes to the OPM, it is particularly important to ensure that the OPM serial number is clearly indicated on the previously rejected fingerprint cards attached to the new retakes.

- (3) Fingerprint retakes for individuals being processed for OPM full field investigations, National Agency Checks with Credit, or National Agency Checks and Inquiries with Credit shall be forwarded to the following address:

U. S. Office of Personnel Management
Personnel Investigations Division
NACI Center
Boyers, PA 16018

- (4) Fingerprint retakes for individuals being processed for FBI investigations shall be submitted to the following address:

Federal Bureau of Investigation
U. S. Department of Justice
ATTN: Identification Division
Washington, DC 20535

- (5) If an individual's fingerprints cannot be classified after 2 attempts (original submission and 1 retake consisting of a newly obtained fingerprint card), the clearance determination may be rendered without classifiable fingerprints by the cognizant DOE security office.

- c. DOE F 5631.16, "File Summary Sheet," shall be prepared and placed in the individual's personnel security file.
- d. The applicable forms shall be enclosed in a transmittal jacket or envelope which lists on the outside the full name, the DOE file number, and the type of access authorization requested of the individual.

7. ACCESS AUTHORIZATION FOR OTHER FEDERAL AGENCY EMPLOYEES. All requests for access authorization of employees of other Federal agencies or departments and their contractors shall be processed through the Director of Safeguards and Security, DOE. Personnel of the Department of Defense and the National Aeronautics and Space Administration may have access to Restricted Data under the certification procedures outlined in DOE 5631.4, CONTROL OF CLASSIFIED VISITS, except in cases indicated below.
 - a. DOD and NASA Personnel Assigned to the Department. These individuals shall require DOE access authorization and shall in their assigned capacity 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 an appropriate certification of clearance from their Department or 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 regulations.
 - b. DOD and NASA Personnel Assigned to Other Federal Agencies. When these individuals require DOE access authorization, the requests must be initiated by the agency to which they are assigned.
8. DOE AND DOE CONTRACTOR PERSONNEL ASSIGNED TO DOD OR NASA. Any DOE or DOE contractor employee acting as a consultant or member of an advisory board of DOD or NASA who in that capacity possesses appropriate DOD or NASA clearance shall, for the purposes of this Order, be considered as a temporary employee of DOD or NASA. In this capacity he/she may communicate Restricted Data to personnel of DOD or NASA and their contractors in accordance with the security regulations of DOD or NASA. In the event the DOE employee or contractor does not require a clearance or access authorization for DOE work, but does require a clearance for assignments to the other agency, it shall be the responsibility of the other agency, rather than DOE, to request the appropriate investigation, adjudicate the reported information, and grant the appropriate type of clearance.

9. ADDITIONAL REQUIREMENTS FOR INVESTIGATING NATURALIZED U. S. CITIZENS AND INDIVIDUALS WHO HAVE RESIDED IN FOREIGN COUNTRIES.

- a. Additional investigative information is required of individuals who became naturalized U.S. citizens subsequent to their 18th birthday or U.S. citizens who have resided in foreign countries, for the purpose of determining their eligibility for access authorization. The supplemental information outlined in Attachment II-2, "Additional Information To Be Obtained for Investigation of Naturalized U.S. Citizens or Individuals Who Have Resided in Foreign Countries" shall be furnished by the applicant. This shall be submitted to the investigative agency with the completed SF-86.
- b. If, upon review of SF-86 by the DOE security office, it appears unlikely that an adequate investigation is possible, all material pertaining to the case shall be forwarded to the Office of Safeguards and Security for discussion with the investigative agencies (Department of State, Immigration and Naturalization Service, and other Federal agencies), as appropriate. The Office of Safeguards and Security shall then advise the requesting DOE security office on whether sufficient information can be obtained to determine the individual's eligibility for access authorization. In cases where the individual has resided in or has relatives living in a country where the language is written in a non-Roman alphabet (e.g., Hebrew, Arabic, Chinese, Japanese, or Russian), the individual should be requested to furnish the identifying information on former overseas addresses and on relatives written in the other alphabet.

10. TRANSMITTAL OF INVESTIGATIVE REPORTS UPON COMPLETION. The OPM forwards reports of full field investigations and the results of National Agency Checks with Credit and National Agency Checks and Inquiries with Credit directly to the requesting organization. Completed FBI investigations are sent to the Office of Safeguards and Security. The documents are then transmitted to the appropriate field element. Upon receipt of the reports, each field element shall enter the date the reports were received into the Central Personnel Clearance Index following instructions contained in the "System Reference Manual."

11. CANCELLATION OF REQUESTS FOR ACCESS AUTHORIZATION OR INVESTIGATION.

- a. Cancellation Prior to Completion of Investigation. When a request for access authorization or investigation of an individual is withdrawn prior to completion of the investigation, National Agency Check with Credit, or National Agency Check and Inquiry with Credit, the Office of Safeguards and Security shall immediately be notified by telephone in order to discontinue the investigation. The call shall be followed by a teletype message containing the full name of the individual, date of

birth, social security number, the DOE security file number, the name of the investigative agency, and the date and type of request being canceled (Q, Top Secret, L, or Secret). The Office of Safeguards and Security shall immediately notify the investigative agency by telephone to discontinue the investigation, and shall confirm this notice by letter for FBI cases, forwarding a copy to the interested field element. The field element shall enter the cancellation information into the Central Personnel Clearance Index following instructions contained in the "System Reference Manual."

- b. By agreement with the FBI and OPM, the Department is charged for the full cost investigation if any field investigation has been scheduled or conducted.
 - c. Cancellation After Completion of Investigation. When a request for access authorization is canceled or withdrawn after completion of the investigation, but prior to granting of access authorization, the cognizant Departmental Element shall enter this information into the Central Personnel Clearance Index.
 - d. Cancellation of Request for Reinvestigation. When an individual terminates employment, or the need for access authorization no longer exists, the manager of the operations office, or for Headquarters cases (including regional employees), the servicing personnel office or the employing personnel or security office, shall immediately notify the Office of Safeguards and Security by telephone, so that the reinvestigation may be discontinued. A teletype memorandum shall follow to verify the cancellation. Names may be included on messages concerning applicant type investigations, provided that the individuals are identified as subjects of reinvestigation. In addition, two separate actions must be taken to update the Central Personnel Clearance Index: (1) The current, active clearance must be terminated, and (2) the pending reinvestigation must be closed either by a deletion or by evaluation of the reports and submission of the results to Central Personnel Clearance Index.
12. REQUESTS FOR COPIES OF MISSING REPORTS. Requests for copies of missing reports shall be made by memorandum to the Office of Safeguards and Security for processing to the OPM or FBI. Each request shall be accompanied by a copy of the DP-1, SF-85, or SF-86 which served as the basis for the investigation. Upon receipt of copies of the missing reports, they shall be forwarded to the requesting office by the Office of Safeguards and Security together with the DP-1, SF-85, or SF-86.
13. TYPES OF INVESTIGATIONS.
- a. Federal Bureau of Investigation.

- (1) Background Investigation covers the individual's adult life since his or her 18th birthday. It includes contacting personal references provided by the individual, information on the individual's present and past residences and employment, and a record of the person's education. All military service records shall be checked. All information will be obtained from places of education attended (not below high school); from police departments and credit bureaus at all places of residence and employment during the most recent 15 years or since the individual's 18th birthday; from embassies for all periods of overseas residence (plus State Department investigation if possible), and from the Bureau of Vital Statistics if inconsistencies develop regarding the individual's name or date and place of birth. A name check shall be conducted with the FBI's criminal and subversive files, the OPM Security Investigations Index, Defense Central Index of Investigations (DCII), and for foreign-born individuals or spouses, the Central Intelligence Agency (CIA) and Immigration and Naturalization Service (INS). The CIA also shall be checked if extensive foreign travel has been indicated. A fingerprint check is also conducted.
- (2) File and Fingerprint Check consists of fingerprint card classification through the FBI's Identification Division, along with a corresponding name check through the FBI's criminal and subversive files.

b. Office of Personnel Management.

- (1) National Agency Check with Credit consists of a records check of the individual's name with the FBI's criminal and subversive files, OPM's Security Investigations Index, DCII, INS (whenever U.S. citizenship by other than birth is indicated), and the CIA (whenever extensive foreign travel is indicated). In addition, fingerprint check shall be made through the FBI's Identification Division, and a credit check conducted.
- (2) National Agency Check and Inquiry with Credit includes the checks conducted for a National Agency Check with Credit plus written inquiries sent to the individual's supervisors at places of employment during the most recent 5 years, police departments having jurisdiction over the individual's residences during the most recent 5 years, all places of education where the individual received a degree relating to the position applied for, all places of education during the most recent 5 years, and listed references. A credit check is also conducted.

