U.S. NUCLEAR REGULATORY COMMISSION

DIRECTIVE TRANSMITTAL

TN: DT-04-07

To: All NRC Employees and NRC Management Directives Custodians

Subject: Transmittal of Management Directive12.3, "NRC Personnel Security Program"

Purpose: Directive and Handbook 12.3 are being revised to enhance clarity and to reflect organizational changes within NRC. Changes were made to the responsibilities and authorities portion of the directive to include the responsibilities of the NRC Office of Nuclear Security and Incident Response that was established in 2002.

Office and Division of Origin: Office of Administration
Division of Facilities and Security

Contact: Patricia Smith, 301-415-7739

Date Approved: November 17, 1999 **(Revised: April 27, 2004)**

Volume: 12 Security

Directive: 12.3, NRC Personnel Security Program

Availability: Rules and Directives Branch
Office of Administration
Michael T. Lesar, 301-415-7163
Christy Moore, 301-415-7086

NRC Personnel Security Program

Directive 12.3

Contents

NRC Personnel Security Program
Directive 12.3

Policy
(12.3-01)

It is the policy of the U.S. Nuclear Regulatory Commission to establish a personnel security program to ensure that determinations are made in accordance with pertinent laws, Executive Orders, management directives, and applicable directives of other Federal agencies for an NRC access authorization (i.e., security clearance); an NRC employment clearance (i.e., pre-appointment investigation waiver, Section 145b of the Atomic Energy Act of 1954 (AEA), as amended); unescorted access to nuclear power facilities for NRC employees or contractors; access to special nuclear material by NRC licensees; access to unclassified Safeguards Information (SGI); access to sensitive NRC information, technology systems or data; unescorted access to NRC facilities; visits involving classified National Security Information (NSI), Restricted Data (RD), or Sensitive Compartmented Information (SCI); and providing information to foreign regulatory assignees. It is also NRC policy that its workplace be free from illegal use, possession, or distribution of controlled substances.

Objective
(12.3-02)

To provide assurance that NRC employees, consultants, contractors, and licensees are reliable and trustworthy to have access to NRC facilities, classified information, sensitive NRC information and equipment, nuclear power facilities, and special nuclear material.

Organizational Responsibilities and Delegations of Authority

(12.3-03)

Commission

(031)

Performs the Commission functions specified in 10 CFR Part 10 relative to personnel security clearance cases subject to personnel security hearing procedures.

Deputy Executive Director for Management Services (DEDM)

(032)

- Performs the functions assigned to the DEDM under 10 CFR Part 10, including appointment of the NRC Hearing Counsel and the granting, suspension, denial, or revocation of access authorization. (a)

- Grants exemptions to 10 CFR Parts 25, "Access Authorization for Licensee Personnel," and 95, "Security Facility Approval and Safeguarding of National Security Information and Restricted Data," when a finding can be made that the requested exemption does not endanger the common defense and security, as authorized by SECY-80-387. (b)

- Performs the functions of the designated NRC Senior Agency Official, pursuant to the provisions of Section 6.1(a) of Executive Order (E.O.) 12968, "Access to Classified Information," to direct and administer the NRC's Personnel Security Program, including active oversight and implementation of continuing security education and awareness programs, to ensure that the order is effectively carried out. (c)

- Approves NRC's employment of individuals before the security investigation is completed, as required by Section 145b of the

Organizational Responsibilities and Delegations of Authority

(12.3-03) (continued)

Deputy Executive Director for Management Services (DEDM)

(032) (continued)

AEA, provided that the individual is not granted access to classified NSI, the requesting office clearly demonstrates a need for the individual, and an affirmative recommendation is made by the Director of the Division of Facilities and Security (DFS), Office of Administration (ADM). (d)

- Grants, under the authority in Section 145b, AEA, access to RD and other NRC classified information to designated members of Congress (no investigation to be conducted). This access, as authorized by SECY-81-291, applies to members of Congress serving on NRC Congressional Oversight Subcommittees. (e)

- Establishes, under the authority of Section 145g, AEA, standards and specifications in writing as to the scope and extent of investigations, the reports of which NRC will use to make the determination that permitting a person access to RD will not endanger the common defense and security. (f)

General Counsel (GC)

(033)

- Performs the functions assigned to the GC under 10 CFR Part 10, including concurrence in the issuance of subpoenas. (a)

- Performs legal review of matters related to personnel security. (b)

Organizational Responsibilities and Delegations of Authority

(12.3-03) (continued)

Inspector General (IG)

(034)

Provides DFS, ADM, with information obtained in audits and investigations that is relevant to security issues.

Director, Office of International Programs (OIP)

(035)

Approves or disapproves the assignment of foreign regulatory employees to NRC after security approval from DFS, ADM, and coordination with the office to which the person is temporarily assigned.

Director, Office of Administration (ADM)

(036)

- Performs the functions assigned to ADM under 10 CFR Part 10. (a)

- Oversees the NRC personnel security program as carried out by DFS, ADM. (b)

Director, Office of Investigations (OI)

(037)

- Coordinates with DFS whenever information derived from DFS files alone and not corroborated by other means is used in OI reports. (a)

- Provides security-related information to DFS developed on NRC employees, licensees, licensee applicants, licensee contractors, or vendor personnel who currently possess or are

Organizational Responsibilities and Delegations of Authority

(12.3-03) (continued)

Director, Office of Investigations (OI)

(037) (continued)

in the process of obtaining an access authorization or other security determination. (b)

Director, Office of Human Resources (HR)

(038)

Concurs in a request for a pre-appointment investigation waiver under Section 145(b) of the AEA.

Director, Office of Nuclear Security and Incident Response (NSIR)

(039)

Informs ADM of any changes to the access authorization program requirements for NRC - licensed facilities to ensure comparability between licensee and NRC programs.

Office Directors and Regional Administrators

(0310)

- Ensure that NRC employees, NRC contractor personnel, and any other personnel under their jurisdiction are cognizant of and comply with the provisions of this directive and handbook, as appropriate. (a)

- Ensure that NRC licensee and licensee-related personnel under their jurisdiction are cognizant of and comply with the personnel security provisions of 10 CFR Parts 10, 25, and 95. (b)

Organizational Responsibilities and Delegations of Authority

(12.3-03) (continued)

Office Directors and Regional Administrators

(0310) (continued)

- Advise DFS of any information that indicates noncompliance with this directive and handbook or that is otherwise pertinent to the proper protection of classified interests, SGI, sensitive unclassified information, or NRC property. (c)

- Notify DFS of individuals under their jurisdiction who possess an access authorization, or for whom an access authorization has been requested, who are hospitalized or otherwise treated for an illness or mental condition that may cause defects in their judgment, trustworthiness, or reliability, and of any subsequent developments as required by Handbook 12.3. (d)

- Notify DFS of persons under their jurisdiction possessing access authorizations or who are disabled for a prolonged period (over 90 days), who die, who for any other reason no longer require access authorization, require change of access authorization, or who are subject to any circumstance that may affect their continued eligibility for access authorization or access approval. (e)

- Report immediately to the IG and DFS all alleged or suspected incidents of employee or contractor fraud, misconduct, unauthorized disclosure, or misuse of automated information systems. (f)

Director, Division of Facilities and Security (DFS), ADM

(0311)

- Plans, develops, establishes, and administers policies, standards, and procedures for the overall NRC personnel

Organizational Responsibilities and Delegations of Authority

(12.3-03) (continued)

Director, Division of Facilities and Security (DFS), ADM

(0311) (continued)

security program, including denial or revocation in cases involving substantially derogatory information falling within 10 CFR 10.11 when the case has not been favorably resolved through an interview or other investigation. (a)

- Administers the visitor control program, including incoming and outgoing visits requiring access to classified NSI, the assignment of foreign regulatory employees to the NRC in coordination with the Office of International Programs, and the acceptance and issuance of security assurances to and from foreign governments. (b)

- Serves as the NRC central point of contact with the Federal Bureau of Investigation, the Office of Personnel Management, the General Services Administration, and other investigative agencies on NRC personnel security matters. (c)

- Recommends to the DEDM an AEA Section 145b pre-appointment investigation waiver. (d)

- Supplies OIG with the information necessary to conduct investigations and audits. (e)

Applicability

(12.3-04)

This directive and handbook apply to all NRC employees, licensees, consultants, experts, panel members, applicants for employment, and other persons designated by the DEDM as well as to all NRC contractors and subcontractors to whom they apply as a condition of a contract or a purchase order.

Organizational Responsibilities and Delegations of Authority

(12.3-03) (continued)

Handbook

(12.3-05)

Handbook 12.3 provides guidelines for personnel security, classified visits, drug testing, and foreign assignees.

Exceptions or Deviations

(12.3-06)

Exceptions or deviations to this directive and handbook may be granted by the Director of DFS, in writing, except for those areas in which the responsibility or authority is vested solely with the Commission, the DEDM, or the Director of ADM and is nondelegable; or for matters specifically required by law, Executive Order, or directive to be referred to other management officials.

References

(12.3-07)

Code of Federal Regulations—

10 CFR 1.12, "Office of the Inspector General."

10 CFR Part 10, "Criteria and Procedures for Determining Eligibility for Access to Restricted Data or National Security Information or an Employment Clearance."

10 CFR Part 25, "Access Authorization for Licensee Personnel."

10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data."

References

(12.3-07) (continued)

32 CFR Part 147, "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information."

Department of Defense

"National Industrial Security Program Operating Manual (NISPOM)," DOD 5220.22-M, January 1995, and Supplement 1, February 1995.

Executive Orders—

10450, "Security Requirements for Government Employment," April 27, 1953, as amended.

10865, "Safeguarding Classified Information Within Industry," February 20, 1960, as amended.

12564, "Drug-Free Workplace," September 15, 1986.

12958, "Classified National Security Information," as amended, March 28, 2003.

12968, "Access to Classified Information," August 2, 1995.

United States Code

Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).

"Crimes and Criminal Procedures" (Title 18, *United States Code*).

Energy Reorganization Act of 1974, as amended (42 U.S.C. 5801 et seq.).

Freedom of Information Act of 1966 (5 U.S.C. 522).

References

(12.3-07) (continued)

Inspector General Act (5 U.S.C. App. 3).

Privacy Act of 1974, as amended (5 U.S.C. 552a).

"Section 503 of the Supplemental Appropriation Act of 1987, Public Law 100-71," July 11, 1987.

"Suspension and Removal" (5 U.S.C. 7532).

U.S. Nuclear Regulatory Commission

NRC Management Directives—

3.1, "Freedom of Information Act."

3.2, "Privacy Act."

3.4, "Release of Information to the Public."

10.1, "Appointments, General Employment Issues, Details, and Position Changes."

11.1, "NRC Acquisition of Supplies and Services."

12.2, "NRC Classified Information Security Program."

NRC SECY-80-387, "Delegation of Authority to Grant Exemptions to 10 CFR Parts 25 and 95," August 15, 1980.

NRC SECY- 81-291, "Approval Under Section 145b of the Atomic Energy Act of 1954, as Amended, to Grant Access to Restricted Data and Other NRC Classified Information to Designated Members of Congress (No Investigation To Be Conducted)," May 5, 1981.

