

**U.S. NUCLEAR REGULATORY COMMISSION MANAGEMENT DIRECTIVE (MD)**

<b>MD 12.3</b>	<b>NRC PERSONNEL SECURITY PROGRAM</b>	<b>DT-17-227</b>
<i>Volume 12:</i>	Security	
<i>Approved By:</i>	Cynthia A. Carpenter, Director Office of Administration	
<i>Date Approved:</i>	October 8, 2013	
<i>Cert. Date:</i>	N/A, for the latest version of any NRC directive or handbook, see the <a href="#">online MD Catalog</a> .	
<i>Issuing Office:</i>	Office of Administration Division of Facilities and Security	
<i>Contact Name:</i>	Janice Kelsh 301-415-7747	Linda Watson 301-415-7409

**EXECUTIVE SUMMARY**

Directive and Handbook 12.3 are being revised to reflect changes in the personnel security program, specifically, implementation of Executive Orders 13467 and 13488; Homeland Security Presidential Directive-12 (HSPD-12); Presidential Policy Directive 19; and the Office of Personnel Management’s policy changes on investigative products. Changes also have been made to the NRC Drug-Free Workplace Plan.

**TABLE OF CONTENTS**

<b>I. POLICY</b> .....	<b>2</b>
<b>II. OBJECTIVE</b> .....	<b>2</b>
<b>III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY</b> .....	<b>3</b>
A. Commission.....	3
B. Executive Director for Operations (EDO).....	3
C. Deputy Executive Director for Corporate Management (DEDCM).....	3
D. General Counsel (GC).....	4
E. Office of the Inspector General (OIG).....	4
F. Director, Office of International Programs (OIP).....	4
G. Director, Office of Administration (ADM).....	4
H. Director, Office of Investigations (OI).....	5
I. Chief Human Capital Officer (CHCO).....	5
J. Director, Office of Nuclear Security and Incident Response (NSIR).....	5

K. Office Directors and Regional Administrators .....5  
 L. Director, Division of Facilities and Security (DFS), ADM.....6  
**IV. APPLICABILITY .....6**  
**V. DIRECTIVE HANDBOOK .....7**  
**VI. EXCEPTIONS OR DEVIATIONS .....7**  
**VII. REFERENCES.....7**

**I. POLICY**

- A.** 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 (E.O.), management directives (MD), and applicable directives of other Federal agencies for the following:
1. NRC access authorization (security clearance);
  2. NRC employment clearance (pre-appointment investigation waiver, Section 145b of the Atomic Energy Act of 1954 (AEA), as amended);
  3. Unescorted access to nuclear power facilities for NRC employees or contractors;
  4. Access to special nuclear material by NRC licensees;
  5. Access to unclassified Safeguards Information (SGI);
  6. Access to sensitive NRC information, technology systems, or data;
  7. Unescorted access to NRC facilities;
  8. Visits involving classified National Security Information (NSI), Restricted Data (RD), or Sensitive Compartmented Information (SCI); and
  9. Provision of information to foreign regulatory assignees.
- B.** It is also NRC policy that its workplace be free from illegal use, possession, or distribution of controlled substances.

**II. OBJECTIVE**

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.

### III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

#### A. Commission

1. Performs the Commission functions specified in Title 10 of the *Code of Federal Regulations* (CFR) Part 10, "Criteria and Procedures for Determining Eligibility for Access to Restricted Data or National Security Information or an Employment Clearance," for personnel security clearance cases subject to personnel security hearing procedures.
2. Only the Commission may grant temporary access authorization for access to Restricted Data (RD).

#### B. Executive Director for Operations (EDO)

The Executive Director for Operations (EDO) approves the sensitivity criteria to be used in determining whether individual contractor employees require information technology (IT) Level I or Level II approval for access to NRC IT systems or access to sensitive information.