- (3) Minimum Background Investigation (MBI) consists of the National Agency Check and Inquiry described above and a credit search. In addition, to ensure adequate coverage, telephone inquiries are made whenever the initial written inquiries are not returned.
 - (4) Limited Background Investigation (LBI) consists of a National Agency Check with Credit plus personal interviews with selected sources covering specific areas of the subject's background during the most recent 1 to 3 years, and written inquiries and record searches for a total of 5 years.
 - (5) Background Investigation (BI) consists of a National Agency Check with Credit plus written inquiries, record searches, credit search, and personal interviews with selected sources covering specific areas of the subject's background up to the past 7 years, but for not less than 5 years.
 - (6) Special Background Investigation (SBI) consists of a National Agency Check with Credit plus written inquiries, record searches, credit search, and personal interviews with selected sources covering specific areas of the subject's background during the most recent 15 years.
- c. Background Investigations by Other Federal Agencies. Reports of personnel security investigations by other Federal agencies may be accepted in lieu of reports by the OPM provided that (1) the investigation meets the scope and extent of the OPM investigation; (2) a security clearance has been granted by another Federal agency based on such investigation and report; and (3) the investigation was conducted within the last 10 years and has been updated within the last 5 years with a minimum of a National Agency Check.
- d. Incomplete National Agency Checks. To expedite the processing of Secret, L, and LX access authorizations, the Department accepts National Agency Checks from OPM which are incomplete, provided the missing checks are clearly identified. The OPM has been advised that FBI and OPM checks must be completed prior to submission to DOE. Upon receipt of incomplete National Agency Checks, managers of field elements may, when the situation so requires, grant Secret, L, or LX access authorization, provided that as a minimum:
- (1) A review of the SF-86 or other security forms and the checks received is favorable.
 - (2) The individual and his or her employer or prospective employer furnish satisfactory evidence indicating that no adverse circumstances of a security nature surrounded the individual's

military service, employment, or foreign travel. Submission by the individual of his or her discharge papers or passport, either directly to DOE, current employer, or prospective employer will ordinarily suffice for this purpose.

- (3) Documentation of the incomplete information is recorded in the case file.
 - (4) A further review of the case shall be made when the missing checks are received.
- e. Requests for Full Field Investigation When National Agency Checks Reveal Derogatory Information. When the National Agency Check discloses substantially derogatory information in relation to the DOE access authorization criteria, the manager of the operations office has the option of conducting an interview, arranging for psychiatric evaluation, or submitting a request for a full field investigation to the Office of Personnel Management. If a full field investigation is requested it should be transmitted with a letter setting forth the reasons for the request, accompanied by two copies of an up-to-date SF-86; and a new SF-87 if more than 6 months has elapsed since the request for National Agency Check was forwarded to the OPM.

14. REQUESTING FBI INVESTIGATION FOR INDIVIDUALS TRANSFERRED TO POSITIONS OF A HIGH DEGREE OF IMPORTANCE OR SENSITIVITY.

- a. When an individual whose access authorization was based on an investigation conducted by the OPM or another Government agency that conducts personnel security investigations is being transferred to a position certified by the Department as a position of a high degree of importance or sensitivity (see Chapter I), a request for a full field investigation shall be forwarded to the FBI by the field element. If the individual has been the subject of an OPM full field investigation within the past 3 years, the manager may authorize the transfer to the new position, provided the existing personnel security file is reviewed by a personnel security specialist before the transfer takes place, and this review has not revealed any unresolved derogatory information. In such cases, the individual shall be processed for an FBI reinvestigation when the existing investigation is 5 years old. The manager of the operations office may also authorize the transfer to the new position prior to receipt of a completed FBI full field investigation, provided the existing personnel security file is reviewed before the transfer takes place and there is no security objection to such action.
- b. In requesting this investigation, the FBI will be furnished with the following:
 - (1) An original plus one copy of an up-to-date SF-86 which shall indicate that the position is of a high degree of importance or sensitivity;

- (2) A new fingerprint card; and
 - (3) One copy of each of the reports of the previous investigation conducted by OPM or another Federal agency.
15. REQUESTING EXPEDITED INVESTIGATIONS. In instances where there is an emergency or critical need for the immediate services of an individual being processed for a full field investigation, the investigative agency can be requested to conduct the investigation on an expedited basis. The following procedures shall be followed in such cases:
- a. The field office requesting the expedited service on an FBI investigation shall forward a memorandum to the Chief of the Policy and Administrative Review Branch (DP-344.1). The memorandum must indicate the name, DOE file number, number and date the investigation was requested, as well as justification for the expedited service. The Chief of the Policy and Administrative Review Branch shall review the request for expedited service, and if approved, shall make the necessary arrangements with the FBI.
 - b. When expedited service on an OPM investigation is required, the field element shall forward a cover memorandum to OPM requesting such service. That memorandum should be included in the request package with the SF-86.
 - c. All copies of the paperwork being submitted to the investigative agency shall be stamped "EXPEDITE" at the time they are forwarded to OPM or the FBI.
16. DOCUMENTATION REQUIRED IN GRANTING ACCESS AUTHORIZATIONS.
- a. When access authorization has been granted, the field element shall make the appropriate entry into the Central Personnel Clearance Index, onto the File Summary Sheet in the individual's Personnel Security File, and shall also notify the requesting office.
 - b. DOE F 5631.12, "Process Index Cards," may be used to provide an alphabetical index of all individuals processed for access authorization.
17. REOPENING OF CASES IN WHICH REQUESTS FOR ACCESS AUTHORIZATION WERE CANCELLED.
- a. Full Field Investigations.

- (1) When a full field investigation which was discontinued prior to completion is again required, the field element shall request a reopening of the investigation by forwarding the SF-86 to the appropriate agency. The SF-86 should be marked "Reopen Case" and the date of the previous request and cancellation should be indicated. The extent of reports previously received (e.g., NAC only, partial full field reports) will aid the investigative agency in rescheduling the case.
 - (2) When the request for access authorization has been canceled (e.g., employee not hired, or does not require access authorization) after the completion of the investigation and updating of the investigation is deemed necessary, the procedure outlined in subparagraph 17a(1) of this chapter shall be followed.
 - (3) If more than a year has elapsed or any significant changes are known to have occurred since the execution of the previous SF-86, a new form and fingerprint cards must be submitted.
- b. Copies. If the original investigation was not made by the same investigative agency, one copy of each report of the previous investigation and new security forms shall be forwarded with the request.
- c. Reopening of Reinvestigations Previously Conducted. When a reinvestigation which was discontinued prior to completion is again required, field elements shall request such action by forwarding a SF-86, with the appropriate entry on Part 1 of the form, to the FBI or OPM.

18. DEPARTMENTAL CUSTODY OF INVESTIGATIVE REPORTS.

- a. Because of the privileged nature of the information contained in the investigative reports and the personnel security files, they shall be made available within DOE only to Departmental employees who are conducting, processing, or adjudicating an investigation on the individual for security clearance or access authorization, suitability for Federal employment, a criminal violation, or to ensure compliance with Departmental regulations. Appropriate measures will be taken for their handling, transmission, and housing to assure that this requirement is carried out. Reports or information contained therein shall not be made available to contractors' representatives.
- b. Availability of Investigative Reports. Reports of investigation on individuals who have been processed for DOE access authorization may be

shown to representatives of agencies or other entities identified as routine users as described in DOE system of Records-43, "Personnel Security Files," provided such representatives show that they have an official interest in the information contained in the reports. Unless the Office of General Counsel approves another use or action, the following restrictions will apply to the availability and use of investigative reports. Representatives shall not be given copies of the reports but shall be advised that reports may be requested directly from the FBI, OPM, or other Federal investigative agency that originated the report. Representatives may also review copies of security interviews and hearing transcripts, but only if the subject of the investigation has given written authorization for the release of the transcripts. The release executed by the individual must explicitly refer to the interview and/or hearing transcript or summary contained in the DOE personnel security file. A copy of the release and a listing of the material released shall be maintained in the individual's DOE personnel security file. In addition, the procedures in the following paragraphs must be adhered to by DOE security officials.

- c. In accordance with Public Law 93-579, 5 U.S.C. section 552a, Privacy Act of 1974, an accounting shall be maintained of each disclosure of the contents of a DOE personnel security file to any other agency representative or other individual as described in paragraph 19b above, to review the investigative reports, copies of security interviews, and hearing transcripts. Prior to the physical review of the personnel security file, the following information shall be noted in the file:
 - (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 Departmental employee releasing the information.
- d. Pursuant to the Privacy Act, 5 U.S.C section 552a(b)(7), information may be released to "another agency or 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 been 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."
- e. Prior to the release of personnel security files containing classified information, the DOE employee responsible for releasing the file shall

be assured that the reviewer possesses the appropriate level of access authorization or clearance, and has an official need-to-know.