NRC System of Records NRC-39, "Personnel Security Files and Associated Records—NRC."

NRC Personnel Security Program

Handbook 12.3

Contents

Part I

Contents (continued)

Contents (continued)

Part I
NRC Access Types

Introduction (A)

NRC reviews and makes eligibility determinations for NRC access authorization and/or employment clearance, unescorted access to nuclear power facilities, access to Safeguards Information (SGI), access to sensitive NRC information technology systems or data, or unescorted access to NRC facilities. Exhibits 1 through 6 are provided to explain in greater detail the requirements of MD 12.3. (1)

See Exhibit 6 for security clearances/access types and investigative requirements for those with authorized access and an established need-to-know. (2)

Personnel security and associated records maintained under the provisions of the NRC personnel security program are protected from public disclosure under the provisions of the Privacy Act of 1974, as amended, and are subject to the routine uses specified for NRC System of Records NRC-39, "Personnel Security Files and Associated Records—NRC." (3)

Position Sensitivity Criteria (B)

These criteria determine whether a person in a particular NRC position requires a "Q" or a high public trust "L(H)" security clearance on the basis of an SSBI by the Office of Personnel Management (OPM) or the Federal Bureau of Investigation (FBI), or an "L" security clearance, as a minimum, on the basis of an access national agency check with inquiries (ANACI).

Special Sensitive Positions of a High Degree of Importance or Sensitivity for Sensitive Compartmented Information (1)

People in positions of a high degree of importance or designated as special-sensitive require an NRC "Q" access authorization

Position Sensitivity Criteria (B) (continued)

Special Sensitive Positions of a High Degree of Importance or Sensitivity for Sensitive Compartmented Information (1) (continued)

based on an OPM or FBI SSBI pursuant to Section 145f of the Atomic Energy Act of 1954 (AEA), as amended. These positions include the following:

- The Chairman (a)
- An NRC Commissioner (b)
- The Inspector General (IG) (c)
- Any person who requires access to sensitive compartmented information (d)

Positions of a Critical-Sensitive Designation That Require a "Q" Clearance (2)

People in certain critical-sensitive positions must have an NRC "Q" access authorization based on an SSBI. Functions considered critical-sensitive and requiring a "Q" clearance have one or more of the following characteristics:

- Access to Secret or Top Secret-Restricted Data or Top Secret National Security Information (a)
- Access to Confidential Restricted Data involving broad naval nuclear propulsion program policy or direction (e.g., preliminary safety analysis reports, final safety analysis reports, and amendments thereto). This does not apply to information associated with the transportation, storage, or disposal of naval nuclear propulsion fuel or components that is classified as Confidential Restricted Data (b)

Position Sensitivity Criteria (B) (continued)

Positions of High Public Trust That Require an "L(H)" Clearance (3)

People in positions of high public trust require an "L(H)" access authorization based on an OPM SSBI. The types of functions considered to be of high public trust include one or more of the following characteristics:

- Final approval of plans, policies, or programs that directly affect the overall operations and direction of the NRC. (a)

- Responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or the capability to access a computer system during its operation or maintenance in such a way that could cause, or that has a relatively high risk of causing, grave damage; or the capability to realize a significant personal gain from computer access. (b)

- Resident inspectors. (c)

- Such other duties requiring high public trust as determined on an as-needed basis by the Deputy Executive Director for Management Services (DEDM). (d)

"L" Positions of a Noncritical-Sensitive Designation (4)

People in any NRC position not covered by Section (B)(1), (2), or (3) of this part require an NRC "L" access authorization based on an ANACI investigation.

Access Authorization Requests (C)

Employees (1)

Access authorizations ("Q," "L(H)," or "L"), for NRC employees, applicants for NRC employment (i.e., anyone who has received an

Access Authorization Requests (C) (continued)

Employees (1) (continued)

authorized conditional offer of employment), and NRC experts, panel members, and consultants must be requested from the Division of Facilities and Security (DFS), Office of Administration, on NRC Form 236, "Personnel Security Clearance Request and Notification," by the employing division director or his or her designee. Requests for access authorization are submitted through the Office of Human Resources (HR) or the Regional Personnel Office (RPO), as appropriate. The Office of the Inspector General (OIG) requests are forwarded directly to DFS. Instructions are printed on the reverse side of the form. (a)

The NRC official (HR or regional designee) responsible for submitting NRC Form 236 to DFS with a completed security forms packet shall ensure that the information shown on the applicant's employment form is consistent with the information reflected in Part 1 of the "Questionnaire for National Security Positions" (QSP, Standard Form [SF] 86). If the information is not consistent, an explanation and assessment should be furnished to DFS regarding the inconsistency. (b)

All applicants for an NRC access authorization must meet the investigative coverage requirements for the immediate period prior to the date the applicant signed his or her security forms. (For "Q" and "L(H)" clearances, the applicant must meet the immediate 10-year coverage requirement. For "L" clearances, the requirement is the immediate 7-year coverage period.) All NRC employees must have a security clearance or a temporary waiver of a clearance (see Section 145b of the AEA). The temporary waiver is normally granted to new employees while an investigation is being conducted to meet the requirements for a security clearance. The temporary waiver does not permit access to classified information. An investigation of an applicant's background is conducted by the Security Branch to provide the basis for the temporary waiver. A more thorough investigation, usually conducted by the Office of Personnel Management,

Access Authorization Requests (C) (continued)

Employees (1) (continued)

provides the basis for granting a clearance. For "Q" and "L(H)" clearances, the investigation will cover the last 10 years. For "L" clearances, the investigation will cover the last 7 years. Applicants living overseas for extended periods (1 year or more) during these 7- or 10-year periods may not be able to be investigated in a timely manner, which could result in a decision not to grant the temporary waiver or a delay of the clearance. (c)

A security orientation briefing must be given to NRC employees and consultants requiring access authorizations when they enter duty status. This briefing will normally be given by a representative of the Division of Facilities and Security (DFS) or, in a regional office, by a regional security representative (see Exhibit 1). (d)

Contractors (2)

Access authorizations for NRC contractors, subcontractors, or other individuals who are not NRC employees (e.g., other Government agency personnel or licensees) may be requested on NRC Form 237, "Request for Access Authorization." The requester must forward this form to DFS or, if otherwise indicated, to the approving official of the NRC office sponsoring the activity that requires NRC access authorization. Instructions are printed on the reverse side of the form.* (a)

At those contractor facilities at which NRC is not the cognizant security authority (CSA), access authorizations will be requested following the procedures of the CSA. (b)

A foreign ownership, control, or influence (FOCI) review must be completed with a favorable determination on a company before

*All contractors must meet the same investigative requirements as listed under "Employees" in Section (C)(1) above.

Access Authorization Requests (C) (continued)

Contractors (2) (continued)

granting personnel security clearances. A FOCI is not required for information technology (IT) access or building access. (For further guidance on FOCI, refer to MD 12.1, "NRC Facility Security Program," and MD 12.2, "NRC Classified Information Security Program.") (c)

A security orientation briefing must be given to NRC contractors requiring access authorizations when they enter on duty. This briefing will normally be given by a representative of the Division of Facilities and Security (DFS) or, in a regional office, a regional security representative (see Exhibit 1). (d)

Security Forms Packet for an Access Authorization Request (3)

Unless otherwise indicated, each request for access authorization must be accompanied by a properly completed security forms packet consisting of— (a)

- SF 86, QSP. (Part 2 of the QSP is the privacy portion and is to be placed in the sealed envelope, NRC Form E-1, provided to the respondent. The NRC will maintain the privacy of the information provided on this form, Parts 1 and 2.) (i)

- Two applicant fingerprint cards (SF 87 for Federal employee applicants or FD 258 for contractors), or equivalent electronic fingerprint images. (ii)

- NRC Form 176, "Security Acknowledgment." (iii)

- One copy of Optional Form (OF) 612, "Optional Application for Federal Employment"; résumé; or equivalent for NRC applicants (not required for contractors). (iv)

Access Authorization Requests (C) (continued)

Security Forms Packet for an Access Authorization Request (3) (continued)

- A Section 145b (AEA) memorandum (not required for contractors or licensees). (v)
- NRC Form 236 (for NRC employees) and NRC Form 237 (for contractors or licensees requiring access authorization). (vi)
- OF 306, "Declaration for Federal Employment" (not required for contractors or licensees). (vii)
- Reference checks (not required for contractors or licensees). (viii)
- Education verification (not required for contractors or licensees). (ix)
- NRC Form 448, "Request for Appointment of a Consultant, Expert, or Member" (for consultants; not required for contractors, NRC applicants, or licensees). (x)
- Foreign national questionnaire. (xi)
- Dual citizenship questionnaire. (xii)
- NRC Form 89, "Photo-Identification Badge Request" (for NRC contractors; not required for NRC employees, licensees, or consultants). (xiii)

DFS will return requests for access authorization to the requester if— (b)

- All security forms are not completed and signed as required. (i)
- The printed content of the security or release form is altered. (ii)

Access Authorization Requests (C) (continued)

Security Forms Packet for an Access Authorization Request (3) (continued)

- Required information is not provided. (iii)
- The forms are illegible. (iv)
- The "Authorization for Release of Information" on the SF 86 is not signed. (v)

Information entered on the forms in the security packet will be used in conjunction with any other relevant information to determine an individual's initial or continued eligibility for an access authorization, an employment clearance, unescorted access to nuclear power facilities, access to SGI, or access to sensitive NRC IT systems or data. (c)

Cancelled or Withdrawn Request (4)

When a request for an applicant's access authorization is to be withdrawn or cancelled, DFS should be notified immediately by telephone or e-mail so that the investigation may be promptly discontinued. The notification should contain the full name of the individual, the date of the request, and the type of access authorization being cancelled. Telephone notifications must be promptly confirmed in writing to DFS.