#### C. Deputy Executive Director for Corporate Management (DEDCM)

1. Performs the functions assigned to the Deputy Executive Director for Corporate Management (DEDCM) in accordance with 10 CFR Part 10, including the granting, suspension, denial, or revocation of access authorization (see 64 *Federal Register* 15636, "Conformance to National Policies for Access to and Protection of Classified Information," April 1, 1999).
2. Grants exemptions to 10 CFR Part 25, "Access Authorization," and Part 95, "Facility Security Clearance 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 the Office of the Secretary (SECY) in SECY-80-387, "Delegation of Authority to Grant Exemptions to 10 CFR Parts 25 and 95."
3. Performs the functions of the designated NRC senior agency official in accordance with the provisions of Section 6.1(a) of 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, and ensure that the order is effectively carried out.
4. Approves NRC's employment of individuals before the security investigation is completed, as required by Section 145b of the 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).

5. Grants access, in accordance with the authority in Section 145b of the AEA, 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, "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)," applies to members of Congress serving on NRC congressional oversight subcommittees.
6. Establishes, in accordance with the authority in Section 145g of the 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.

**D. General Counsel (GC)**

1. Performs the functions assigned to the General Counsel (GC) in accordance with 10 CFR Part 10, including appointment of hearing counsel and concurrence in the issuance of subpoenas.
2. Performs legal review of matters related to personnel security.

**E. Office of the Inspector General (OIG)**

Provides DFS, ADM, with information obtained in audits and investigations that is relevant to security issues consistent with 10 CFR 1.12, "Office of the Inspector General."

**F. Director, Office of International Programs (OIP)**

1. 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.
2. Provides assistance, when needed, to the Office of Nuclear Security and Incident Response (NSIR), Division of Security Operations (DSO), for certifying security assurances of foreign nationals requiring access to classified information.

**G. Director, Office of Administration (ADM)**

1. Performs the functions assigned to ADM in accordance with 10 CFR Part 10, including appointing the NRC hearing examiner, serving as the official contact between the individual and the agency, and concurring on written communication between the Director of DFS, ADM and the DEDCM relative to clearance, suspension, and denials.
2. Oversees the NRC personnel security program as carried out by DFS, ADM.

3. Serves as the agency drug program coordinator and oversees the drug testing program.

#### **H. Director, Office of Investigations (OI)**

1. Coordinates with DFS, ADM whenever information derived from DFS, ADM files alone and not corroborated by other means is used in OI reports.
2. Provides security-related information to DFS, ADM developed on licensees, licensee applicants, licensee contractors, or vendor personnel who currently have or are in the process of obtaining a "Q," "L," or reciprocal level access authorization or other security determination.

#### **I. Chief Human Capital Officer (CHCO)**

1. Concurs in a request for a pre-appointment investigation waiver in Section 145b of the AEA, in accordance with Management Directive 10.1, "Appointments, General Employment Issues, Details, and Position Changes."
2. Prepares appropriate personnel actions when an NRC employee's clearance is suspended and/or revoked.

#### **J. Director, Office of Nuclear Security and Incident Response (NSIR)**

1. Informs ADM of any changes to the access authorization program requirements for NRC-licensed facilities to ensure comparability between licensee and NRC programs.
2. Certifies that a foreign national who requires access to classified information has the appropriate security assurance through his or her government.

#### **K. Office Directors and Regional Administrators**

1. Ensure that NRC employees, NRC contractor personnel, and any other personnel under their jurisdiction are cognizant of and comply with the provisions of MD 12.3, as appropriate.
2. 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.
3. Advise DFS, ADM of any information that indicates noncompliance with MD 12.3 or that is otherwise pertinent to the proper protection of classified information, SGI, sensitive unclassified information, or NRC property.
4. Notify DFS, ADM 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 the handbook to this directive.

5. Notify DFS, ADM of persons under their jurisdiction possessing access authorizations who are disabled for a prolonged period (6 months or more), are deceased, have terminated employment, require change of access authorization, or who are subject to any circumstance that may affect their continued eligibility for access authorization.
6. Report immediately to OIG and DFS, ADM all alleged or suspected incidents of employee or contractor fraud, misconduct, unauthorized disclosure, or misuse of automated information systems.