19. RELEASE OF CONTENTS OF PERSONNEL SECURITY FILES.

- a. Background investigations shall not be released to any individual while the investigation or adjudication of eligibility for access authorization is pending. On completion of the security review process, resulting in a final determination to grant or deny access authorization, a request for the background investigation by the individual may be granted.
- b. Exemptions under 5 U.S.C. 552a(k)(2) and (k)(5) provide a basis for withholding this information until the security review process is completed, and the individual's due process rights are protected because disclosure of all probative derogatory information is made prior to the security review hearing.
- c. Disclosure of information in the background investigation to other officers and employees of the Department who need the records to perform their duties is permitted by Title 5 U.S.C. 552a(b)(1) of the Privacy Act. A psychiatrist conducting an evaluation at the request of DOE may be permitted access to the information contained in the background investigations in accordance with DOE 1800.1A.
- d. Upon receipt of an individual's request for disclosure of his/her background investigation, the Department will advise the individual that the request must be made to the FBI, OPM or other investigating agency conducting the background investigation. The investigating agency will determine if the information will be disclosed.

20. NOTIFICATION OF ACCESS AUTHORIZATION DETERMINATION. The Department's determination to grant or deny access authorization shall be furnished in writing, or orally with written confirmation, to the employer, prospective employer, or access permittee who initiated the request. This information may also be furnished to representatives of DOE contractors, representatives of the Armed Forces, or other Federal agencies having an official interest in the individual. Determinations to grant access authorization shall not be given in writing to the individual except:

- a. In cases in which the determination was made as a result of a completion of the DOE administrative review process as specified in 10 CFR 710.
- b. When the individual is also the designated official in the agency, firm, or organization to whom written notifications are forwarded.
- c. When a favorable determination has been made following a security interview and the individual is furnished a Security Advisory Letter.

21. CONTENTS OF AND ARRANGEMENT OF DATA IN PERSONNEL SECURITY FILES. The personnel security file (PSF) of any individual who is being or has been processed for DOE access authorization, whether active or terminated, shall contain the original or a copy of any document related to an investigation, including an investigative report prepared by a Federal investigative agency prior to the granting of access authorization, or any documents, correspondence, or forms involving the individual subsequent to the initial clearance action. The PSF shall be arranged so that administrative material is fastened to the left side, and adjudicative material shall be fastened to the right side. Material on each side of the folder shall be arranged in chronological order, from bottom to top, except as noted below.
- a. Administrative material includes memoranda and other correspondence relating to the administrative handling of the case. This includes requests for clearances; prescreening forms, notes to the file (except notes containing investigative or adjudicative data); requests to other offices for interviews; security advisory letters; suspension correspondence, notification letters, and responses thereto; special authorizations for sensitive or compartmented information including Top Secret production, stockpile and weapons data; security badge and briefing forms; and similar data. A File Summary Sheet (DOE Form 5631.16 or equivalent) shall be placed on the top of all other material on the left side of the PSF.
 - b. Adjudicative material includes all investigative material relating to determining eligibility for access authorization. This includes the DP-1; SF-85; SF-86; SF-87; FD-258; FBI Forms T-1, 1-C, T-2, I-4 or other identification records; Security Acknowledgement forms; reports of investigation from any Government agency or local law enforcement activity, the Office of the Inspector General, or contractor security personnel; letters, memorandums or notes to file containing investigative data; summaries of investigation; reports of hospitalization or treatment for mental illness, alcoholism, or other substance abuse; interview transcripts or summaries; DOE Forms 5631.5 through 5631.10, as appropriate; release forms signed by the subject of the PSF; letters of interrogatory to the individual and responses thereto; requests for psychiatric and/or psychological evaluations and responses thereto; case evaluations; and any other material relating to the adjudication of the individual's eligibility for a DOE access authorization.

FORMS REQUIRED FOR SECURITY INVESTIGATIONS

Position	Access Type	SF-86, (original plus 2 copies) and Security Acknowledgement DOE 5631.18 (1 original)	Fingerprint Cards 2 originals FD-258 SF-87	SF-171 (1 copy)
DOE employees and consultants, other Government agency employees, and Congressional and judicial staff members	Q Sensitive	X	X	X
	Q Nonsensitive, Top Secret, L, and Secret	X	X	X
DOE contractor employees and consultants, and employees of access permit holders	Q Sensitive, Q Nonsensitive, Top Secret, L, and Secret	X	X	

ADDITIONAL INFORMATION TO BE OBTAINED FOR INVESTIGATION OF NATURALIZED U.S.
CITIZENS OR INDIVIDUALS WHO HAVE RESIDED IN FOREIGN COUNTRIES

1. EMPLOYMENT. The names and addresses of individuals living in the United States who were associated with the applicant in the foreign country as supervisor, employee, or fellow worker.
2. RESIDENCE. The names and addresses of individuals living in this country and abroad who were neighbors of the applicant during residence abroad.
3. REFERENCES. The names and addresses of individuals living in this country who were closely associated with the applicant and who can verify the applicant's addresses, employment, and activities in the foreign country.
4. ADDRESSES. The names, addresses, and occupations of nonrelatives with whom the applicant has resided in a foreign country.
5. RELATIVES. The occupations and the full names of all relatives listed on the SF-86 and any other relatives residing in Communist-controlled countries or countries that are hostile to the United States. If a relative is employed by a foreign government, secure the details. Ascertain the degree and frequency of contact with these relatives.
6. CORRESPONDENCE. The names, addresses, and occupations of individuals (other than relatives covered in item 5 above) residing outside the U.S. with whom the applicant corresponds, and the nature of the correspondence.
7. ORGANIZATIONS. The applicant's membership in all foreign organizations except religious, including the date of membership and offices held. Include description of the nature and purpose of the organization and the applicant's reason for joining, where appropriate.
8. FINANCIAL INTERESTS. Whether the individual holds any financial or other obligations or interests in foreign countries. If so, such interests should be fully explained.
9. PASSPORTS. Whether the individual has a valid, active passport issued by a government other than the United States. If so, the following data should be provided:
 - a. The issuing country(ies), date of issue, and if applicable, the date renewed.
 - b. Whether more than one individual is listed on the passport(s).

- c. The reason the passport(s) was obtained, how often has it been used, and for travel to which country(ies).
 - d. Whether the application, renewal, or use of the passport require the individual to swear an oath of allegiance to another country.
 - e. Whether the individual is willing to relinquish the passport(s) and submit evidence of such relinquishment to DOE.
 - f. Whether the individual can offer assurance that he/she will not apply for another country passport while employed in a position requiring a DOE access authorization.
10. DUAL CITIZENSHIP. In order to determine whether the applicant is a dual citizen, and, if so, what actions (if any) the applicant will take to divest himself/herself of such ties to a foreign entity or government the following information is to be obtained from the individual.
- a. Whether the individual considers himself/herself to be a dual citizen. If so, the countries of citizenship should be listed.
 - b. For the purpose of being processed for a DOE access authorization, it should be determined whether the individual is willing to formally renounce the other country citizenship and submit evidence of such renouncement to DOE. If not, the reasons therefor should be given.

CHAPTER III

SCREENING AND ANALYSIS OF PERSONNEL SECURITY CASES AND METHODS FOR
DETERMINING ACCESS AUTHORIZATION ELIGIBILITY

1. SCREENING. Upon receipt of completed full field investigations, National Agency Checks and Inquiries with Credit, or National Agency Checks with Credit, the individual assigned the function of screening will check the investigative reports to ensure that the items listed on the SF-86, or other related forms have been covered and that the required DOE scope of investigation for the particular type of clearance has been met.
 - a. Full Field (Background) Investigations.
 - (1) Places of residence, employment, education, military service, and so forth, are checked to ascertain that they have in fact been adequately covered by the investigation.
 - (2) All items of derogatory information and mitigating information should be listed in writing and documented with date and signature of the reviewer.
 - (3) Those cases in which the investigation is complete and no derogatory information has been reported are appropriately documented. If the individual assigned to this function has been delegated authority in writing to grant access authorization, the authorization shall be so noted in the file. However, at least 5 percent of such cases shall be reviewed by a senior security analyst to ensure that the investigation is in fact complete and that derogatory information is not present. Notification of access authorization for cases under review shall not be sent until the review verifies that the investigation is complete and no derogatory information is present. Such verification is documented by the date and signature of the reviewing official on the DOE F 5631.16, "File Summary Sheet."
 - (4) When the DOE F 5631.16 is completed and signed and the reports of investigation, DP-1, SF-85 or SF-86, and related documents are properly arranged in the file folder, the case shall be forwarded to designated personnel for further processing.
 - b. National Agency Checks With Credit and National Agency Checks And Inquiries With Credit: Individuals screening and analyzing these checks must determine whether all items as stated in Chapter II, paragraph 14b, are covered. Derogatory and mitigating information should be listed and documented with the date and signature of the reviewer.