Contractual Language for Unescorted Access by NRC Contractors (D)

Sponsoring Office Responsibilities for Unescorted Access of NRC Contractors (1)

The NRC sponsoring office shall decide whether performance under an NRC contract, interagency agreement (IAA), or memorandum of understanding (MOU) will involve unescorted

Contractual Language for Unescorted Access by NRC Contractors (D) (continued)

Sponsoring Office Responsibilities for Unescorted Access of NRC Contractors (1) (continued)

access to nuclear power facilities, access to SGI, access to NRC IT systems or sensitive information, or building access. For these contracts, the sponsoring office shall state on the appropriate procurement request document that— (a)

– "This contract requires unescorted access to nuclear power facilities by contractor employees," or "This contract requires contractor access to nuclear power reactor SGI," or "This contract requires access to NRC information technology systems or sensitive information." (i)

– "This contract requires continuous unescorted access (in excess of 30 days or more) to NRC Headquarters or regional office facilities, or otherwise requires NRC photo-identification or keycard badges." (ii)

Include an NRC Form 187, "Contract Security and/or Classification Requirements," according to the requirements of Management Directive (MD) 11.1, "NRC Acquisition of Supplies and Services." (See MD 12.1, "NRC Facility Security Program," for escort and badge responsibilities and also MD 11.1, Section 5.7, "Security Requirements.") (b)

Any contractor employee who is granted access in accordance with this section will be afforded due process if derogatory information is developed that could result in that access being denied or revoked. The contractor employee must be provided written notification of the grounds for the denial or revocation. Additionally, the contractor employee must be given the opportunity to provide additional relevant information relating to the denial or revocation. Furthermore, the contractor employee will be provided an impartial and independent review of all the information on which the denial or revocation was based. (c)

Contractual Language for Unescorted Access by NRC Contractors (D) (continued)

Unescorted Access at Nuclear Power Reactor Facilities (2)

Individual contractors requiring access will be approved for unescorted access to protected and vital areas of nuclear power facilities in accordance with the following procedures:

- Interim Approval (a)

  Interim approvals may be obtained by two methods:

  – For the first method, the contractor employee shall submit to DFS through the NRC project officer the following information: (i)

    - A completed personnel security forms packet, including an SF 86 QSP. (*a*)

    - Copies of the contractor employee's 5-year employment and education history checks, including verification of the highest degree obtained. (*b*)

    - A reference from at least one additional person not provided by the individual. (*c*)

    - A psychological assessment designed to evaluate the possible impact of any noted psychological characteristics that may have a bearing on trustworthiness and reliability. (*d*)

    - A signed copy of NRC Form 570, "Access Authorization Acknowledgement." (The contractor employee's signature indicates that he or she understands his or her responsibility to report to NRC any information bearing on his or her continued eligibility for access authorization as specified in 10 CFR 10.11.) (*e*)

Contractual Language for Unescorted Access by NRC Contractors (D) (continued)

Unescorted Access at Nuclear Power Reactor Facilities (2) (continued)

- A certification that the contractor company has found all checks acceptable. (*f*)

- In limited cases, as determined by the sponsoring office, a copy of the contractor's 1-year employment check, along with items (D)(2)(a)(i)(*a*) and (*c*) through (*f*) of this part. (*g*)

  DFS will conduct criminal history and credit checks and hold a security assurance interview with the contractor employee as specified in the above items. On the basis of the result of these checks, DFS will determine the contractor employee's eligibility for interim access and will indicate “objection” or “no objection” to the sponsoring office, pending completion of the required background investigation.

– For the second method, the contractor employee will be fingerprinted by the utility and the individual will be subject to the utility's access authorization program. (ii)

- Final Approval (b)

  Final access approval will be granted after—

  – The required investigation on the individual has been completed and has received a favorable adjudication review, resulting in NRC's endorsement of the individual's unescorted access at all nuclear facilities as long as the individual employee is employed on the contract and provided no new issue information is developed that may bring the individual’s eligibility into question. (i)

Contractual Language for Unescorted Access by NRC Contractors (D) (continued)

Unescorted Access at Nuclear Power Reactor Facilities (2) (continued)

– The contractor has obtained unescorted access authorization (other than interim access) at the specific facility through that utility's access authorization program. (ii)

– The individual possesses a valid Federal Government-issued security clearance as verified by DFS. (iii)

- Resolving Questions of Eligibility (c)

The investigation described in Section (D)(2)(b)(i) of this part may involve an ANACI or other investigation as DFS deems necessary. Any question regarding the contractor employee's eligibility for unescorted access to protected or vital areas of nuclear power facilities will be resolved before granting a final approval.

- Notification of Unusual Circumstances (d)

When a contractor who possesses interim or final unescorted access to nuclear power facilities or access to SGI is hospitalized or otherwise treated for an illness or mental condition that may cause a defect in the person's judgment or reliability, the person's contracting officer, the security officer, or other person so designated must promptly report the circumstances to the Director of DFS.

Access to Safeguards Information (SGI) by NRC Contractors (E)

The NRC sponsoring office shall decide whether performance under an NRC contract will involve access to SGI. This access may require a national agency check with law and credit (NACLC) or other investigation as DFS deems necessary. On the basis of the review of the applicant's security forms by DFS and/or the receipt of adverse information by NRC, the individual may be denied access to SGI until a final determination of his or her eligibility for access is made. SGI access for contractor employees may be granted under licensee programs. See MD 12.6, "NRC Sensitive Unclassified Information Security Program," for further information.

Access to NRC IT Systems or Sensitive Information by NRC Contractors or Consultants (F)

The Executive Director for Operations (EDO) approved the sensitivity criteria to be used in determining whether individual contractor employees shall require IT Level I or Level II approval for access to NRC IT systems or sensitive information. An IT Level I or Level II approval shall require a background investigation. IT Level I or Level II access is also required for contractors working offsite with sensitive unclassified information. (1)

Contractors being processed for IT access, either Level I or Level II, must be granted either an interim access or a final access based on a background investigation. An investigation of an applicant's background is conducted by the Security Branch to provide the basis for the interim access. A more thorough investigation covering the last 7 years, usually conducted by the Office of Personnel Management, provides the basis for granting the final access. Applicants living overseas for extended periods (1 year or more) during the last 7 years may not be able to be investigated in a timely manner, which could result in a decision

Access to NRC IT Systems or Sensitive Information by NRC Contractors or Consultants (F) (continued)

not to grant interim access or a delay of the determination to grant final access. (2)

IT Level I (a)

IT Level I involves responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design of a computer system, including the hardware and software; the capability to access a computer system during its operation or maintenance in such a way that could cause or that has a relatively high risk of causing grave damage; or the capability to realize a significant personal gain from computer access. Such positions may involve—

- Responsibility for the development, direction, implementation, and administration of agency computer security programs, including direction and control of risk analysis or threat assessment. (i)

- Significant involvement in life-critical or mission-critical systems. (ii)

- Responsibility for the preparing or approving of data for input into a system that does not necessarily involve personal access to the system but creates a high risk for grave damage or realizing significant personal gain. (iii)

- Relatively high-risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of either— (iv)

  – Dollar amounts of $10 million per year or greater. (*a*)

Access to NRC IT Systems or Sensitive Information by NRC Contractors or Consultants (F) (continued)

IT Level I (a) (continued)

– Lesser amounts if the activities of the individual are not subject to technical review by higher authority at the IT Level I to ensure the integrity of the system. (*b*)

- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software. (v)

- Other positions that involve relatively high risk for causing grave damage or realizing significant personal gain. (vi)

IT Level II (b)

IT Level II includes all other individuals with access to IT systems or sensitive information, including those needing an NRC local area network (LAN) account. (i)

Individual contractor employees requiring access will be approved for access in accordance with the following procedures. (ii)

Interim Approval (c)

The contractor employee shall submit a completed personnel security forms packet, including an SF 86 QSP, an FD 258, and an NRC Form 89, to DFS through the NRC project officer. (i)

The project officer shall forward the completed security forms packet to DFS together with a written request, including employer name and contract number, identifying whether the contractor employee shall be processed for IT Level I or Level II access and the specific criterion(ia) that applies (apply). (ii)

Access to NRC IT Systems or Sensitive Information by NRC Contractors or Consultants (F) (continued)

Interim Approval (c) (continued)

DFS will conduct criminal history and credit checks, review form SF 86, and determine the contractor employee's eligibility for interim access and will issue a memorandum reflecting interim approval or disapproval to the sponsoring office, pending completion of the required background investigation. (iii)

Resolving Questions of Eligibility (d)

On the basis of DFS's review of the contractor employee's security forms, background investigation, and/or the receipt of issue information, the Chief of the Security Branch (SB) may deny a contractor employee access to NRC IT systems or sensitive information until a final determination of eligibility for access is made.

Final Approval or Disapproval (e)

Upon receipt of the complete investigation, DFS will adjudicate the packet. A final letter will be issued by DFS to the sponsoring office indicating approval or denial for IT Level I or Level II access.

Contractors Requiring Building Access to NRC Facilities (G)

The number of contractors under escort working in the building should be minimized. The NRC sponsoring office shall decide whether performance under an NRC contract, purchase order, IAA, MOU, or similar agreement will involve unescorted building access (over a period of more than 30 calendar days) or requires an NRC photo-identification or keycard badge to NRC Headquarters buildings or regional office facilities. If it is determined that the work will take more than 30 days, or that the

Contractors Requiring Building Access to NRC Facilities (G) (continued)

work requires a photo-identification badge, approval for unescorted building access must be received by DFS before the onsite work begins. For these contractual or other similar arrangements or agreements requiring unescorted building access to the NRC facilities, the sponsoring office shall include an NRC Form 187 with Section 5F checked. (1)

Individual contractor employees or other individuals requiring building access will be approved for continuous unescorted access in accordance with the following procedures: (2)

Contractor Building Access Procedures

Approval for granting contractors unescorted building access must be based on 5 years of investigative coverage in the U.S. Contractors with less than 5 years of investigative coverage in the U.S. may be granted unescorted building access with restrictions specified by DFS, such as going through lobby screening procedures before each entry to the building.

- Interim Building Access Approval or Denial (a)

  The contractor shall submit the following information to DFS through the NRC Headquarters or regional project officer: a completed General Services Administration (GSA) Form 176, "Statement of Personal History," and two FD 258s, "Fingerprint Chart," or electronic fingerprints, and NRC Form 89, "Photo Badge Request." All foreign nationals or naturalized citizens must provide original legal residence documentation (e.g., a naturalization certificate or a resident card) in person to the SB. For regional offices, the HR representative may conduct this verification and forward it to the SB. (i)

  On the basis of the DFS review of the applicant's security forms and credit and criminal history, DFS will determine the individual's eligibility for interim access and will indicate

Contractors Requiring Building Access to NRC Facilities (G) (continued)

approval or disapproval to the sponsoring office, pending completion of the required preliminary security checks and final adjudication by GSA. (ii)

- Final Approval or Denial (b)

  Final unescorted building access approval will be granted under one of the following conditions:

  – After completion of the required GSA background investigation and a favorable determination, the individual's unescorted access to NRC facilities will be granted. (i)

  – As determined by DFS, the individual possesses a valid NRC access approval, security clearance, or equivalent investigation conducted by an authorized Federal investigative agency (the investigation must be within the most recent 5 years). (ii)

- Reinvestigation (c)

  This approval is valid for 5 years from the date of the notification letter to the requester, provided that the individual remains employed by the same employer and under the contract, MOU, IAA, or similar arrangement. In accordance with GSA requirements, each individual who is approved for unescorted building access must be recertified every 5 years from the date of the initial approval and each subsequent reinvestigation. (i)

  Ninety days before the expiration of the initial approval, and each subsequent recertification, the contractor will submit a GSA Form 176, "Statement of Personal History," and two FD 258s to DFS, through the NRC Headquarters or regional project officer, for each individual who requires reinvestigation. With timely application and in the absence of any adverse

Contractors Requiring Building Access to NRC Facilities (G) (continued)

information, the individual will maintain unescorted building access pending reinvestigation. If the contractor fails to submit a timely application, unescorted building access approval will expire at the end of the 5-year period and the individual will be denied admittance to NRC facilities. (ii)

- Resolving Questions of Eligibility (d)

  Any questions regarding the individual's final eligibility for continuous unescorted building access to NRC facilities on the basis of the GSA investigation will be resolved directly between the individual and GSA.