#### **L. Director, Division of Facilities and Security (DFS), ADM**

1. Plans, develops, establishes, and administers policies, standards, and procedures for the overall NRC personnel security program, including denial or revocation in cases involving substantially derogatory information falling within 10 CFR 10.11, "Criteria," when the case has not been favorably resolved through an interview or other investigation.
2. 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 OIP, and the acceptance and issuance of security assurances to and from foreign governments.
3. Serves as the NRC central point of contact with the Federal Bureau of Investigation, the Office of Personnel Management, and other investigative agencies on NRC personnel security matters.
4. Recommends to the DEDCM approval of Section 145b waiver of the Atomic Energy Act of 1954 for employing an individual before the completion of the security investigation.
5. Supplies OIG with the personnel security information necessary to conduct investigations and audits.

#### **IV. APPLICABILITY**

MD 12.3 applies to all NRC employees, licensees, consultants, experts, panel members, applicants for employment, and other persons designated by the DEDCM, as well as to all NRC contractors and subcontractors to whom it applies as a condition of a contract or a purchase order.

## V. DIRECTIVE HANDBOOK

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

## VI. EXCEPTIONS OR DEVIATIONS

Exceptions to or deviations from MD 12.3 may be granted by the Director of DFS, ADM, in writing, except for those areas in which the responsibility or authority is vested solely with the Commission, the DEDCM, or the Director of ADM, and is nondelegable, or for matters specifically required by law, E.O., or directive to be referred to other management officials.

## VII. REFERENCES

### *Code of Federal Regulations*

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

10 CFR Part 7, "Advisory Committees."

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 11, "Criteria and Procedures for Determining Eligibility for Access to or Control Over Special Nuclear Material."

10 CFR Part 25, "Access Authorization."

10 CFR 73.21, "Protection of Safeguards Information: Performance Requirements."

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

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

### *Department of Health and Human Services*

Mandatory Guidelines for Federal Workplace Drug Testing Programs, at <http://www.gpo.gov/fdsys/pkg/FR-2008-11-25/pdf/E8-26726.pdf>.

### *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 Federal Workplace," September 15, 1986.

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

13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," June 30, 2008.

13488, "Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust," January 16, 2009.

13526, "Classified National Security Information," December 29, 2009.

### ***Federal Register Notice***

"Conformance to National Policies for Access to and Protection of Classified Information" (April 1, 1999, 64 FR 15636).

### ***Nuclear Regulatory Commission Documents***

Management Directive—

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."

10.122, "Employee Assistance and Wellness Services Program."

11.1, "NRC Acquisition of Supplies and Services."

12.1, "NRC Facility Security Program."

12.2, "NRC Classified Information Security Program."

12.6, "NRC Sensitive Unclassified Information Security Program."

NRC Forms Library on SharePoint:

<http://portal.nrc.gov/nrcformsportal/default.asp>.

NRC System of Records NRC-35, "Drug Testing Program Records—NRC," at

<http://www.nrc.gov/reading-rm/foia/privacy-systems.html>.

NRC System of Records NRC-39, "Personnel Security Files and Associated Records—NRC," at <http://www.nrc.gov/reading-rm/foia/privacy-systems.html>.

NUREG/BR-0134, "NRC Drug-Free Workplace Plan," Revision 2, March 2007.

NUREG/BR-0136, "The NRC Drug Testing Manual," August 2008.



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

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.

Yellow Announcement 08-040, "General Notice of NRC Drug Testing Program Changes and Notice of Employee Awareness Sessions," as the revised NRC Drug-Free Workplace Plan (August 2007) at <http://www.internal.nrc.gov/announcements/yellow/2008/2008-040.html>.

### ***Other Documents***

Agreement Between the United States of America and the International Atomic Energy Agency for the Application of Safeguards in the United States (and Protocol Thereto), November 18, 1977, at <http://www.state.gov/t/isn/5209.htm>.

Homeland Security Presidential Directive-12 (HSPD-12), August 27, 2004.

Presidential Policy Directive 19, "Protecting Whistleblowers with Access to Classified Information," October 10, 2012.

Treaty on the Non-Proliferation of Nuclear Weapons, March 5, 1970.

### ***United States Code***

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

Controlled Substances Act (CSA), Title II of the Comprehensive Drug Abuse Prevention and Control Act of 1970, Pub. L. No. 91-513, 84 Stat. 1236 (October 27, 1970) (22 U.S.C. et seq.).

Fair Credit Reporting Act of 1970 (15 U.S.C. 1681 et seq.).