2. ANALYSIS.

- a. Analysis of reports of investigation is performed to evaluate the reported information, favorable and unfavorable, in relation to the "Criteria and Procedures for Determining Eligibility for Access to Classified Matter and Significant Quantities of Special Nuclear Material," (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 question, but it may be offset when considered with other reported mitigating information. Therefore, the analysis of personnel security cases shall not be performed as a mechanical or routine function, but rather as one of the most important aspects of the overall personnel security program.
- b. If the investigation is complete in all respects and reported derogatory information is clearly outside the scope of the Criteria, the manager of the field element, or the individual who has been delegated this authority in writing, may grant access authorization:
 - (1) On the existing record; or
 - (2) After additional investigation, psychiatric evaluation, or an interview which extends or further clarifies the reported information.
- c. In cases in which the reported information falls within one or more of the categories in the Criteria and the case cannot be resolved locally, the manager of the operations office shall forward to DP-34, a duplicate of the personnel security file, together with a summary statement and a recommendation for a method to be employed in resolving the question of the individual's eligibility for access authorization.

3. REFERRAL OF CASES FOR REVIEW AND ADVICE. Managers of operations offices are not precluded from referring any case to the Director of Safeguards and Security for review and advice. However, any case that is 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 has been delegated the responsibility of reviewing all cases referred under 10 CFR 710.10 for determination of the method by which the question of eligibility for access authorization will be resolved. DP-34 may:

- a. Authorize the granting of access authorization based on the existing records or after receipt of additional investigation.

- b. Determine that the question of eligibility cannot be resolved by additional investigation, psychiatric evaluation, or interview, in which case the initiation of the Department's administrative review procedures (10 CFR 710.22, et seq.) is authorized.
5. INTERVIEWS. Because the Criteria limits the use of the hearing procedure to cases in which questions of eligibility cannot be favorably resolved by interview, psychiatric evaluation, or additional investigation, conducting interviews becomes a very important function of a personnel security official.
 - a. If it has been determined that an interview is necessary, it shall be conducted by a personnel security specialist who is cognizant of all the questions or items of information to be explored.
 - b. All interviews shall be recorded. The interview may then be transcribed or summarized. In cases where a transcript is not prepared, the recorded interview must be retained and protected in the same manner as a Personnel Security File.
6. SECURITY ADVISORY LETTERS. When questions concerning an individual's initial or continued eligibility for a DOE access authorization have been favorably resolved through a security interview with the individual, the individual shall be so informed by means of a security advisory letter signed by the manager of the operations office, or in Headquarters cases, the Director of Safeguards and Security. The security advisory letter shall be sent to the individual only after the individual has been granted a DOE access authorization or a decision has been made to continue the individual's current DOE access authorization. A copy of the letter shall be placed in the individual's personnel security file with an acknowledgment of the receipt of the letter manifested by his or her signature. The purpose of the letter, which may be delivered directly or sent to the individual, is to advise the individual and state for the record that:
 - a. A security interview was conducted with the individual at a specific time, date, and place by a DOE security official.
 - b. The interview was conducted in order to outline to the individual the nature of the circumstances or activity which caused a security concern and to permit the individual an opportunity to provide specific information in response to these concerns. The nature of the circumstances or activity shall be outlined as follows:
 - (1) The date, time, and place of the proscribed circumstances or conduct (if applicable) shall be indicated;

- (2) A specific provision of 10 CFR 710.11 shall be cited; and
 - (3) The nature of the improper action shall be outlined.
- c. The information provided by the individual in response to the investigative material presented has been reviewed and evaluated by DOE security officials and a determination made that further processing under 10 CFR 710.20, et. seq., is not warranted at this time.
 - d. Should the individual continue to be involved in the derogatory activity that prompted the interview, within the meaning of 10 CFR 710.11, while still employed in a position requiring a DOE access authorization, a question could be raised concerning the individual's continued eligibility for a DOE access authorization. (The contents of this paragraph shall be included in the letter only if appropriate. For example, such a reference will not be appropriate if an individual was interviewed concerning relatives residing in a Communist bloc country.)
 - e. A security advisory letter will not be provided to the individual if it is established during the personnel security interview that the information that raised a security concern is totally without merit. For example, if derogatory financial information is provided and it is determined that the information is erroneous, then a security advisory letter need not be sent to the individual. The individual's Personnel Security File shall, however, be noted to reflect that the derogatory information that was reported has been totally mitigated or resolved.
7. INTERROGATORIES. As an alternative to an interview, a letter of interrogatory may be sent to the individual provided the information required is not of a serious nature (e.g., an unlisted relative), or the geographic location of the subject would make it extremely difficult to arrange for a personal interview. The individual's response to the interrogatory will be reviewed and evaluated to assure that any security concern that caused the letter to be written is resolved. If it is determined that the individual's response does not favorably resolve the security concern, a personnel security interview will be scheduled with the individual in order to further explore the concern.
 8. ADDITIONAL INVESTIGATIONS. When an additional investigation is required to expand, resolve, or corroborate information, the field element can submit the request directly to the local OPM or FBI supervisory investigator.
 9. SPECIAL UPDATES. In cases in which the investigation was completed by OPM within the most recent 18 months, OPM shall conduct a special update full field investigation at a reduced rate of charge. Such requests should be transmitted to OPM with an indication on the SF-86 that the case is a special update.

10. DRUG CERTIFICATIONS. In the event that there is information indicating that the individual has illegally used or trafficked in a controlled substance as defined in section 202 of the Controlled Substances Act of 1970 (21 U.S.C. section 812), a security interview will be conducted to determine the extent and duration of such drug involvement and the individual's future intentions. 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 prohibited use of or involvement with controlled substances. If, after being granted a DOE access authorization (or having a DOE access authorization continued), the individual who signed a Drug Certificate violates the terms of the certificate, an immediate evaluation of the circumstances of such violation shall be conducted, and the individual's continued eligibility for a DOE access authorization shall be determined under the procedures stipulated in the provisions of 10 CFR 710.
11. ADMINISTRATIVE REVIEW PROCEDURES. In cases where the reported derogatory information is not favorably resolved through an interview, a psychiatric evaluation, or an additional investigation, the Director of Safeguards and Security shall authorize proceedings in accordance with procedures set forth in 10 CFR 710.
12. PERSONS TREATED FOR MENTAL ILLNESS OR MENTAL CONDITIONS. To assist in determining whether reported information involving mental illness or conditions falls within the Criteria, the following guidelines are provided:
 - a. When a DOE or DOE contractor employee or consultant possessing DOE access authorization is hospitalized or otherwise treated for a mental illness or mental condition which may cause a significant defect in judgment or reliability, the DOE supervisor or a responsible official of a DOE contractor shall report this information to the manager of the cognizant field office, or, for Headquarters cases, the Director of Safeguards and Security, DP-34. Upon determination by the employer that the employee or consultant is able to perform his/her regular duties, the individual's access to classified information may be continued unless the manager of the field office determines that there is meaningful evidence that there may be a significant defect in such individual's judgment or reliability within the meaning of 10 CFR 710.11(h), in which case the procedures outlined in subparagraph 12c below shall be followed.
 - b. As an aid in determining the individual's judgment or reliability, the manager may accept previously rendered competent medical advice or records that are in possession of DOE or a DOE contractor. The manager may also have a psychiatric examination conducted by a qualified

physician designated by the Department. In such a case, the individual shall be requested to submit to an examination and to execute a consent form, DOE F 5631.10, "Waiver," for the examination.