A contractor employee or other individual requiring unescorted building access shall not be provided unescorted access to NRC facilities until he or she is approved for interim or final access in accordance with these procedures. (3)

NRC Project Managers may be issued a security infraction, in accordance with the procedures described in MD 12.1, for situations in which contractors under their control do not follow the access procedures of this management directive. Examples may include situations in which a contractor requires access for more than 30 days and does not receive access approval from DFS or situations in which a contractor is denied access and is subsequently escorted into the building for work. (4)

Any exception to the requirements of this section requires the approval of the Director of DFS. Examples may include the need to escort contractors to work within NRC spaces for more than a period of 30 days or situations in which escort requirements could be relaxed if the escort would be subjected to hazardous conditions. (5)

Investigations (H)

The hiring or employing office, in concert with HR and DFS, shall determine the position sensitivity for NRC employees, applicants for employment, consultants, experts, and panel members, using the criteria specified in Section (B) of this part, before requesting access authorization for these individuals. The access authorization or similar access approval level or type of investigation required for NRC contractor and subcontractor employees will usually be determined on the basis of their classified access requirements, their need for unescorted access to nuclear power facilities, their access to SGI, access to NRC IT systems or sensitive information, or unescorted access to NRC Headquarters or regional office facilities. (1)

In lieu of an OPM investigation and report, NRC may accept an investigation for a position of high public trust from another Federal Government department or agency that conducts personnel security investigations (current within the most recent 5 years), provided that an equivalent investigation and access authorization has been granted to the individual by another Government agency on the basis of such an investigation and report. (2)

Reciprocity of "Q" and "L" Access Authorization (I)

An NRC "Q," "L," and an "L(H)" access authorization may be granted by NRC if a pre-existing equivalent investigation is less than 5 years old and of the required level for the clearance requested. A current SF 86 or SF 86C is also required. (1)

Except when an agency has substantial information indicating that an employee may not satisfy the eligibility standards for an access authorization, background investigations and eligibility determinations conducted by other competent Federal authorities shall be accepted. (2)

Reopening of Cancelled Cases (J)

For any requests that are cancelled before the investigation is completed, and more than 90 days have elapsed since the security forms originally submitted were signed, the individual will be required to update a copy of the forms and re-sign and date the forms so that they may be submitted for investigation.

Pre-appointment Investigation Waiver With No Access to Classified Information (K)

The DEDM is authorized to approve the employment of an individual before completion of the security investigation and the reports required by Section 145b of the AEA. This authority may not be redelegated and is limited to situations in which the individual will not have access to classified information. Also, there must be an affirmative recommendation from the Director of DFS and a clear need shown by the requesting organization to use the services of that individual during the required investigation. In the event there is more than one applicant, a separate letter for each applicant must be submitted. (1)

A request for a pre-appointment investigation waiver (Exhibit 2) must be forwarded to HR for evaluation and processing, with the exception of waivers involving OIG. If concurred in by HR and the Director of DFS, HR will forward the request to the DEDM for approval or disapproval. OIG will forward a request for a pre-appointment investigation waiver to DFS. If concurred in by DFS, OIG may send the request directly to the DEDM for approval or disapproval. All waivers must— (2)

- Be requested by the office director or the deputy office director for headquarters personnel or by the regional administrator or deputy regional administrator for regional personnel. (a)

- Be justified by indicating that a serious delay or interference to an essential NRC operation or program will occur unless the individual is employed with a waiver as soon as possible. (b)

Pre-appointment Investigation Waiver With No Access to Classified Information (K) (continued)

- Indicate that administrative controls will be established to ensure that the individual will not have access to classified National Security Information (NSI) or Restricted Data (RD) until the appropriate access authorization is granted. (c)

- Be concurred in by the Director or Deputy Director of HR, the Director of DFS, and if regional personnel are involved, the Regional Personnel Officer. (d)

HR and DFS shall process all Section 145b requests in accordance with Exhibit 3 of this handbook. HR or the RPO, when applicable, must provide DFS with the results of pre-employment checks conducted on NRC applicants who are being considered for employment under Section 145b. (3)

An exception to personal reference checking for consultants or experts may be recommended to the Director of HR by the office director or the regional administrator in those cases in which the consultant or expert is known to be highly regarded and respected in the professional community. This recommendation must be reflected in the Section 145b request (Exhibit 2). (4)

In the case of students being considered for temporary summer appointments, personal reference checking must be conducted in accordance with the procedures specified in Exhibit 3. (5)

Circumstances Affecting Eligibility For Access Authorization (L)

When a person who possesses or is being processed for NRC access authorization, unescorted access to nuclear power facilities, access to SGI, or access to NRC IT systems or sensitive information, or unescorted building access to NRC facilities is hospitalized or otherwise treated for an illness or mental condition

Circumstances Affecting Eligibility For Access Authorization (L) (continued)

that may cause a defect in the person's judgment or reliability, the person's employer (i.e., in the case of an NRC employee, the employee's office director, regional administrator, or other designated official) shall promptly report the circumstances to the Director of DFS. (1)

In the case of contractor personnel, the circumstances must promptly be reported to the Director of DFS by the contracting officer, the security officer, or other person so designated. (2)

The reporting requirements of Sections (N)(1) and (2) of this part do not relieve an individual from the requirement to report to DFS his or her arrest as required by the QSP (SF 86), the security acknowledgment (NRC Form 176), or other form signed by the individual. The arrest must be reported within 5 workdays. (3)

Other circumstances that may affect a person's initial or continued eligibility for NRC access authorization, employment clearance, unescorted access to nuclear power facilities, access to SGI, or access to NRC IT systems or sensitive information are listed in 10 CFR 10.11. These matters must also be promptly reported to the Director of DFS by the person's designated employment official. (4)

Individuals are encouraged and expected to report any information that raises doubts as to whether another individual's continued eligibility for access to classified information is clearly consistent with the national security. (5)

NRC employees and designated management officials are encouraged to seek information and assistance available from the NRC Employee Assistance Program Manager concerning issues that may affect an individual's eligibility for security clearance, including sources of assistance about financial matters, mental health, and substance abuse. NRC contractor personnel and others may seek assistance from similar financial, health, and substance abuse organizations in the local community. (6)

Determination of Eligibility for Access Authorization (M)

Except as provided for in Section (P) of this part, an NRC "L," "L(H)," or "Q" access authorization shall be granted only to employees and contractors who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. The determination of eligibility for access authorization will be consistent with 10 CFR Part 10. (1)

Applicants for NRC security clearances at the "L," "L(H)," or "Q" level will be required to sign an SF 312, "Classified Information Nondisclosure Agreement," before the granting of the security clearance. (2)

The SF 312 is executed in accordance with Executive Orders (E.O.s) 12958 and 12968 and 10 CFR 25.23 and 95.33. The SF 312 is an agreement between the United States and an individual who is cleared for access to NSI. Before an individual is granted a security clearance, he or she shall attend a security briefing and execute an SF 312. The term "individual" refers to all NRC employees, contractors, licensees, and those who the Commission deem as needing access to classified information requiring an NRC access authorization. Those requiring a badge will be issued one indicating the level of access granted after they sign the SF 312. (3)

Temporary Access To Classified Information (N)

Only the Commission may grant an interim access authorization for access to RD. (1)

Temporary Access To Classified Information (N) (continued)

Requests for temporary access to classified information must be forwarded to DFS in the same manner as requests for access authorization and must include the forms and information specified in Section (C) of this part. These requests also must include a justification from the NRC sponsoring office that a serious delay or interference in an operation or project essential to an NRC program may be experienced unless the designated individual is granted immediate access to classified information. (2)

HR or the RPO, as appropriate, must provide DFS with the results of the pre-employment checks on NRC applicants who are being considered for interim access authorization (see Exhibit 3 for the scope of the required pre-employment checks). (3)

If DFS's evaluation of the information developed on an applicant is unfavorable, DFS will inform the requester of its determination in the matter and, if applicable, HR. (4)

Access Authorization for Dual Citizens (O)

A dual citizen, that is, a U.S. citizen who is also a citizen of another country, or non-U.S. citizens may be processed for an "L," "L(H)," or "Q" access authorization when the need is adequately supported and investigative coverage in the United States can be obtained for the immediate 10-year retrospective period.

Access Authorization for Non-U.S. Citizens (P)

As provided for in E.O. 12968, where there are compelling reasons in furtherance of the NRC's mission, individuals who possess a special expertise may, at the discretion of the EDO or the DEDM, be granted an NRC "L," "L(H)," or "Q" access

Access Authorization for Non-U.S. Citizens (P) (continued)

authorization with access to classified information limited to the specific programs, project, contracts, licenses, certificates, or grants for which there is a need for access. Such individuals shall not be eligible for access to any greater level of classified information than the U.S. Government has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only if the previous 10 years of the subject's life has been within the United States and can be appropriately investigated. This clearance will only be valid at the NRC as specified in E.O. 12968, Section 2.6. (1)

An interview with the applicant will be conducted and include the applicant's— (2)

- Statement and disclosure of national allegiance. (a)
- Intent as to permanent residence in the United States. (b)
- General attitude toward the United States vis-a-vis the country of the applicant's current citizenship. (c)
- For dual citizens, eligibility and intention to maintain dual citizenship. (d)
- Previous civilian or military service with a foreign government. (e)
- Family or other relatives abroad or employed by a foreign government. (f)
- The names and addresses of U.S. citizens who can furnish information as to the applicant's background and activities outside the United States. (g)

A verbatim transcript or detailed summary of the interview will be maintained and provided to the applicant upon request. (3)

Access Authorization for Non-U.S. Citizens (P) (continued)

If DFS concludes that adequate support exists to initiate the investigation, the pertinent record will be forwarded to the investigation agency. An SSBI will be required for an "L" or "Q" access authorization. (4)

If DFS concludes that there are significant issues in the case that will require further review, the NRC sponsor will be informed. (5)

Personnel Reporting Responsibilities (Q)

Information not previously reported to the SB and bearing on an individual's continued eligibility for access to NRC facilities, material, or classified information must be reported to the SB by the individual within 5 working days unless noted otherwise. Employees are required to comply with the reporting responsibilities set forth in this management directive. Employees are encouraged and expected to report promptly any information on themselves or others that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security. Reportable information includes but is not limited to—

- Use of intoxicating beverages habitually to excess without evidence of rehabilitation or reformation or being hospitalized or treated for alcohol abuse. (1)

- Use of, trafficking in, sale, transfer, or possession of a drug or other substance listed in the Schedule of Controlled Substances, U.S. Drug Abuse Regulation and Control Act of 1970, as amended (except as prescribed by a physician licensed to dispense drugs in the practice of medicine), without evidence of rehabilitation or reformation. (2)

- Commission of, attempted commission of, or conspiracy to commit any act of sabotage, treason, or sedition. (3)

Personnel Reporting Responsibilities (Q) (continued)

- Holding membership in, with the intention of furthering the aims of, and actively participating in any foreign or domestic organization or group that advocates the commission of illegal acts by force or violence. (4)