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

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, Pub. L. 100-71, July 11, 1987.

**U.S. NUCLEAR REGULATORY COMMISSION DIRECTIVE HANDBOOK (DH)**

<b>DH 12.3</b>	<b>NRC PERSONNEL SECURITY PROGRAM</b>	<b>DT-17-227</b>
<i>Volume 12:</i>	Security	
<i>Approved By:</i>	Cynthia A. Carpenter, Director Office of Administration	
<i>Date Approved:</i>	October 8, 2013	
<i>Cert. Date:</i>	N/A, for the latest version of any NRC directive or handbook, see the <a href="#">online MD Catalog</a> .	
<i>Issuing Office:</i>	Office of Administration Division of Facilities and Security	
<i>Contact Name:</i>	Janice Kelsh 301-415-7747	Linda Watson 301-415-7409

**EXECUTIVE SUMMARY**

Directive and Handbook 12.3 are being revised to reflect changes in the personnel security program, specifically, implementation of Executive Orders 13467 and 13488; Homeland Security Presidential Directive-12 (HSPD-12); Presidential Policy Directive 19; and the Office of Personnel Management’s policy changes on investigative products. Changes also have been made to the NRC Drug-Free Workplace Plan.

**TABLE OF CONTENTS**

<b>I.</b>	<b>NRC ACCESS TYPES .....</b>	<b>3</b>
	A. Introduction.....	3
	B. Position Sensitivity Criteria .....	4
	C. Access Authorization Requests .....	5
	D. Contractual Language for Unescorted Access by NRC Contractors .....	9
	E. Access to Safeguards Information (SGI) by NRC Contractors .....	10
	F. Access to NRC Information Technology (IT) Systems or Sensitive Information by NRC Contractors or Consultants .....	11
	G. Contractors Requiring Building Access (BA) to NRC Facilities.....	13
<b>II.</b>	<b>INVESTIGATIONS AND DETERMINING ELIGIBILITY FOR ACCESS AUTHORIZATION.....</b>	<b>15</b>
	A. Investigations .....	15
	B. Reciprocity of “Q” and “L” Access Authorization.....	15

C. Reopening of Canceled Cases .....	16
D. Pre-Appointment Investigation Waiver with No Access to Classified Information .....	16
E. Circumstances Affecting Eligibility for Access Authorization .....	17
F. Determination of Eligibility for Access Authorization .....	18
G. Temporary Access to Classified Information.....	18
H. Access Authorization for Dual Citizens .....	19
I. Access Authorization for Non-U.S. Citizens .....	19
J. Personnel Reporting Responsibilities .....	20
K. Reinvestigation Program .....	23
L. Termination of Access Authorization.....	24
M. Clearance Suspension and Revocation .....	24
N. Termination of Contractor Unescorted Building Access (BA), Information Technology (IT) Access, Power Reactor Access, and Safeguards Information (SGI) Access.....	25
O. Badging Requirements in Homeland Security Presidential Directive-12 (HSPD-12).....	25
<b>III. CONTROL OF VISITS INVOLVING CLASSIFIED INFORMATION .....</b>	<b>25</b>
A. Introduction.....	25
B. General .....	26
C. Outgoing Visits by NRC Employees, Contractors, and Licensees.....	27
D. Incoming Visitors .....	28
E. Visits Involving Access to Sensitive Compartmented Information (SCI) .....	30
F. Visits Involving Access to Classified Information by Foreign Nationals Sponsored by Foreign Governments or International Organizations .....	30
G. Visits to Foreign Governments or Activities by NRC Personnel .....	31
H. Records of Visit Requests .....	31
<b>IV. ASSIGNMENT OF FOREIGN REGULATORY EMPLOYEES TO THE NRC .....</b>	<b>31</b>
A. Introduction.....	31
B. Activity Plans .....	31
C. Assignments.....	31
D. Background Check .....	33
E. Assignee Agreements.....	33
F. Security Plans .....	34
G. Assignee Responsibilities .....	35
H. Evaluation of Assignees .....	35