- (1) The psychiatrist shall submit a written report of his or her professional opinion to the manager of the operations office on whether the individual suffers from a mental illness or condition which causes or may cause a significant defect in the individual's judgment or reliability.
 - (2) If the individual refuses to submit to an examination, the manager of the operations office shall refer the case to the Director of Safeguards and Security.
- c. If the manager finds that there may be a significant defect in the reliability or judgment of the individual, the manager shall determine whether the individual's access authorization should be suspended pending the administrative review procedure. The access authorization of an individual shall not be suspended except by direction of the manager of the operations office.
- d. If a psychiatric examination is conducted as described in paragraph 12b above, the psychiatrist who is to examine the individual on behalf of DOE shall be notified that he or she may be called upon to testify as a witness in a hearing before a Hearing Officer if such a hearing is held. Only physicians consenting to testify should be designated for examining purposes. The examining physician shall not be appointed as a Hearing Officer or as a Personnel Security Review Examiner in the instant case.
13. DISCLOSURE OF REPORTED INFORMATION. Following notification to an individual of the opportunity to request a hearing before a Hearing Officer, the contractor or prospective contractor may, upon inquiry, be informed of the status of the case but not of the information requiring its referral to a Hearing Officer.
14. TIME ELEMENT IN PROCESSING CASES. The following time schedules (working days) shall be observed in processing cases:
- a. Initial screening and notification of the granting of access authorization shall be accomplished within 7 days of the receipt of completed investigations which have been evaluated and found not to contain derogatory information.
 - b. Within 30 days of the receipt of a completed investigation, one of the following actions shall be taken:

- (1) Access authorization shall be granted;
 - (2) Additional investigation shall be requested;
 - (3) An interview with the individual shall be scheduled;
 - (4) A letter of interrogatory shall be sent to the individual; or
 - (5) The case shall be referred to the Director of Safeguards and Security as containing substantially derogatory information.
- c. After a field element or Headquarters requests approval to proceed with Administrative Review processing, the following timeframes should be used as a guide in the various processing steps:
- (1) The Office of Safeguards and Security shall render a determination on the request for the initiation of Administrative Review proceedings within 30 days.
 - (2) After the receipt of the Office of Safeguards and Security response, the field element shall prepare and deliver a notification letter to the individual within 30 days of its receipt of the case.
 - (3) The individual is responsible for responding to the notification letter within 20 days of receipt of the letter.
 - (4) Should the individual fail to respond to the notification letter within 20 days, the individual shall be recontacted within 3 days to determine whether he or she intends to avail himself or herself of the right to a DOE Personnel Security Hearing. Unsuccessful attempts to locate an individual who has failed to respond should be documented and the case should then be forwarded to the Director, Office of Safeguards and Security, for transmittal to DP-1.
 - (5) A hearing before a DOE Hearing Officer shall be held within 90 days of the receipt of individual's request for a hearing.
 - (6) The court reporter shall return the transcript of the hearing to the appropriate DOE office within 20 days of the completion of the hearing or closing of the record.
 - (7) Within 5 days of its receipt of the completed hearing transcript, the field office shall transmit it to the Hearing Officer.

- (8) The Hearing Officer should return a written statement of findings and recommendations to the field element Manager within 30 days of receipt of the hearing transcript.
- (9) The field element Manager shall review and transmit the Hearing Officer's findings and recommendations to the Director of Safeguards and Security within 10 days of receipt of the Hearing Officer's report, unless the report must be returned to the Hearing Officer for correction.
- (10) The Office of Safeguards and Security shall forward a letter to the individual within 5 days of receipt of an adverse recommendation from the Hearing Officer.
- (11) The individual has 5 days from receipt of the letter described in paragraph (10) above to request a review by the Personnel Security Review Examiners and 10 days to submit a brief, unless an extension has been granted by the Director of Safeguards and Security.
- (12) The Office of Safeguards and Security shall forward the case to the Personnel Security Review Examiners within 5 days of receipt of the individual's request for such a review or receipt of the individual's brief.
- (13) The Personnel Security Review Examiners shall return a recommendation to the Office of Safeguards and Security for transmittal to DP-1 within 45 days of receipt of the case.
- (14) The Office of Safeguards and Security shall prepare and type a consolidation package within 45 days of the receipt of all 3 Personnel Security Review Examiner reports.
- (15) General Counsel shall review and comment on the legal sufficiency of the case within 20 days of receipt of the case from the Office of Safeguards and Security.
- (16) The Director of the Personnel Assurance Division, Office of Safeguards and Security shall concur in recommended action within 5 days of receipt of the case from General Counsel.
- (17) The Director of the Office of Safeguards and Security shall concur in recommended action within 5 days of receipt of the case from the Director of the Personnel Assurance Division.

- (18) The Deputy Assistant Secretary for Security Affairs (DP-30) shall concur in the case within 5 days of receipt from the Director of the Office of Safeguards and Security.
- (19) The Assistant Secretary for Defense Programs shall make a final determination within 10 days of receipt of the case from the Deputy Assistant Secretary for Security Affairs.

15. REFERRAL FOR SUITABILITY DETERMINATION.

- a. DOE Applicants for Employment, Employees, and Consultants. In all such cases, the reports of investigation received by the Office of Safeguards and Security will first be reviewed by the servicing personnel office. The servicing personnel office must notify DOE personnel security within 30 days if action will be taken against the individual. Unless DOE security officials consider it necessary for reasons of security to proceed with the security clearance determination (for example, an employee continues to have access to classified information or special nuclear material), a determination will be rendered as to the individual's initial or continued eligibility for Federal employment prior to determining the individual's eligibility for DOE security clearance.
- b. Other Federal Agency or Department Employees and Consultants. In cases where employment suitability information is developed, the reports of investigation will first be reviewed by the appropriate Federal agency or department official. The other agency/department official must notify DOE personnel security within 30 days if action will be taken against the individual. Unless DOE security officials consider it necessary for reasons of security to proceed with the security clearance determination (for example, an employee continues to have access to classified information or special nuclear material), a determination will be rendered as to the individual's initial or continued eligibility for Federal employment prior to determining the individual's eligibility for DOE security clearance.

CHAPTER IV

INTERIM ACCESS AUTHORIZATIONS AND WAIVERS OF PREAPPOINTMENT
FULL FIELD INVESTIGATIONS

1. GENERAL. Only under exceptional circumstances and when such action is clearly consistent with the national interest will an individual be permitted to have access to classified matter or will a DOE employee be allowed to occupy a critical-sensitive position prior to completion of the appropriate investigation. In all cases, interim access authorization to either Restricted Data or National Security Information or waivers of preappointment full field investigations shall be considered temporary measures, pending completion of investigation which must be in process. Interim access authorization to Restricted Data shall be approved only by the Assistant Secretary for Defense Programs, and interim access to National Security Information and waivers of preappointment full field investigations shall be approved only by the Secretary. Requests for interim access authorization shall be made only in cases where access to Restricted Data requires the individual to have a Q access authorization or when access to National Security Information requires a Top Secret access authorization. Employees, access permit holders, or individuals whose access requires L or Secret access authorizations shall not be processed for interim access authorizations.
2. INTERIM ACCESS AUTHORIZATION TO RESTRICTED DATA OR SPECIAL NUCLEAR MATERIAL.
 - a. A written request for Interim Access Authorization, will be submitted directly to DP-34, and must be supported by a certification that:
 - (1) Serious delay or interference to an operation or project essential to a DOE program may be experienced unless the named individual is granted access to Restricted Data prior to completion of the authorization procedures; and
 - (2) The services of a qualified person previously cleared or authorized access by DOE cannot be obtained.
 - b. If a full field investigation has not been requested prior to the request for interim access to Restricted Data, this request, accompanied by the forms required for the level of access authorization requested (see Chapter II), must be made concurrently with the submission of the request for Interim Access Authorization.
 - c. Upon receipt of the Request for Interim Access Authorization and the appropriate DOE security forms, DP-34 shall review the security forms and conduct other agency indices checks as appropriate. If any DOE or other agency security file exists and is available for review, a review shall be conducted by DP-34 prior to further processing. Once indices checks and

file reviews have been completed, DP-34 shall prepare a DOE F 5631.32 ("Request for Interim Access Authorization") for the signature of the Assistant Secretary for Defense Programs. DP-34 shall provide an appropriate security recommendation as to whether the interim access authorization should be granted. Once a determination has been rendered, the DOE F 5631.32 will be returned to DP-34 who will notify the requestor of the determination and any security stipulations connected with the granting of the interim access authorization.

3. INTERIM ACCESS AUTHORIZATION TO NATIONAL SECURITY INFORMATION OR FORMERLY RESTRICTED DATA. A request for interim access authorization to National Security Information or Formerly Restricted Data may be submitted for consideration when such access is required to meet a critical need prior to completion of the clearance process. The authority to approve such interim access rests with the Secretary.
 - a. Interim access authorization to National Security Information or Formerly Restricted Data may be requested when:
 - (1) A review of past employment and results of reference checks indicate that the possibility of derogatory information being developed by a full field investigation is remote; and
 - (2) The need to have the individual commence work involving National Security Information or Formerly Restricted Data is clearly urgent and in the national interest.
 - b. In cases involving Headquarters, the head of the first tier organization, or his or her deputy, or for individuals employed at field elements, the manager of the operations office, or his or her deputy, must certify to the above conditions. This authority may not be redelegated. If there is a reporting relationship to a line official at Headquarters, that official must also certify that the conditions are met.
 - c. The head of the major first tier organization, or his or her deputy, or for individuals employed at field elements, the manager of the operations office, or his or her deputy, shall prepare and forward a memorandum to the appropriate Headquarters official, if any, for certification and submission to the Director of Personnel (MA-20). All requests must be submitted to MA-20 at least 20 working days prior to the proposed start of duty for new DOE employees, or the proposed effective date of reassignment for current DOE employees. MA-20 will arrange for appropriate reviews with DP-34 and the Assistant Secretary, Management and Administration, and for Secretarial action.
4. WAIVER OF PREAPPOINTMENT FULL FIELD INVESTIGATION. DOE shall process requests for waivers of preappointment full field investigations in accordance with the procedures established in Chapter 736 of the Federal Personnel Manual (FPM).