- Advocating or participating in the activities of a group or organization that has as its goal revolution by force or violence to overthrow the Government of the United States, or the alteration of the form of the Government of the United States by unconstitutional means, with the knowledge that such support will further the goals of the group or organization. (5)

- Renouncing U.S. citizenship or representing a foreign nation in activities that may be contrary to the national security of the United States. (6)

- Parent(s), brother(s), sister(s), spouse, or offspring assuming residence in a nation whose interests may be adverse to the interests of the United States, or in satellite states or occupied areas thereof. (7)

- Observing or having knowledge of another individual who willfully violates or disregards security or safeguards regulations. (8)

- Refusing to testify before a congressional committee, a Federal or State court, or a Federal administrative body regarding charges relevant to eligibility for NRC security access authorization. (9)

- Engaging in any conduct or being subject to any circumstances that tend to show the individual is not reliable, honest, or trustworthy and without evidence of reformation. (10)

Personnel Reporting Responsibilities (Q) (continued)

- Any criminal conduct that indicates a history or pattern of criminal activity that creates doubt about a person's judgment, reliability, or trustworthiness. This category includes any allegations or admissions of criminal conduct regardless of whether the person was formally charged. (11)

- Being hospitalized or entering an institution for the treatment of a mental or emotional problem, or otherwise being treated for a mental illness or other such condition that may cause a significant defect in judgment or reliability. (12)

- Any employment or association or change in employment or association with a foreign or foreign-owned interest or representatives. (13)

- Contact with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information. (14)

- Effort by any individual to obtain or gain unauthorized access to classified information or special nuclear material (SNM). (15)

- Any financial considerations that indicate an inability or an unwillingness to satisfy debts, not meeting financial obligations, and financial problems linked to gambling, drug abuse, alcoholism, or other issues of a security concern. (16)

- Individuals who marry or cohabitate in a spouse-like relationship after they have submitted an SF 86 shall furnish DFS with an original NRC Form 354, "Data Report on Spouse." (17)

Reinvestigation Program (R)

The NRC reinvestigation program is designed to ensure the continued eligibility for access authorization of individuals employed by the NRC. The program applies to all those who possess "Q," "L(H)," or "L" access authorization, including NRC employees, consultants, experts, panel members; former Chairman and Commissioners who retain their clearances after terminating their employment when continued access to classified information is required in the conduct of the agency's activities; congressional staff members cleared by NRC; employees and consultants of NRC contractors; and all others who possess an NRC access authorization. DFS must reevaluate the continued eligibility of those individuals cleared. (See Exhibit 4 for "Q" and "L" reinvestigation requirements.) (1)

DFS will initiate a reinvestigation every 5 years for "Q" and "L(H)" (high public trust) clearances and every 10 years for "L" clearances. DFS will notify the individuals who are to be reinvestigated and the dates by which they are to complete the security forms packet. DFS will advise the former Chairman and Commissioners who have retained their NRC security clearances, congressional staff members, and contractor organizations directly. (2)

Each individual must complete the security forms packet and return it to the SB, DFS, by the specified date. Contractor personnel should return forms through their security office. If the contractor fails to submit forms by the specified date, the NRC security clearance or access for contractor personnel may be administratively terminated. (3)

Upon favorable review of the investigation, DFS will provide the Official Personnel File (OPF) file center with a copy of the certification of investigation to be retained in the employee's personnel file. (4)

Termination of Access Authorization (S)

Access authorization will be terminated and a security termination statement (NRC Form 136) must be signed when— (1)

- An NRC employee, consultant, or contractor is separated from employment with NRC. (a)
- In the case of a non-NRC employee, an individual is separated for a period of 30 days or more from activities for which he or she was granted an access authorization. (b)
- Access authorization is no longer required. (c)

Upon the voluntary or involuntary separation (e.g., death) from employment or revocation of clearance of a person who holds an NRC access authorization, the employing office at headquarters or the regional office or facility (e.g., an NRC contractor) must as a minimum— (2)

- Provide prompt notification of the termination of employment to SB/DFS. (a)
- Ensure that all classified and sensitive unclassified documents charged to the person are accounted for and properly disposed of. (b)
- Arrange for the immediate return of badges, passes, and other forms of official identification to the responsible NRC security point of contact. (c)
- Notify DFS to remove the individual's name from all access lists. (d)
- Ensure that combinations are changed to which the person had access. (e)

Termination of Access Authorization (S) (continued)

- Arrange for the person's name to be removed from access permissions to critical or sensitive areas, such as telephone closets and computer rooms. (f)

Upon completion of a security termination statement, the signed copy of the security termination statement must be forwarded to SB/DFS. DFS will retain the statement. (3)

In the case of the disability of a person when it is apparent that the disability will render the individual unable to perform his or her duties for at least 6 months, prompt notification must be made to DFS and measures similar to those specified in Section (T)(2)(b) through (f) of this part must be employed. (4)

Termination of Employment in the Interest of National Security (T)

The DEDM may suspend or revoke a security clearance when suspension or revocation is considered to be in the best interest of national security in accordance with 5 U.S.C. 7532. (1)

The criteria set forth in 10 CFR 10.11 must be followed to determine whether an action should be taken under 5 U.S.C. 7532. (2)

When a hearing is held under 5 U.S.C. 7532, the NRC's “Procedures for the Conduct of Hearings Under 5 U.S.C. 7532" (Exhibit 5) must be used. (3)

Termination of Contractor Unescorted Building Access, IT Access, Power Reactor Access, and SGI Access (U)

The NRC sponsoring office or project officer must immediately notify DFS in writing when a contractor employee no longer requires unescorted access to nuclear power facilities, access to SGI, access to NRC IT systems or sensitive information, or unescorted access to NRC Headquarters or regional office facilities.

Part II
Control of Visits Involving Classified Information

Introduction (A)

Standards and procedures are given for the protection of classified information involved in the course of visits to NRC, or visits by NRC employees and NRC contractors to other Government agencies and contractors.

General (B)

Before disclosing classified information to any visitor, individuals must confirm the visitor's identity, need-to-know, and level of access authorization. (1)

NRC or contractor officials (e.g., supervisors) must ensure that visit requests are submitted early enough for timely processing and notification of the person or facility to be visited. (2)

Continuing visit approval for 1 year or less may be granted for repeated visits to NRC, the Department of Energy (DOE), or other facilities. A single visit request form may be used if the repeated visits are to the same facility and involve the same individuals, the same level of classified information (e.g., Secret), and the same type of classified information (e.g., Restricted Data [RD]). (3)

Visit requests of an unusual or emergency nature for which timely notification cannot be given may be transmitted to the NRC Division of Facilities and Security (DFS), Office of Administration, by facsimile or telephone. Telephone arrangements must be immediately confirmed with DFS in writing. Visit requests that are not in writing or that do not provide timely notification may not be accepted at some facilities. (4)

General (B) (continued)

Classified information must not be given to NRC employees or other individuals who possess an NRC red (no access) badge. (5)

Access to classified information other than that authorized in the visit request must not be granted, regardless of the level of access authorization stipulated for the visitor. (6)

The NRC office, NRC contractor, or other NRC activity visited shall establish appropriate administrative controls over the movement of approved visitors to ensure that they are given access only to the classified information authorized. (7)

Neither classified nor unclassified naval nuclear propulsion information may be disclosed to individuals who are not U.S. citizens or to others not authorized access to this information. (8)

If appropriate, the visitor should confirm in advance with the facility to be visited that necessary approvals have been received. (9)

Access to RD requires a "Q" or "L" access authorization, depending on the classification level of the RD, except as provided in Section (D)(1) of this part. (10)

Requests for visits to NRC offices or divisions, except as indicated in Section (C)(1)(a) of this part, to NRC contractors, to other NRC facilities, or to other Government agencies involving classified information must be requested on NRC Form 277, "Request for Visit," or in an appropriate written request containing the following information: (11)

- Identity of each visitor, including full name, social security number, citizenship, date of birth, and organization with which affiliated. (a)

General (B) (continued)

- Specific information to which access is requested, including the classification level and type of information, for example, RD or National Security Information (NSI). (b)

- Access authorization level ("Q", "L", Top Secret, Secret, or Confidential) and the need-to-know of each person certified by an appropriate official. (c)

- Purpose of the visit. (d)

- Name and location of facility(ies) to be visited. (e)

- Anticipated dates of visit and names of persons to be visited. (If a conference is involved, provide the date, place, and sponsor of the conference.) (f)

- Name, title of position, organization, and telephone number of the person who prepared the request. (g)

- Requests for visits to NRC, NRC contractors, or other NRC facilities by individuals outside NRC should be faxed to (301) 415-5364 or sent to the following address: (h)

  U.S. Nuclear Regulatory Commission
  Chief, Security Branch
  Division of Facilities and Security
  Washington, D.C. 20555-0001

Classified notes or other classified records must not be released to a visitor to take outside the facility without the express permission of the person visited. If the visit is in connection with a conference or other such activity, the express permission of the person responsible for the activity must be obtained. Also, records so released must be protected in accordance with Management Directive (MD) 12.2, "NRC Classified Information Security Program." (12)

Outgoing Visits by NRC (C)

For visits to NRC Headquarters and regional offices, a request for visit or access approval (NRC Form 277) is not necessary. The employee's NRC photo-identification badge will serve to identify the employee and the access authorization held. A blue badge signifies a “Q” access authorization and a yellow badge an “L.” A red photo-identification badge allows access to sensitive unclassified information, that is, OUO, SGI, Proprietary, with a need-to-know and signifies no access authorization for classified information has been granted to the employee. (1)

For visits to NRC contractors, licensees and their related facilities, and to other Government agencies or their contractors, NRC employees should submit an NRC Form 277 to DFS at least 7 working days before the initial date of the visit. When acting as representatives of the Federal Government in their official capacities, NRC employees such as regional inspectors, OI and OIG investigators, and OIG auditors may visit a contractor or licensee facility without furnishing advance notification, provided these employees present appropriate NRC credentials upon arrival. (2)

Access to weapons data, sensitive nuclear material production information, inertial fusion data, advanced isotope separation technology, uranium enrichment technology, or naval nuclear propulsion information requires special processing and approval by DOE. For this reason, an NRC Form 277 should be submitted to DFS at least 15 working days before the initial visit date. (3)

For visits to facilities performing work on naval reactors for DOE, an NRC Form 277 should be received at least 15 working days before the initial visit date, especially for visits that do not involve inspections. (4)

DOE requires that NRC submit the NRC Form 277 15 days before the first day of the visit. (5)

Outgoing Visits by NRC (C) (continued)

For visits to facilities other than NRC, an NRC Form 277 or other written request for visit or access approval should be approved by the NRC office or division sponsoring the contract for certification of the individual's need-to-know, then submitted to DFS for verification of access authorization. DFS forwards the visit request to the facility to be visited. At those contractor or licensee facilities at which NRC is not the cognizant security authority (CSA), the visit control procedures of the CSA shall be followed. (6)

Requests to visit NRC offices should be submitted directly to DFS at least 7 working days before the initial date of the visit. (7)

Requests for visits to facilities performing work on naval reactors for DOE should be received by the NRC sponsoring office or division at least 15 working days before the initial visit date. (8)

NRC consultants who plan to visit NRC employees directing or monitoring their consultant interests will not be required to submit an NRC Form 277. The person visited must confirm the NRC consultant's need-to-know and required access authorization level before classified Information is disclosed to the visitor. (9)

Incoming Visitors (D)

NOTE: NRC DOES NOT ACCEPT INTERIM CLEARANCES

Required Information (1)

As a minimum, the information required for incoming visitors should include the full name of the visitor, the agency affiliation, the purpose of the visit, the date of the visit, the name of the person to be visited, and the type of access required.