**V. NRC’S DRUG-FREE WORKPLACE PLAN .....35**

A. General .....35

B. NRC’s Drug Testing Program .....36

C. Deferral of Drug Testing .....37

D. Drug Testing when an Employee is Working under the NRC’s Flexiplace Program .....37

E. Positive Drug Test Result .....37

**EXHIBITS**

Exhibit 1 Security Orientation Briefing for New NRC and Contractor Employees .....38

Exhibit 2 Standard Operating Procedures for Pre-Employment Screening of NRC Applicants .....39

Exhibit 3 “Q,” “L(H),” and “L” Reinvestigation Program Requirements .....41

Exhibit 4 Security Clearances/Access Types .....43

**I. NRC ACCESS TYPES**

**A. Introduction**

1. The U.S. Nuclear Regulatory Commission reviews and makes eligibility determinations for NRC access authorization and/or employment clearance (in accordance with Executive Order (E.O.) 12968, “Access to Classified Information,” and E.O. 10450, “Security Requirements for Government Employment”), unescorted access to nuclear power facilities, access to Safeguards Information (SGI) (in accordance with E.O. 10865, “Safeguarding Classified Information Within Industry”), access to sensitive NRC information technology systems or data, and unescorted access to NRC facilities.
2. Exhibits 1 through 4 are provided to explain in greater detail the requirements of Management Directive (MD) 12.3.
3. Exhibit 4 lists security clearances/access types and investigative requirements for those with authorized access and an established need-to-know.
4. Personnel security and associated records maintained in accordance with the provisions of the NRC personnel security program are protected from public disclosure in accordance with the provisions of the Inspector General Act

(5 U.S.C. App.), the Privacy Act of 1974, as amended (in accordance with MD 3.1, "Freedom of Information Act"; MD 3.2, "Privacy Act"; and MD 3.4, "Release of Information to the Public"), and are subject to the routine uses specified for NRC System of Records NRC-39, "Personnel Security Files and Associated Records-NRC."

## **B. Position Sensitivity Criteria**

Position sensitivity 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 a Single Scope Background Investigation (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).

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

People in positions of a high degree of importance or designated as special-sensitive require an NRC "Q" access authorization based on an OPM or FBI SSBI in accordance with Section 145f of the Atomic Energy Act of 1954 (AEA), as amended. These positions include—

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

### **2. Positions of a Critical-Sensitive Designation that Require a "Q" Clearance**

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:

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

### 3. Positions of High Public Trust that Require an “L(H)” Clearance

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—

- (a) Final approval of plans, policies, or programs that directly affect the overall operations and direction of the NRC.
  - (b) 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 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.
  - (c) Duties performed by resident inspectors.
  - (d) Other duties requiring high public trust as determined on an as needed basis by the Deputy Executive Director for Corporate Management (DEDCM).
- ### 4. “L” Positions of a Noncritical-Sensitive Designation

People in any NRC position not covered by Sections I.B.1 through 3 of this handbook require an NRC “L” access authorization based on an ANACI investigation.

## C. Access Authorization Requests

### 1. Employees

- (a) Requests for access authorizations (“Q,” “L(H),” or “L”) for NRC employees, applicants for NRC employment (anyone who has received an authorized conditional offer of employment), and NRC experts, panel members, and consultants must be submitted through the Office of the Chief Human Capital Officer (OCHCO) or the regional Human Resources Branch, as appropriate, to the Office of Administration (ADM).
- (b) An NRC official in OCHCO or the regional Human Resources Branch is responsible for submitting NRC Form 236, “Personnel Security Clearance Request and Notification,” on the NRC Forms Library on SharePoint, available at <http://portal.nrc.gov/nrcformsportal/default.asp> to the Personnel Security Branch (PSB), Division of Facilities and Security (DFS), ADM, with a completed security forms packet. Upon favorable review of the access authorization request package, PSB will return the approved NRC Form 236 to OCHCO or the regional Human Resources Branch, as appropriate, indicating the level of access being authorized or documenting the temporary waiver of a clearance. If the outcome of the review is less than favorable, PSB will notify OCHCO or the regional Human Resources Branch.