Waiver of the preappointment investigation requirement on persons entering sensitive positions may only be made in case of an emergency, provided that the head of the department or agency concerned finds that such action is necessary in the national interest, which finding shall be made a part of the records of such department or agency. This general restriction is applicable only to critical-sensitive positions, because DOE will not process waivers for noncritical-sensitive positions. Waiver of the preappointment investigation requirement may not be made in special-sensitive positions. Guidelines for determining position sensitivity are contained in FPM Chapter 731, Subchapter 2, "Position Sensitivity."

- a. Waiver of preappointment investigation may be requested for an individual selected for a critical-sensitive position when:
 - (1) A review of past employment and results of reference checks indicate that the possibility of derogatory information being found by a full field investigation is remote.
 - (2) Meaningful work for the organization can be carried out by the individual without access to classified information, or when the individual is already a DOE employee who has a security clearance, in which case access may be continued.
 - (3) The need to have the individual commence work as soon as possible because of the national interest and in clear emergency.
- b. In Headquarters cases, the head of the first tier organization, or his or her deputy, or for individuals employed at field organizations, the manager of the operations office, or his or her deputy, must certify to the above conditions. This authority may not be redelegated. If there is reporting relationship to a line official at Headquarters, that official must also certify that the conditions are met.
- c. The head of the first tier organization, or his or her deputy, or for individuals employed at field elements, the Head of the Field Element, or his or her deputy, will prepare and forward a memorandum to the appropriate Headquarters line official, if any, for certification and submission to Director of Personnel. All requests must be submitted to the MA-20 at least 20 working days prior to the proposed start of duty for new DOE employees, or the proposed effective date of reassignment for current DOE employees. MA-20 will arrange for appropriate reviews with DP-34, MA-1, and for Secretarial action.
- d. Waivers of preappointment National Agency Checks and Inquiries With Credit, Limited Background Investigations, or Special Background Investigations will not be processed.

5. STANDARDS AND PROCEDURES.

- a. The Office of Safeguards and Security will ensure that the following checks have been made, without disclosing substantially derogatory information, prior to certifying security approval of interim access authorizations or waivers of preappointment full field investigations:
- (1) Form SF-86 signed by the individual has been reviewed;
 - (2) DOE files and DOE contractor files have been checked, including the results of preemployment inquiries;
 - (3) FBI file and fingerprint check have been requested;
 - (4) The OPM Security Investigations Index has been checked;
 - (5) A full field investigation has been requested;
 - (6) Records from the individual's most recent employer have been checked;
 - (7) For current or former Federal employees, the security files at the former agency have been checked; and
 - (8) The individual has been interviewed regarding any derogatory information that has been found.
- b. Requests for central FBI file and fingerprint checks and full field investigations for these cases shall be initiated by forwarding the following:
- (1) SF-86 and SF-87 or FD-258, with a special letter requesting full field investigation. In addition, the special marking "Interim Access Authorization" is stamped on:
 - (a) All copies of the SF-86;
 - (b) SF-87 or FD-258;
 - (c) The request for investigation letter; and
 - (d) The transmittal jacket or envelope.
 - (2) The special letter to OPM or the FBI, as appropriate, shall request that a central FBI file check be made and the results furnished to the Department as quickly as possible.

CHAPTER V

DATA ON SPOUSES

1. GENERAL. To implement Section 145a of the Atomic Energy Act of 1954, as amended, and Executive Order 10450, which require an investigation and report on an individual's character, associations, and loyalty, the Department needs information on spouses. In carrying out investigations of applicants, inquiries and record checks are made on spouses and former spouses named on the SF-86. However, when an individual marries after being granted access authorization, data on his/her spouse cannot be obtained without the cooperation of the individual in furnishing biographical data. DOE requires that individuals who marry after being granted access authorization complete a DOE F 5631.34 if their spouse does not now nor never has possessed a DOE access authorization. A DOE-cleared individual who marries a DOE-cleared individual is not required to submit DOE F 5631.34 since the Department has already established biographical information on the spouse. The form is also required for any cleared individual or applicant for access authorization who is married to a foreign national or a naturalized U.S. citizen.
2. PROCEDURES.
 - a. Cleared Individuals Who Marry.
 - (1) Within 45 days of marriage to an individual who does not now nor never has possessed a DOE access authorization, an individual who has been granted access authorization shall submit two copies of DOE F 5631.34 to the appropriate field element.
 - (2) A local agency check shall be made by either the FBI or OPM on the spouse; and
 - (3) The duplicate copy of DOE F 5631.34 shall be forwarded to DP-34 for requesting appropriate central file checks.
 - b. Individuals Whose Spouses Are Foreign Nationals or Naturalized U.S. Citizens.
 - (1) Applicants for access authorization shall submit, in addition to the required forms from Attachment II-1, two copies of DOE F 5631.34.
 - (2) A copy of DOE F 5631.34 shall be sent to the investigative agency with the request for investigation and the required security forms in applicant cases, and to DP-34 if the individual has already been granted access authorization.
 - (3) DP-34 shall initiate such investigation of the spouse of an individual who has been granted access authorization as may be appropriate, shall forward the reports of investigation to the manager of the field element concerned, and shall make any necessary name change on the Central Personnel Clearance Index.

- c. Name Changes. Whenever a DOE-cleared individual has a name change (e.g. resulting from a change in marital status) the individual must notify the appropriate DOE security office so that the appropriate name change can be made on the Central Personnel Clearance Index.
3. ADDITIONAL REQUIREMENTS. In reviewing the DOE F 5631.34 and investigative reports received on a spouse who is a foreign national or naturalized U.S. citizen, special consideration shall be given to the following:
 - a. How recently the spouse entered the U.S.
 - b. Whether the interests of the country of which the spouse is (or was) a citizen are inimical to the interests of the U.S.
 - c. Whether the spouse has close relatives residing in countries whose interests are inimical to those of the U.S. (to be evaluated in relation to 10 CFR 710).
 - d. In cases involving a spouse who is a foreign national, whether the spouse has declared his or her intention to become a U.S. citizen.

CHAPTER VI

ACCESS AUTHORIZATIONS FOR FOREIGN NATIONALS, INDIVIDUALS POSSESSING DUAL
CITIZENSHIP, AND NATURALIZED U.S. CITIZENS

1. REQUIREMENTS. Access authorization may be granted to a foreign national or dual citizen only when there is clear evidence that the applicant has unique talents or skills not possessed to a comparable degree by an available U.S. citizen and the position for which the individual is being considered is one that is essential to the Department's mission. The decision to consider a foreign national or dual citizen for access authorization must be based on the assumption that such an individual is a calculated risk. A decision must be made on whether sufficient information can be obtained to decide the individual's access eligibility.
2. STANDARDS AND PROCEDURES FOR PROCESSING FOREIGN NATIONALS.
 - a. Field Elements shall:
 - (1) Receive and consider requests for access authorizations for foreign nationals originated by Departmental Elements and contractors under their jurisdiction.
 - (2) Conduct an interview with all foreign nationals seeking DOE access authorization to develop the detailed information described in attachment II-2 of this Order.
 - (3) Evaluate the security risk arising from foreign national status, considering the following factors:
 - (a) The nationality of the foreign national;
 - (b) Whether sufficient security investigation can be obtained;
 - (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 evidenced an intention to become a U.S. citizen.
 - (4) Transmit requests which appear consistent with the requirements expressed above, together with all information and documents described in paragraph 2d below, to DP-34.