Restricted Data (2)

RD in the possession of NRC, its contractors, or in NRC facilities must not be released to an individual unless he or she has the

Incoming Visitors (D) (continued)

Restricted Data (2) (continued)

appropriate NRC or DOE access authorization and the need for access has been properly certified by the security office.

National Security Information (3)

Classified information (NSI), other than RD, may be furnished to individuals when they have the required access authorization and their need for access is confirmed by the NRC security office to be visited.

Other Classified Information (4)

For incoming visitors requiring access to classified information, including RD, a memorandum signed by a security office representative from the requesting agency should be submitted to DFS for processing and approval by the NRC activity involved.

Representatives of Other Agencies (5)

If authorized by the Director of DFS, representatives of other agencies (e.g., the Federal Bureau of Investigation or the Office of Personnel Management) acting in their official capacities may be granted access to classified information upon presentation of proper credentials. In case of doubt about identity or the level of access authorized, DFS will verify these credentials or the level of access by contacting a security official of the agency or activity involved.

Members of Congress and Congressional Staff (6)

Visits to NRC, NRC contractors, or other activities associated with the NRC program involving access to RD or other classified information by members of Congress may be approved by directors of headquarters offices or divisions, or by regional administrators. The identity of the visitors and their need-to-know

Incoming Visitors (D) (continued)

Members of Congress and Congressional Staff (6) (continued)

must be established by the responsible congressional official. The proposed visit must be coordinated with the Director of DFS to certify access authorization and with the Director of the NRC Office of Congressional Affairs.

Immigrant Aliens Admitted to the United States for Permanent Residence (7)

Visit requests for immigrant aliens who possess security clearances will be handled in accordance with the procedures specified in this section.

Visits Involving Access to Sensitive Compartmented Information (E)

Visitors to the NRC must have their Sensitive Compartmented Information (SCI) access authorization and need-to-know forwarded to the Special Security Officer in the Office of Nuclear Security and Incident Response (NSIR). As a minimum, the information required for these visits should include the full name of the visitor, the agency affiliation, the purpose of the visit, the date of the visit, the name of the person to be visited, and the SCI compartments involved. This information may be provided by secure fax, telephone by a known or verifiable Special Security Officer of the agency or department requesting the visit, or by memorandum. If access to classified information other than SCI is involved, the need for this access must be certified and the required access authorization must be verified. (1)

NRC employees visiting other Government agencies or departments, or their contractors, shall contact the Special Security Officer in NSIR to have their SCI access authorization properly forwarded to the agency to be visited. A request for access to classified information other than SCI may be included

Visits Involving Access to Sensitive Compartmented Information (E) (continued)

with the request for SCI or may be processed separately in accordance with the procedure specified in this part. (2)

Visits by Foreign Nationals Sponsored by Foreign Governments or International Organizations (F)

Requests for foreign nationals to visit NRC, NRC contractors, or other activities associated with the NRC program must be forwarded to the Director of DFS. Any security assurance the foreign nationals may possess must be officially certified to DFS by an authorized official of the foreign government sponsoring the visit, with the assistance of the Office of International Programs (OIP), if necessary. If the foreign nationals do not possess security assurance, OIP shall request DFS to conduct investigative checks. For further guidance on the disclosure of classified information to foreign nationals, refer to MD 12.2. (1)

Representatives of the International Atomic Energy Agency (IAEA) who are authorized to make visits to or inspect NRC-licensed facilities in accordance with the U.S./IAEA Safeguards Agreement may be authorized access to classified information, except for RD, on the basis of a DFS-issued disclosure authorization letter (DAL). The DAL will specify the names of the IAEA representatives and the classified information authorized, in addition to other relevant information. For further guidance on the disclosure of classified information to IAEA representatives, refer to MD 12.2. (2)

Visits to Foreign Governments or Activities by NRC Personnel (G)

For visits to foreign governments or activities by NRC personnel, an NRC Form 277 should be submitted to DFS for processing and coordination with OIP when classified information is involved. If an

Visits to Foreign Governments or Activities by NRC Personnel (G) (continued)

NRC Form 277 is not available, the information listed under Section (B)(12) of this part should be submitted to DFS. (1)

These visit requests should be submitted at least 30 days in advance of the initial visit date. (2)

Records of Visit Requests (H)

Records of visit requests consisting of the NRC Form 277 or its equivalent and any related correspondence must be retained for 2 years after the expiration date of the visit authorized by the requesting office and the office of the facility visited.

Part III
Assignment of Foreign Regulatory Employees to NRC

Introduction (A)

Guidelines are given for the prevention of unauthorized access to classified information or sensitive unclassified information by foreign regulatory employees assigned to the NRC. The responsibilities of the Office of International Programs (OIP), the Division of Facilities and Security (DFS, Office of Administration), supervisors, and employees also are specified in this part.

Activity Plans (B)

OIP, in cooperation with DFS, will establish and coordinate the assignee program and individual assignee activity plans that enumerate the variety of activities in which the assignee is expected to participate.

Assignments (C)

Consideration for assignments will be given in the following order of priority: (1)

- Nationals from developing countries building or operating U.S.-type light-water reactors. (a)

- Nationals from other countries with which NRC has entered into information exchange and cooperation arrangements. (b)

- Nationals from the International Atomic Energy Agency (IAEA) member states sponsored under the IAEA Fellowship Program, if different from Sections (C)(1)(a) and (b) of this part. (c)

Assignments (C) (continued)

- Other foreign nationals as decided on a case-by-case basis. (d)

Within each of these categories, preference will be given, in general, to nationals from countries party to the Treaty on the Non-Proliferation of Nuclear Weapons. Foreign nationals actively engaged in unsafeguarded nuclear activities in non-nuclear weapons states will not normally be selected. (2)

All personnel accepted for NRC assignments of generally not less than 6 months should—(3)

- Be fluent in English. (a)

- Have successfully completed an NRC-approved English language foreign competency examination. (b)

- Have professional training, experience, or education. (c)

- Be certified as regular employees of either their national regulatory agencies or of other institutes or organizations responsible for performing domestic regulatory and safety functions. (d)

The sponsoring government, institute, or other organization must bear all costs associated with the assignment, including, but not limited to, the assignee's salary, travel, and per diem. Any questions about costs should be referred to OIP. Assignees should be largely self-sufficient after orientation in order to minimize the impact on the NRC staff. Personal services such as assistance with housing and other orientation briefings will be handled by the embassy of the assignee's country or by local representatives of his or her institution. Assignees will normally be given duties similar to those of NRC employees, without special “diverse experience” assignments, except when convenient to NRC. (4)

Assignments (C) (continued)

OIP must notify the Commission promptly whenever an application from a sensitive country is received to allow the Commission the opportunity to request any action they believe necessary while the staff is attempting to arrange placement and before any commitment is made. Another notification to the Commission must be prepared as soon as details of the proposed assignment are confirmed within the staff and at least 1 full week before the assignment is formally approved. Special care must be taken in regard to security considerations in selecting and screening foreign nationals, placing them within the staff, monitoring them closely, and educating their supervisors and co-workers. (5)

OIP shall forward all formal NRC letters of invitation accepting proposed assignments through State Department channels in conformance with and in furtherance of U.S. laws, regulations, and policy directives and objectives. Letters of invitation must be countersigned and returned to OIP 4 weeks before the assignee's expected arrival at NRC. (6)

OIP approves or disapproves the assignment of a foreign national to NRC and designates the office to which the foreign national will be assigned, subject to the concurrence of the cognizant office director or regional administrator and DFS. (7)

Foreign nationals will not be assigned to the Commission, to the Office of the Secretary, to the Office of the Executive Director for Operations, to office directors, or to offices in which classified information or other sensitive information is often in use. Generally, assignments will not be made to branches in which large amounts of classified or other sensitive unclassified information is processed or stored, or to areas near these branches. (8)

Background Check (D)

Before inviting the foreign regulatory employee to join NRC, OIP will obtain the required background and biographical data and

Background Check (D) (continued)

submit them to DFS with a request that the appropriate indices check be conducted by the appropriate agencies (the Central Intelligence Agency, the Federal Bureau of Investigation, and the Department of State). Information that creates a question as to whether assignment of the foreign national is consistent with the national interest will be evaluated by DFS and forwarded with a recommendation to OIP.

Assignee Agreements (E)

Foreign assignees will be required to sign a commitment patterned after the agreement signed by the Government contract consultants agreeing not to take any proprietary documents away from their proper place of use and storage and not to disclose proprietary information or otherwise violate the conditions under which NRC staff members receive and use this information. The signing of the confidentiality agreement by the assignee is made a condition of the assignment under the terms of the agency-to-agency agreement that both the NRC and the foreign regulatory agency sign. Specific procedures are as follows:

- The supervisor of an assignee will make a determination of the need for an assignee to have access to proprietary information. A separate determination of need will be made for the proprietary information related to each program area in which the assignee is authorized to work. The supervisor will prepare a note concerning this access and will maintain a listing of documents to which the assignee has access. Whenever work on a program area is terminated, and at the end of each assignment, the assignee will return all proprietary documents. The supervisor of the assignee shall ensure that all documents on the assignee's list are returned. (1)

- Access to special classes of information identified in 10 CFR 2.790(d), including details of facility security plans, material control and accounting information, and Safeguards

Assignee Agreements (E) (continued)

Information that is subject to 10 CFR 73.21, must not be granted unless approved by NSIR. (2)

Security Plans (F)

Representatives from DFS, OIP, and the office to which the foreign employee will be assigned will work together to define the assignment and to develop a security plan for each assignee. This task will be completed before the invitation letter is issued. The host office will be primarily responsible for developing the plan. This plan must be developed and approved before the assignee arrives. Each foreign assignee will be required to read, agree to, and sign the security plan. The plan will require the approval of OIP, the host office, and DFS and must include the following elements: (1)

- Description of the physical location of the assignment within NRC, a licensee facility, or another facility. (a)

- Identification of specific areas to which assignees are to be given unescorted access in order to perform essential responsibilities. (The assignee's access should be consistent with the requirements of DFS and the assignments of the host office.) (b)

- Explanation of special badging required and associated restrictions. (c)

- Explanation of restrictions on the use of, or connection to, NRC computing resources such as local area networks, other NRC computing systems, document management systems, and sensitive data. (d)

- Discussion of the ways in which commercial or foreign proprietary information must be protected if the assignment