- (c) An applicant for an NRC access authorization must be a U.S. citizen and meet the investigative coverage requirements for U.S. residency for the immediate period before the date the applicant signed the security forms. For "Q" and "L(H)" clearances, the applicant must meet the immediate 10-year U.S. residency coverage requirement. For "L" clearances, the requirement is the immediate 7-year U.S. residency 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 employees access to classified information. A pre-employment review of an applicant's background is conducted by PSB to provide the basis for the temporary waiver. A background investigation, conducted by OPM, provides the basis for granting a clearance.
  - (d) For "Q" and "L(H)" clearances, the required investigation will cover the last 10 years. For "L" clearances, the investigation will cover the last 7 years. Applicants living overseas for extensive periods (1 year or more, excluding formal educational purposes) during the 7- or 10-year periods cannot be investigated in a timely manner in most cases. For this reason, applicants who have lived overseas for an extended period of time are not eligible for interim access authorization due to the difficulty in obtaining investigative coverage overseas. This may also result in a delay or the inability to process the final access authorization approval or clearance.
  - (e) 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 PSB, or in a regional office by a regional security representative (see Exhibit 1).
2. Contractors (Information Technology (IT) and Building Access (BA))
- (a) An NRC contractor, subcontractor, or other individual who is not an NRC employee (for example, other Government agency personnel or licensees) requiring access to the local area network (LAN) and/or unescorted building access (BA) must submit a request for such access on NRC Form 89, "Badge Request." A contractor requiring a national security clearance is processed using NRC Form 237, "Request for Access Authorization." The requester must forward this form to PSB, 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 NRC Form 237. See Section I.C.3 of this handbook, "Security Forms Packet for an Access Authorization Request."
  - (b) At contractor facilities at which NRC is not the cognizant security authority (CSA), access authorizations will be requested following the procedures of the CSA.

- (c) A foreign ownership, control, or influence (FOCI) review must be completed by the Office of Nuclear Security and Incident Response (NSIR) with a favorable determination on a company before granting personnel security clearances. An FOCI is not required for IT access or BA. (For further guidance on FOCI, refer to MD 12.1, "NRC Facility Security Program," and MD 12.2, "NRC Classified Information Security Program.")
  - (d) All contractors requiring an NRC access authorization or a national security clearance must meet the investigative coverage requirements for U.S. residency for the immediate period before the date the contractor signed the security forms. For all access authorizations or "L" clearances, the requirement is the immediate 7-year U.S. residency coverage period. For "Q" and "L(H)" clearances, the contractor must meet the immediate 10-year U.S. residency coverage requirement. A pre-employment review of a contractor's background is conducted by PSB to provide the basis for an interim access authorization approval. A background investigation conducted by OPM provides the basis for granting a final access approval or clearance. Applicants living overseas for extensive periods (1 year or more, excluding formal educational purposes) during the 7- or 10-year periods cannot be investigated in a timely manner. For this reason, applicants who have lived overseas for an extended period of time are not eligible for interim access authorization due to the difficulty in obtaining investigative coverage overseas. This may also result in a delay or the inability to process the final access authorization approval or clearance.
  - (e) Foreign nationals (non-U.S. citizens) are not eligible for a national security clearance. However, at the discretion of the DEDCM, foreign nationals may be processed for access authorizations with access to classified information limited to the specific programs, projects, contracts, licenses, or grants for which there is a need for access, if they meet the 7- or 10-year U.S. residency requirements (see Section II.I of this handbook for additional details).
  - (f) A security orientation briefing must be given to NRC contractors granted national security clearances. This briefing will normally be given by a representative of PSB, or in a regional office by a regional security representative (see Exhibit 1 to this handbook).
3. Security Forms Packet for an Access Authorization Request
- (a) Unless otherwise indicated, each request for access authorization must be accompanied by a properly completed security forms packet containing the following:
    - (i) Signature pages from the Electronic Questionnaires for Investigations Processing (e-QIP). Applicants must complete Standard Form (SF)-86, "Questionnaire for National Security Positions" (QSP) (initiated by PSB in



e-QIP), except BA applicants who are required to complete SF-85, "Questionnaire for Non-Sensitive Positions."