- (5) Upon approval of the requests by DP-34, process the requests in accordance with Chapter II of this Order, except that the determination to grant access authorization for foreign nationals shall be made by the managers of the operations offices and, in Headquarters, by the Director of Safeguards and Security (DP-34), without power of redelegation.
- (6) Forward to DP-34:
 - (a) A duplicate personnel security file of cases containing derogatory information;
 - (b) A report reflecting the data set forth in paragraph 2g below, when foreign nationals are employed on work requiring DOE access authorization; and
 - (c) Supplemental reports of any significant change in the individual's citizenship or employment status.
- b. Heads of Headquarters Elements shall review requests for foreign national access authorizations referred to them and shall transmit to DP-34 only those requests in which they find that the individual in question will materially benefit a DOE program by contributing unique or unusual skills or talents not possessed to any comparable degree by an available U.S. citizen.
- c. The Director of Safeguards and Security shall:
 - (1) Evaluate the security risk arising from foreign national status, taking into consideration those factors set forth on page VI-1, paragraph 2a(2);
 - (2) With the interested Headquarters official, jointly determine whether the potential contribution of the individual outweighs the security risk arising from foreign national status and shall return the application to the concerned field element with appropriate instructions regarding further processing; and
 - (3) Maintain liaison with other Federal agencies responsible for issues concerning foreign nationals.
- d. Information Required to Process Requests for Access Authorization for Foreign Nationals.
 - (1) SF-86, SF-87 or FD-258, and DOE 5631.18;
 - (2) Statement concerning program for which foreign national was recruited and specific access to classified information to be afforded.

- (3) Statement indicating title of position, location, and documentation indicating compliance with requirements expressed in paragraph 2a(2) above.
 - (4) Verbatim transcript or detailed summary of interview reflecting information which will aid in the investigation and the evaluation of the individual's eligibility for access authorization, including detailed information on steps taken by the individual to become a citizen of the United States; data on previous civilian or military service with a foreign government; information on family or other relatives abroad; family, legal, and financial ties abroad; and whether any relatives are employees of a foreign government; and the names of U.S. citizens who can furnish information on the individual's background and activities prior to his or her entrance into the United States.
- e. Scope of Investigation. A full field investigation shall be required for all levels of access authorization for foreign nationals. In cases where the individual has resided in, or has relatives living in a country where the language is written in a non-Roman alphabet (e.g., Hebrew, Arabic, Chinese, Japanese, Russian), the individual should furnish the information on former overseas addresses and on relatives in the non-Roman alphabet.
- f. Extension, Transfer, or Reinstatement of Access Authorization. Access authorization for a foreign national may be extended, reinstated, or accepted for transfer with the concurrence of the Headquarters official having functional interest in the work to be done by this individual and in accordance with procedures provided in Chapter VII.
- g. Reporting:
- (1) The reports forwarded to the Director of Safeguards and Security, as specified on page VI-2 paragraph 2a(5) shall reflect the following:
 - (a) Full name of the foreign national;
 - (b) Alien registration number;
 - (c) Type and date of access authorization required;
 - (d) Citizenship;
 - (e) Status of application for U.S. citizenship;
 - (f) Employer; and
 - (g) Description of duties and access required.

- (2) Supplemental reports shall reflect any substantial change in any of the above. In the event the foreign national becomes a citizen, the date and number of the naturalization certificate and place of naturalization shall be reported.
3. DUAL CITIZENSHIP. Individuals who possess dual citizenship status (i.e., are simultaneously a citizen of the United States and another country) will only be processed for a DOE access authorization provided they are advised prior to the initiation of the investigation that they shall be required to formally renounce their non-U.S. citizenship before a DOE access authorization will be granted. If the individual agrees to take action to formally renounce the non-U.S. citizenship, the investigation may be initiated with the appropriate investigative agency.
- a. Prior to being granted a DOE access authorization, an individual 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 renouncement 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 or her non-U.S. citizenship should accompany the notarized statement, as well as any document generated by the other country's government which acknowledges that the individual is no longer considered a citizen of that country.
 - b. If an individual possessing dual citizenship status declines to renounce non-U.S. citizenship, he or she must be processed for a DOE access authorization in accordance with the requirements on page VI-1, paragraphs 1 and 2.
 - c. The requirements in paragraphs 3a and b above may be waived by the Manager of Operations and DP-34 for DOE Headquarters, if it is determined that the individual's action to renounce the non-U.S. citizenship would be detrimental to the individual or DOE security objectives. A copy of the security evaluation documenting the exception shall be maintained in the individual's DOE Personnel Security File.
4. NATURALIZED U.S. CITIZENS. In cases where the individual became a U.S. citizen through naturalization subsequent to his/her 18th birthday, additional steps must be taken to ensure that the scope of the investigation is adequate.
- a. Prior to submission of the request for investigation to the investigative agency, an interview must be held or a signed response to a letter of interrogatory must be received covering the information described in Attachment II-2 of this Order.
 - b. A counterintelligence briefing should be given to the individual in conjunction with the granting of DOE access authorization. The responsibility for conducting these briefings will be assigned by the Manager of the Operations Office who will also determine their content.

CHAPTER VII

EXTENSIONS, TRANSFERS, TERMINATIONS AND
REINSTATEMENTS OF ACCESS AUTHORIZATIONS

1. EXTENSIONS AND TRANSFERS.

a. Definitions.

- (1) Extension of an Access Authorization is a field element authorization permitting an individual with an active access authorization under the jurisdiction of another field element to have concurrent access to classified matter or special nuclear material under the jurisdiction of the extending element.
- (2) Transfer of an Access Authorization is an acceptance by a field element of the active access authorization granted by another field element simultaneously with the termination of that access authorization by the latter.

b. Requests for Extension or Transfer of Access Authorizations received by field elements shall contain the full name of the individual, date of birth, social security number, and DOE file number (if known), to establish positive identification.

c. Procedures. The following procedures shall govern the handling of requests for the extension or transfer of active access authorizations.

- (1) The field element having custody of the individual's personnel security file shall inform the element extending the access authorization, or accepting it for transfer, of the following:
 - (a) The individual's date of birth;
 - (b) The individual's clearance status;
 - (c) The type of investigation upon which access authorization was based;
 - (d) If reinvestigated, date and action taken; and
 - (e) Whether the personnel security file contains unresolved derogatory information.
- (2) After positive identification has been established and based on the information received, the individual's access authorization shall be

extended or accepted for transfer unless the personnel security file contains unresolved derogatory information.

- (3) In case of transfer, the personnel security file shall be reviewed upon receipt and a note made to document the review before it is filed.
 - (4) When supplemental investigation is deemed appropriate, requests for such an investigation shall be submitted directly to the appropriate investigative agency.
 - (5) In cases involving the extension or transfer of an access authorization to a position certified as being "of a high degree of importance or sensitivity" and where the previous investigation was conducted by the OPM or another Federal agency, the request for the new investigation shall be forwarded to the FBI accompanied by a new SF-86, fingerprint card, and one copy each of the previous investigative reports (see Chapter II for detailed instructions).
 - (6) When derogatory information is found after access authorization has been granted and the information is not resolved, extension or transfer of access authorization shall not be accepted. Such cases shall be referred to DP-34, in accordance with Chapter III.
 - (7) In extension cases, the field office which granted the original (or oldest active clearance if the original access authorization has been terminated) access authorization shall be indicated on CPCI as being the file location and shall be responsible for the implementation of the Reinvestigation Program requirements as described in Chapter VIII. The only exception to this will be when the subsequent clearance extension or action results in a higher level of access authorization being granted. In such a case, the office granting the higher level of access authorization shall be indicated as the file location and will implement the Reinvestigation Program requirements.
- d. Documentation of Extensions and Transfers. The office extending the access authorization and the office accepting the transfer of an access authorization shall update the Central Personnel Clearance Index using instructions contained in the "System Reference Manual."
- e. Access Permit Program. Q and L access authorizations may be extended or transferred when appropriate to the access permit program and reclassified as Q(X) or L(X) access authorizations. Similarly Q(X) and L(X) access authorizations may be extended or transferred when appropriate to DOE contractor operations and reclassified as Q nonsensitive and L access authorizations.

- f. Interim Access Authorizations. Interim access authorizations will not be extended nor transferred. An individual with an interim access authorization will not be certified for a classified visit outside of the DOE complex.
- g. In the event the office that originated the clearance terminates the access authorization, the file shall be sent to the office to which the access authorization had been extended as described below in paragraph 2e.