Security Plans (F) (continued)

requires access to this information. (Assignments should normally be tailored so that they do not require access to this information.) (e)

- Instructions on alerting co-workers about an assignee's presence and the assignee's restricted access, both physical and informational, including a DFS counterintelligence-type briefing. (f)

- Assignment of a supervisor and an alternate to monitor the assignee's day-to-day activities. (g)

- Requirement for monthly or quarterly progress reports from the assignee. (Copies of the report are to be sent to the supervisor and other appropriate persons in the office to which the foreign national is assigned.) (h)

- Requirement for a mid-point (or more frequent) interview by DFS of the assignee, the assignee's supervisors, and, as appropriate, the assignee's co-workers to ensure that the assignee and supervisors are continuing to comply with the approved security plan. (Any problems will be reported to OIP and any other appropriate office.) (i)

If later experience indicates that the security plan requirements cannot be met, or conditions change that warrant a possible change in requirements, or if any other problems arise, the supervisor will immediately advise OIP and DFS. Any changes in the security plan must be approved by DFS and OIP. (2)

DFS will issue assignees special identification badges. These badges, while allowing assignees unescorted access to specific areas, are prominently marked “Assignee” and are color-coded red for “no access.” Foreign assignees will be required to wear their badges at all times. (3)

Security Plans (F) (continued)

Co-workers and other staff members in the assignee's area also will be made aware of the requirement for the assignee to wear his or her badge at all times. Access by the assignee into other areas not specified in the plan will require that the assignee be escorted by a cleared NRC employee designated by the assignee's supervisor. (4)

The assignee's supervisor will make an initial evaluation of an assignee's work area, as well as a reevaluation at the midpoint of the assignment and at any time the security plan is amended. Any recommendations should be given to DFS for action at this time. (5)

Assignee Responsibilities (G)

Assignees will not authorize visits by other individuals to NRC, NRC contractors, or other NRC facilities. (1)

Assignee duties are to be limited to those that do not require representing NRC in public or acting as an official representative in meetings with NRC licensees. (2)

Assignees will be responsible for obtaining and making whatever copies of records or documents they wish to take with them before completion of their assignments. Assignees will be required to obtain the supervisor's approval before copying these records and will also be required to provide a list of these records to their NRC supervisors, OIP, and DFS. (3)

Evaluation of Assignees (H)

Upon completion of the assignment, OIP will provide an evaluation form to the supervisor. The supervisor shall complete the form and send copies of it to OIP, DFS, and the cognizant office director or regional administrator.

Part IV
Drug Testing Program

NRC's Drug-Free Workplace Plan sets forth objectives, policies, procedures, and implementation guidelines to achieve a drug-free Federal workplace consistent with Executive Order 12564, Section 503 of the Supplemental Appropriations Act of 1987, and Public Law 100-71. NRC's program consists of an Employee Assistance Program, supervisory training, employee education, and drug testing following procedures specified in the Department of Health and Human Services (HHS) Mandatory Guidelines for Federal Workplace Drug Testing Programs. Current HHS Guidelines supersede all previous issues of guidance. (1)

NRC's Drug Testing Program, which is administered by the Security Branch, Division of Facilities and Security, Office of Administration, includes random, applicant, reasonable suspicion, post-accident, voluntary, and followup testing. Employees with access to Sensitive Compartmented Information and/or who require access more than once or twice a year to classified information (e.g., National Security Information or Restricted Data) are subject to random drug testing. Specific policies and procedures are reflected in the NRC Drug-Free Workplace Plan, NUREG/BR-0134, and the NRC Drug Testing Manual, NUREG/BR-0136. (2)

NRC may also conduct drug testing under 10 CFR Part 10 and 11 procedures as drug involvement is an adjudicative concern when making a determination of eligibility for a security clearance/ access authorization. Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information and/or nuclear materials. (3)

Exhibit 1
Security Orientation Briefing for New NRC and Contractor Employees

A security orientation briefing must be given to NRC employees, consultants, and contractors requiring access authorizations when they enter on duty status. This briefing will normally be given by a representative of the Division of Facilities and Security (DFS) or, in a regional office, a regional security representative and will contain the following information:

- The type of security clearances and access approvals granted by NRC and the access those clearances and approvals afford after an official need-to-know has been established. (1)

- Personnel security reporting responsibilities of each individual. (2)

- Prescribed procedures for the storage and handling of classified and sensitive but unclassified information and the importance of protecting this information. (3)

- Physical security aspects of the particular facility, the importance of visitor control, and the names of procedures for protecting Government property. Contractors are not allowed to escort visitors unless prior approval has been granted by DFS. (4)

- Information on where to obtain further guidance or assistance. (5)

Exhibit 2
Format for a Request for a Pre-appointment Investigation Waiver

MEMORANDUM TO: _____, Director
Office of Human Resources

FROM: (Requesting Office Director or Regional Administrator)

SUBJECT: REQUEST FOR EMPLOYMENT APPROVAL PRIOR TO THE GRANTING OF A SECURITY CLEARANCE WHEN ACCESS TO CLASSIFIED MATTER IS NOT INVOLVED

This memorandum relates to the authority vested in the Deputy Executive Director for Management Services (DEDM) for approving employment of an NRC applicant before the completion of the required investigation when access to classified matter will not initially be required.

I request the DEDM's approval to employ the following individual(s) before the completion of the security investigation and report required by Section 145b of the Atomic Energy Act of 1954, as amended. The individual(s) has/have been selected to fill the position(s) indicated. Favorable pre-employment checks have been conducted.

(Name) (Position)

(Provide adequate justification for each request. Justification should not be standardized and should detail why a serious delay or interference with an NRC operation or program will result if the request is not approved. Note: If the request involves interim unescorted access to nuclear power plants for inspectors and resident clerical aides or a recommendation for waiving personnel reference checks for NRC consultants or experts, it should be clearly stated in the justification.)

Administrative controls will be established to ensure that (the individual(s)) will not have access to National Security Information or Restricted Data until he or she is granted an access authorization by the Division of Facilities and Security, Office of Administration.

Exhibit 3
Standard Operating Procedures for Pre-employment Screening of NRC Applicants

The headquarters Human Resources (HR) specialist or the Regional HR Officer will obtain a current résumé or equivalent, and a security forms package (consisting of the SF 86, Parts 1 and 2; two fingerprint charts; and NRC Forms E-1, 176, OF 306, NRC Form 236, and a Section 145b memorandum) from the selectee. The HR specialist or the Regional HR Officer will ensure that appropriate reference checks are conducted using the résumé or equivalent and the SF 86, Part 1, as the source documents. Once the security package is complete, HR will forward it to DFS for processing. (A)

The reference checks will generally follow the format of NRC Form 212, "Qualifications Investigation," plus additional requirements as indicated below. Questions 23, 24, 25, and 26 must be asked of each source. Space is provided on the form for annotations and appropriate comments. Additional pages should be used as needed. (B)

The following additional requirements apply and will be conducted by the hiring office: (C)

- All personnel conducting reference checks must be thoroughly familiar with the NRC Form 212 and reference check techniques. (1)

- Using the résumé, or equivalent, and the SF 86, Part 1, as guides, identify and question employers for at least the past 5 years, where applicable. (2)

- On the basis of the answer to each item or question on NRC Form 212, ask as many followup questions as needed to develop a full response. (3)

- For applicants other than students being considered for temporary summer appointments, reference checks should cover at a minimum the last 5 years. For applicants who do not have 5 years of employment experience, obtain, if possible, references from high school or college sources, as appropriate, to cover at least the past 5 years. For students being considered for temporary summer employment, conduct supervisory reference checks for all jobs held

Exhibit 3 (continued)

during the past 2 years, where applicable. For students who do not have 2 years of employment experience, obtain, if possible, references from school and other sources. In either case, at least two references are required. If any adverse employment or security-related information is noted or developed during processing, the student will be processed in accordance with the normal processing procedures. Summer employees other than students are subject to the normal processing procedures. (4)

- To supplement the education and employment history for applicants other than students being considered for summer employment, develop at least one additional source on the applicant (developed references are not required for students being considered for summer employment). This additional source must not be an individual listed on the OF 612, SF 171, or equivalent or the SF 86 or otherwise provided by the applicant. This source may be developed by asking employers or those responding to education questions if they can name anyone else who has personal knowledge of the applicant. Use NRC Form 212 to obtain the reference from the developed source. (5)

- In all cases, HR will verify dates of attendance at the educational institution, the highest educational level attained, and the type and year of degree. (6)

The HR specialist or the Regional HR Officer will review the results of all the reference checks to determine acceptability of the applicant. If either the HR specialist or the Regional HR Officer has any doubt as to the applicant's acceptability, he or she must discuss whether to proceed with the selecting official. If the decision is to proceed with the applicant, the HR specialist or the Regional HR Officer will certify the acceptability of the security package and will send the complete security forms package, the Section 145b request memorandum, all reference checks, and any other documentation normally required to DFS by overnight mail if from a region or by interoffice mail if from a headquarters office. (D)

Upon receipt of the security package, DFS will— (E)

- Request applicable checks on the selectee. (1)

- Conduct applicable database checks of the selectee. (2)

Exhibit 3 (continued)

- If deemed necessary, contact the selected applicant to discuss in detail the answers provided on the SF 86, as well as any other matters of security concern. (3)

- Evaluate the eligibility of the applicant for a Section 145b employment waiver on the basis of a review of the security package and the results of the applicable checks and the security interview, if conducted, and recommend approval or disapproval. (4)

Exhibit 4
"Q" and "L" Reinvestigation Program Requirements

"Q" and Sensitive Compartmented Information (SCI) Reinvestigation Requirements (A)

For employees, consultants, experts, panel members, former senior NRC officials, contractors and agents of the NRC, and congressional staff members—

- Each individual to be reinvestigated shall submit a new Questionnaire for National Security Positions (QSP, Standard Form 86) and related forms. These forms will be the basis for an investigation as specified below. (1)

- An Office of Personnel Management single-scope background investigation—periodic reinvestigation (SSBI-PR) will be conducted for "Q" cleared individuals other than the Chairman, Commissioners, and the Inspector General, who are subject to a Federal Bureau of Investigation (re)investigation in connection with their Presidential appointment. (2)

- Further investigative coverage may be undertaken on a case-by-case basis if the scheduled coverage is insufficient to obtain the required information. (3)

- Although not normally required for "Q," "L(H)," or "L" reinvestigations, a new set of fingerprint cards may be requested on a case-by-case basis. (4)

"L" Reinvestigation Program Requirements (B)

Each individual to be reinvestigated shall submit a new QSP and related forms. These forms will be the basis for an investigation as follows:

- A national agency check with law and credit (NACLC) shall be conducted. The investigation may be expanded as necessary to determine if access is clearly consistent with national security. (1)

- Further investigative coverage may be undertaken on a case-by-case basis if the scheduled coverage is insufficient to obtain the required information. (2)

Exhibit 5
Procedures for the Conduct of Hearings Under 5 U.S.C. 7532

Purpose of the Procedures (A)

The procedures set forth below are established for the conduct of hearings pursuant to 5 U.S.C. 7532 to determine whether an individual's continued employment with NRC is clearly consistent with the national security. Guidance is provided in 10 CFR 10.10 and 10.11 as to the types of information that raise questions concerning the consistency of an individual's employment and the national security.