- (ii) Two applicant fingerprint cards (SF-87 for Federal employee applicants or FD-258, "FBI Fingerprint Card," for contractors) (available from OCHCO or PSB), or equivalent electronic fingerprint images.
  - (iii) NRC Form 176, "Security Acknowledgment/Access Authorization."
  - (iv) Résumé (for NRC applicants; not required for contractors).
  - (v) NRC Form 236 (for NRC employees) and NRC Form 237 (for contractors or licensees).
  - (vi) OF-306, "Declaration for Federal Employment" (available from OCHCO or PSB) (required for NRC employees and BA contractors).
  - (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) NRC Form 89 (for NRC contractors; not required for NRC employees, licensees, or consultants).
- (b) PSB will return requests for access authorization to the requester if—
- (i) All security forms are not completed and signed as required.
  - (ii) The printed content of the security or release form is altered.
  - (iii) Required information is not provided.
  - (iv) The forms are illegible.
  - (v) The "Certification and Authorization for Release of Information" pages on the SF-86 are not signed.
- (c) Information entered on the forms in the security packet will be used in conjunction with any other relevant information to determine an applicant'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, data, or facilities.

#### 4. Cancelled or Withdrawn Request

When a request for an applicant's access authorization is to be withdrawn or cancelled, PSB 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 applicant, the date of the request, and the type of access authorization being cancelled. Telephone notifications must be promptly confirmed in writing to PSB.

#### **D. Contractual Language for Unescorted Access by NRC Contractors**

1. Sponsoring Office Responsibilities for Unescorted Access of NRC Contractors
  - (a) The NRC sponsoring office must decide whether performance in accordance with an NRC contract, interagency agreement (IAA), or memorandum of understanding (MOU) will involve unescorted access to nuclear power facilities, access to SGI, access to NRC IT systems or sensitive information, or BA. For these contracts, the sponsoring office must state on the appropriate procurement request document that—
    - (i) “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.”
    - (ii) “This contract requires continuous unescorted access (in excess of 30 calendar days) to NRC Headquarters or regional office facilities, or otherwise requires NRC photo-identification or keycard badges.”
  - (b) Include NRC Form 187, “Contract Security and/or Classification Requirements,” available on the NRC Forms Library on SharePoint, according to the requirements of MD 11.1, “NRC Acquisition of Supplies and Services.” (See MD 12.1 for escort and badge responsibilities, and security requirements outlined in the MD 11.1, Handbook.)
2. Unescorted Access at Nuclear Power Reactor Facilities

Individual contractors requiring unescorted access to protected and vital areas of nuclear power facilities (and IT Level II access, if applicable) will be approved in accordance with the following procedures:

##### **(a) Interim Approval**

Interim approvals may be obtained by two methods:

- (i) For the first method, the contractor employee must submit to PSB through the NRC COR a completed personnel security forms packet, including an SF-86. DFS will conduct criminal history and credit checks. 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.

- (ii) For the second method, the contractor employee will be fingerprinted by the facility and those fingerprints will be submitted to the NRC's Criminal History Program for processing. In addition, the applicant will be subject to the utility's access authorization program.

(b) Final Approval

Final access approval will be granted after—

- (i) The required investigation on the applicant has been completed and has received a favorable adjudicative review, resulting in NRC's endorsement of the applicant's unescorted access at all nuclear facilities, as long as the individual employee is employed on the contract, and provided no new issue or information is developed that may bring the applicant's eligibility into question.
- (ii) The contractor has obtained unescorted access authorization (other than interim access) at the specific facility through that utility's access authorization program.
- (iii) The applicant possesses a valid Federal Government-issued security clearance as verified by DFS.

(c) Resolving Questions of Eligibility

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

(d) Notification of Unusual Circumstances

Contractors who possess interim or final unescorted access to nuclear power facilities or access to SGI are subject to the reporting requirements set forth in Section II.J of this handbook. The security officer or designee must promptly report the circumstances to the Director of DFS.

## **E. Access to Safeguards Information (SGI) by NRC Contractors**

The NRC sponsoring office must decide whether performance in accordance with an NRC contract will involve access to SGI. This access may require a National Agency Check with Inquiry (NACI) or other investigation as PSB deems necessary. On the basis of the review of the applicant's security forms by PSB, and/or the receipt of adverse information by NRC, the individual may be denied access to SGI until a final determination of eligibility for access is made. SGI access for contractor employees may

be granted in accordance with licensee programs. See MD 12.6, "NRC Sensitive Unclassified Information Security Program," for further information.