2. TERMINATIONS.

- a. Definition. Termination of access authorization is the discontinuance of an individual's authorization to have access to classified matter or special nuclear material. (For the purposes of this part, terminations do not include suspensions or revocations.)
- b. DOE Access Authorizations Shall be Terminated When:
 - (1) Employment by the Department, its contractors or subcontractors is terminated.
 - (2) Access authorization is no longer required.
 - (3) An individual is on leave of absence or on extended leave and will not require access for at least 90 days. This 90-day period may be adjusted at the discretion of the manager of the operations office, or the Director of Safeguards and Security.
 - (4) Access to classified matter or special nuclear material is no longer required because of termination of employment or transfer to a position not requiring such access. Exceptions may be authorized upon certification by the employer that the individual shall be reemployed or reassigned with access within 3 months and that the Department shall be kept informed of the individual's status.
 - (5) An individual leaves for foreign travel, employment, education, or residence of more than 3 months not involving official U.S. Government business.
- c. Procedures.
 - (1) When an individual no longer requires DOE access authorization, the cognizant DOE security office shall be notified in writing by the employer within 30 days. The notice shall be accompanied by a completed DOE F 5631.29, "Security Termination Statement." When the DOE F 5631.29 cannot be provided, the reasons should be explained in the written notice.

(2) On receipt of this written notice, the cognizant DOE security office will then note in the individual's personnel security file the date and reason for termination of the access authorization, and make the appropriate entry to the Central Personnel Clearance Index.

- d. Termination Because of Foreign Travel. When access authorization is to be terminated as required in paragraph 2b(5) above, the individual shall, if possible, be advised that access authorization is being terminated and the reason therefor, and shall also be informed that it may be reinstated when he or she resumes work requiring it. The reinstatement procedure may require new security forms and/or an updated investigation as noted on page VII-4, paragraph 3.
- e. Transfer of Personnel Security Files of Terminated Cases. When a personnel security file of an individual whose access authorization has been terminated is transferred to another field element for retention, the transferring element shall enter the new file location on the Central Personnel Clearance Index.
- f. Central Personnel Clearance Index. The Office of Safeguards and Security shall maintain a central record of individual terminations and of the locations of files of individuals whose access authorizations have been terminated.
3. REINSTATEMENTS.
- a. Definition. Reinstatement of access authorization permits an individual whose access authorization has been terminated to again have access to classified matter or special nuclear material.
- b. Procedures.
- (1) New Forms. An up-to-date SF-86 shall be obtained if more than 6 months has elapsed since termination of access authorization and more than 1 year has elapsed since the date of the previous form, or any significant changes are known to have occurred since that date. When a SF-86 is not received, a request for reinstatement should contain the date of birth of the individual in order to establish positive identification. A new DOE F 5631.18 shall be obtained in all cases.
- (2) Personnel Security File. A review shall be made of the personnel security file of the individual to determine that the individual being reinstated is identical with the individual whose file is being reviewed and whether the previous investigation consisted of a National Agency Check or a full field investigation by the FBI, OPM, or another Federal agency.

- (3) Requests for Supplemental Investigation or National Agency Check for Reinstatement:
- (a) Supplemental Investigation shall be requested prior to reinstatement when:
- 1 New derogatory information has been found and has not been resolved following the initial granting of access authorization.
 - 2 The reason for the previous termination concerned eligibility for access authorization.
 - 3 In any Q-type case, more than 5 years have elapsed since the previous investigation.
- (b) National Agency Checks with Credit may be requested at the discretion of field elements in reinstating any level of access authorization even if none of the factors in subparagraph 3b(3)(a) above are present. A National Agency Check with Credit shall also be conducted, as a minimum, when more than 5 years has elapsed since the most recent investigation.
- (c) Procedure for Supplemental Investigation for Reinstatement. In requesting supplemental investigation, an original and one copy of a new SF-86 and new fingerprint cards shall be forwarded to the appropriate investigative agency. If the previous investigation was not made by the same investigative agency, one copy of each report of the previous investigation and a copy of the previous security form (DP-1 or SF-86) shall accompany the request .
- (4) "Position of a High Degree of Importance or Sensitivity". Where the reinstatement involves the assignment of an individual to a "position of a high degree of importance or sensitivity" (see Chapter I) and the previous investigation was not conducted by the FBI, a new SF-86 and one copy of each investigative report shall be forwarded to the FBI for investigation. Field elements may authorize the reinstatement of access authorization prior to receipt of the new investigation by the FBI, provided the circumstances listed in subparagraph 3b(3)(a) above do not apply.
- (5) Reinvestigations. Where the reinstatement involves an individual falling within the scope of the reinvestigation program, the case shall concurrently be processed for reinvestigation (see Chapter VIII).

4. TRANSMITTAL OF PERSONNEL SECURITY FILES. Personnel security files being transferred by mail shall be sent via First Class mail, except those classified Secret, which shall be sent via registered mail. This applies to active or inactive files and the mailing of one or more investigative reports to the investigative agencies, Headquarters, or other field elements. A memorandum or other transmittal form shall be used to ensure that a record of the location of personnel security files and reports is maintained. Files shall be transmitted in double envelopes, the inner envelope marked "Security Mail--To Be Opened By Addressee Only," in addition to any classification markings that are required.

CHAPTER VIII
REINVESTIGATION PROGRAM

1. GENERAL INFORMATION. The DOE Reinvestigation Program is designed to ensure the continued eligibility for access authorization of individuals employed in classified programs of the Department. It applies to all individuals possessing DOE security clearance or access authorization except the following:
 - a. Members of the Armed Services;
 - b. Employees of agencies of the Department of Defense (DOD) and their contractors;
 - c. Employees of other executive branch departments or agencies and their contractors who hold DOE Q non-sensitive or L access authorization.

2. REEVALUATION. The eligibility of access authorization of individuals holding DOE access authorization shall be reevaluated every 5 years on the basis of either field reinvestigations, National Agency Checks with Credit, or file and fingerprint checks.

3. DETERMINING THE TYPE OF REINVESTIGATION TO BE CONDUCTED. The type and schedule of reinvestigation to be conducted shall be determined by the access authorization held by the individual. Reinvestigation requirements for each level are listed below.
 - a. Q Sensitive Position Also Designated to be a Position of a High Degree of Importance or Sensitivity (guidelines for making this determination are contained on page I-2, paragraph 2a(1)).
 - (1) After the first 5 years -- Federal Bureau of Investigation (FBI) full field investigation;
 - (2) After 10 and 15 years -- National Agency Check with Credit;
 - (3) After 20 years -- FBI full field reinvestigation; and
 - (4) Every 5 years thereafter -- National Agency Checks with Credit.
 - b. Q and Top Secret (other than those described in subparagraph 3a above).
 - (1) After the first 5 years -- Office of Personnel Management (OPM) Limited Background Investigation (LBI);
 - (2) After 10 and 15 years -- National Agency Checks with Credit;

- (3) After 20 years -- OPM Special Background Investigation; and
- (4) Every 5 years thereafter -- National Agency Checks with Credit.

c. L and Secret.

- (1) After first 5 years -- National Agency Checks with Credit;
- (2) After 10 and 15 years -- review of completed SF-86, plus FBI file and fingerprint check;
- (3) After 20 years -- National Agency Checks with Credit; and
- (4) Every 5 years thereafter -- review of completed SF-86, plus FBI file and fingerprint check.

- 4. SCHEDULING REINVESTIGATIONS. The manager of the operations office shall establish a schedule for submitting requests for and evaluation of reports of reinvestigation for cases under his or her jurisdiction.
- 5. EVALUATION PROCEDURES. The results of the reinvestigation shall be screened and analyzed following the procedures described in Chapter III. The results of the evaluation shall be entered into the Central Personnel Clearance Index following the instructions contained in the System Reference Manual.

CHAPTER IX

ESTIMATES OF REQUESTS FOR SECURITY INVESTIGATIONS

1. GENERAL. Changes in DOE programs, classification levels, and rates of labor turnover affect the number of security investigations that will be required. The Office of Safeguards and Security needs quarterly estimates of requests for security investigations to control funds and to submit to the OPM and FBI in order to determine their staff requirements. (The document which is used as the basis for preparing the annual budget estimates for security investigations shall be provided by DP-34 each year.)
2. PROCEDURES. Managers of the operations offices prepare and submit to DP-34 quarterly estimates of security investigations, as indicated below.
 - a. Form. Estimates shall be submitted on DOE F 5631.3, "Estimated Requirement for Full-Field Investigation and National Agency Checks for Security Clearance."
 - b. Submission Dates. Six-month estimates shall be submitted quarterly by 3-25, 6-25, 9-25, and 12-25 of each year.
 - c. Types of Investigations to be Included. Estimates shall include the numbers of Background Investigations, Limited Background Investigations, Special Background Investigations, and National Agency Checks to be conducted.
 - d. Consideration in Arriving at Estimates.
 - (1) Actual experience of the previous year and months;
 - (2) Changes in programs, changes in classification, contractor's work force levels, and rates of labor turnover; and
 - (3) Use of Secret and L access authorizations to the fullest extent possible.
3. RECORDS. It is recommended that each field element maintain a tracking system of the actual number of investigations processed for each area office and major contractor or project to assist in preparation of estimates.