Notification to Individual of Hearing (B)

A notification letter providing the date, hour, and place of the hearing and the identity of the hearing official will be presented to each individual who has requested a hearing. Where practicable, this letter will be presented to the individual in person at least 10 days in advance of the hearing, which will be scheduled with due regard for the convenience and necessity of the parties. The letter will be accompanied by a copy of these procedures and other administrative instructions, as necessary. (1)

The individual will have the right to appear personally before the hearing official and present evidence on his or her behalf through witnesses or by document or both, and may call, examine, and cross-examine witnesses. The individual may be present during the hearing to the extent permitted by national security concerns. The individual may be accompanied, represented, and advised by counsel or other representatives of his or her own choosing. In this case, the individual shall file with the Deputy Executive Director for Management Services (DEDM) a document designating the attorney or representative and authorizing him or her to receive all correspondence pertaining to the hearing. (2)

NRC Hearing Counsel (C)

The NRC hearing counsel assigned shall, before the scheduling of the hearing, review the information in the case and shall request the presence of witnesses and the production of documents and other physical evidence relied upon in suspending the individual pursuant to the provisions of 5 U.S.C. 7532. When the presence of a

Exhibit 5 (continued)

witness and the production of documents and other physical evidence are deemed by the hearing counsel to be necessary or desirable for a determination of the issues, the Director of the Division of Facilities and Security (DFS), Office of Administration, shall make arrangements for the production of this evidence and for the witnesses to appear at the hearing by subpoena or by other means. (1)

The hearing counsel is authorized to communicate directly with the individual's counsel or representative, or the individual if the individual is not so represented, for purposes of mutually agreeing upon arrangements for expeditious hearing of the case. (2)

The individual is responsible for producing witnesses on his or her own behalf and presenting other evidence before the hearing official to support his or her position. The hearing counsel may at his or her discretion request the Director of DFS to arrange for the issuance of subpoenas for witnesses to attend the hearing on the individual's behalf or for the production of specific documents or other physical evidence, provided the necessity for this assistance has been shown. (3)

Appointment of Hearing Official (D)

NRC shall appoint a hearing official from a list of qualified attorneys possessing the highest degree of integrity, ability, and good judgment. To qualify, an attorney must have an NRC “Q” access authorization. No hearing official will be selected who has knowledge of the case or of any information relevant to the disposition of the case, or who for any reason would be unable to issue a fair and unbiased recommendation.

Prehearing Proceedings (E)

Before the hearing, the hearing official will be furnished the record in the case, consisting of the statement of charges and any associated amendment(s), the request for the hearing and the notice of hearing if it has been issued, and any agreements between the individual and the hearing counsel. (1)

The parties will be notified by the hearing official at least 10 days in advance of the hearing of the date, hour, and place of the hearing. The hearing official may order postponements or continuances from time to time for good cause shown. If, after

Exhibit 5 (continued)

due notice, the individual fails to appear at the hearing, or appears but is not prepared to proceed, the hearing official shall, unless good cause is shown, return the case to the DEDM, who shall make the final determination on the basis of the information in the NRC's possession. (2)

Conduct of Hearing (F)

The hearing official shall conduct the hearing in an orderly, impartial, and decorous manner. Technical rules of evidence may be relaxed so that a full evidentiary record may be made based on all material and relevant facts. (1)

The proceedings will be open only to duly authorized NRC staff representatives, the individual, his or her counsel or representative, and those persons as may be officially authorized by the hearing official. Witnesses shall not testify in the presence of other witnesses except that the hearing official may, at his or her discretion, allow for expert witnesses to be present during testimony relevant to their own testimony. (2)

Witnesses, including the individual, shall be examined under oath or affirmation by the party who called them and may be cross-examined by the other party. The hearing official will rule on all evidentiary matters, may further examine any witness, and may call for additional witnesses or the production of documentary or other physical evidence if, in the exercise of his or her discretion, this additional evidence is deemed necessary to the resolution of an issue. (3)

If it appears during the hearing that Restricted Data or National Security Information may be disclosed, the hearing official shall ensure that disclosure is made only to persons authorized to receive it. (4)

The hearing official may permit the hearing counsel to amend the statement of charges to add or modify charges to be considered at any time during the hearing. In the event of such an amendment, the individual shall be given an opportunity to answer the amended charges. If the changes are of such a substantial nature that the individual cannot answer the amended charges without additional time, the hearing official shall grant such additional time as he or she deems necessary. (5)

Exhibit 5 (continued)

The hearing official may receive and consider evidence in the form of depositions or responses to interrogatories upon a showing that the witness is not available for good reason, such as death, serious illness, or similar cause, or in the form of deposition, interrogatories, affidavits, or statements with agreement of the parties. The hearing official may take official notice at any stage of the proceeding, where appropriate, of any fact not subject to reasonable dispute in that it is either generally known within the United States or capable of accurate and ready determination by resorting to sources whose accuracy cannot reasonably be questioned. A party is entitled, upon timely request, to an opportunity to be heard as to the propriety of taking such official notice. In the absence of prior notification, the request may be made after notice is taken. (6)

Records provided by investigative agencies that were compiled as a regular or routine procedure by the business or agency from which obtained, or other physical evidence other than investigative reports, may be received and considered subject to rebuttal without authenticating witnesses, provided that the investigative agency furnished this information to NRC pursuant to its responsibilities in connection with assisting NRC in determining the individual's eligibility for reinstatement consistent with the national security. (7)

Records compiled in the regular course of business, or other physical evidence other than investigative reports, relating to a controverted issue that because they are classified may not be inspected by the individual, may be received and considered, provided— (8)

- The DEDM has made a determination that the records or other physical evidence appears to be material. (a)

- The DEDM has made a determination that failure to receive and consider the records or other physical evidence would, in view of the fact that access authorization and/or employment clearance is being sought, be substantially harmful to the national security. (b)

- To the extent that national security permits, a summary or description of the records or other physical evidence is made available to the individual. In every such case, information as to the authenticity and accuracy of the physical evidence furnished by the investigative agency must be considered. (c)

Exhibit 5 (continued)

Whenever information is made part of the record under Section (F)(7) or (8) of this exhibit, the record must contain certification evidencing that the required determinations have been made. (9)

If the hearing official determines that additional investigation of any material information is required, he or she shall request in writing that the Director of DFS arrange for the investigation and shall specify those issues upon which more evidence is requested and identify, where possible, any persons or sources that might provide the evidence sought. (10)

A written transcript of the entire proceeding shall be made by a person possessing appropriate NRC access authorization and/or employment clearance and, except for portions containing Restricted Data or National Security Information, or other lawfully withholdable information, a copy of this transcript shall be furnished the individual without cost. (11)

Recommendation of the Hearing Official (G)

The hearing official's findings and recommendation shall be based upon the entire record consisting of the transcript of the hearing, the documentary and other evidence adduced therein, and the statement of charges and any associated amendment and answer. The hearing official also shall consider the circumstances of the receipt of evidence and the nature and sensitivity of the job the individual was performing. (1)

The hearing official shall make specific findings on each charge in the statement of charges, including the reasons for his or her findings, and shall make a recommendation as to the action that should be taken in the case. (2)

The hearing official's recommendation shall be predicated upon his or her findings. If, after considering all the factors, the hearing official is of the opinion that the individual has clearly demonstrated that reinstating his or her access authorization and/or employment clearance, or reinstatement of employment will not endanger the national security, a favorable recommendation must be made; otherwise, an adverse recommendation must be made. (3)

The hearing official shall submit his or her findings and recommendation in a signed report with the record of the case to the DEDM as soon as possible. (4)

Exhibit 5 (continued)

The hearing official shall not consider the possible impact of the loss of the individual's services upon the NRC program. (5)

New Evidence (H)

After the close of the hearing, in the event the individual discovers new evidence not previously available or known to him or her, the individual may petition the hearing official if the hearing official's recommendation has not yet been issued, or thereafter, the DEDM, to reopen the record to receive that evidence. If the hearing official or the DEDM, respectively, deems it material and appropriate, the record may be reopened to accept the evidence either by stipulation, with the agreement of the hearing counsel, or in a reconvened hearing.

Actions by the DEDM on the Recommendations (I)

Upon receipt of the findings and recommendation from the hearing official, and the record, the DEDM at his or her discretion may return the record for further proceedings by the hearing official with respect to specific matters designated by the DEDM. (1)

If no further proceedings are necessary, upon receipt of the findings and the recommendation by the hearing official, the DEDM, on the basis of the record accompanied by all findings and recommendations, shall make a final determination whether the individual will be reinstated or removed in the interest of national security. (2)

In making the determination as to whether the individual will be reinstated or removed in the interest of national security, the DEDM shall give due recognition to the favorable as well as the unfavorable information concerning the individual. (3)

In the event of an adverse determination, the DEDM shall promptly notify the individual of his or her final decision to remove that individual in the interest of national security and of his or her findings with respect to each charge contained in the statement of charges. (4)

In the event of a favorable determination, the DEDM shall promptly notify the individual. (5)

Exhibit 6
Security Clearances/Access Types

Security Clearances/ Access Types	Investigation Required	Authorizes Access to the Following Information (with an established need-to-know)
Q - Top Secret (TS)	Office of Personnel Management (OPM) Single-Scope Background Investigation (SSBI), with SSBI-Periodic Reinvestigation (SSBI-PR) every 5 years	TS/S/C National Security Information, Restricted Data
L- High Public Trust (L(H)) (Secret)	OPM SSBI, with NACLC every 5 years	S/C National Security Information C - Restricted Data
L - Secret (S)	Access National Agency Check with Inquiry (ANACI) and National Agency Check with law and credit (NACLC) for reinvestigations every 10 years	S/C National Security Information C - Restricted Data
U - Top Secret	OPM SSBI, with SSBI-PR every 5 years	Special Nuclear Material in support of the Material Access Authorization Program (MAAP)
R - Secret	NACLC, with NACLC reinvestigations every 10 years	Special Nuclear Material in support of the MAAP

Exhibit 6 (continued)

Security Clearances/ Access Types	Investigation Required	Authorizes Access to the Following Information (with an established need-to-know)
IT Level I Access	Limited Background Investigation (LBI), with NACLC reinvestigations every 10 years	NRC Sensitive Information Technology Systems or Data for the development, direction, implementation, and administration of agency computer programs
IT Level II Access	ANACI, with NACLC reinvestigations every 10 years	NRC Sensitive Information Technology Systems or Data, including those individuals needing an NRC Local Area Network (LAN) account
Building Access/Day Care Access	General Services Administration (GSA) Suitability Determination, with reinvestigations every 5 years	Unescorted access to NRC facilities for vendors, health unit and housekeeping personnel, and so on
Atomic Energy Act, Section 145b, pre-appointment investigation waiver	SF-86 reviewed and NCIC, credit, employment references, and education check conducted	Safeguards Information, Proprietary Information, and Official Use Only information