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

1. The Executive Director for Operations approves the sensitivity criteria to be used in determining whether individual contractor employees 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 requires a background investigation. IT Level I or Level II access is also required for contractors working offsite with sensitive unclassified information.
2. Before starting work, contractors requiring IT access (either Level I or Level II) must be granted either an interim access or a final access based on a background investigation. A pre-employment review of an applicant's background is conducted by PSB to provide the basis for interim access. A more thorough investigation covering the last 7 years, conducted by OPM, provides the basis for granting final access. Applicants living overseas for extensive periods (1 year or more, excluding formal educational purposes) during the 7-year period cannot be investigated in a timely manner. For this reason, applicants who have lived overseas for an extended period of time are not eligible for interim access authorization due to the difficulty in obtaining investigative coverage overseas. This may also result in a delay or the inability to process the final access authorization approval or clearance.

(a) IT Level I

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 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. These positions may involve—

- (i) Responsibility for the development, direction, implementation, and administration of NRC computer security programs, including direction and control of risk analysis or threat assessment.
- (ii) Significant involvement in life-critical or mission-critical systems.
- (iii) Responsibility for preparing or approving 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.

- (iv) Relatively high-risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of either—
  - Dollar amounts of \$10 million per year or greater; or
  - 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.
- (v) Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.
- (vi) Other positions that involve relatively high risk for causing grave damage or realizing significant personal gain.

(b) IT Level II

IT Level II includes all other individuals with access to IT systems or sensitive information, including those needing an NRC LAN account.

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

(a) Interim Approval

- (i) The contractor employee will submit a completed personnel security forms packet to PSB through the NRC COR (see Section I.C.3 of this handbook).
- (ii) The COR will forward the completed security forms packet to PSB for pre-employment checks.
- (iii) PSB will conduct criminal history and credit checks, review form SF-86, "Questionnaire for National Security Positions," and determine the contractor employee's eligibility for interim access. PSB will issue a memorandum reflecting interim approval or disapproval to the COR and sponsoring office, pending completion of the required background investigation.

(b) Resolving Questions of Eligibility

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

(c) Final Approval or Disapproval

Upon receipt of the complete OPM background investigation, PSB will adjudicate the case. A final letter will be issued by PSB to the contracting officer's

representative (COR) and sponsoring office indicating approval or denial for IT Level I or Level II access.

#### **G. Contractors Requiring Building Access (BA) to NRC Facilities**

1. The number of escorted contractors working in the building should be minimized. The NRC sponsoring office must decide whether performance in accordance with an NRC contract, purchase order, IAA, MOU, or similar agreement will involve unescorted BA (in excess of 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 calendar days, or that the work requires a photo-identification badge, approval for unescorted BA must be received by PSB before the onsite work begins. For these contractual or other similar arrangements or agreements requiring unescorted BA to NRC facilities, the COR and sponsoring office must include NRC Form 187 with Section 5.F. checked.
2. Individual contractor employees or other individuals requiring BA will be approved for continuous unescorted access in accordance with the following procedures:
  - (a) Contractor Building Access Procedures

Approval for granting contractors unescorted BA must be based on 10 years of investigative coverage in the United States. Contractors with less than 5 years of investigative coverage in the United States may be granted unescorted BA with restrictions specified by PSB, such as going through lobby visitor screening procedures before each entry to the building.
  - (b) Interim Building Access Approval or Denial
    - (i) The contractor will submit the following information to PSB through the NRC headquarters or regional COR: a completed e-QIP SF-85, OF-306, two FD-258s (or electronic fingerprints), and NRC Form 89. All foreign nationals or naturalized citizens must provide original legal residence documentation (for example, a naturalization certificate or a resident card) in person to PSB. For regional offices, the OCHCO representative may conduct this verification and forward it to PSB.
    - (ii) On the basis of PSB review of the applicant's security forms and credit and criminal history, PSB will determine the applicant's eligibility for interim access and will issue a memorandum reflecting interim approval or denial to the COR, pending completion of the required preliminary checks.

(c) Final Approval or Denial

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

- (i) Upon receipt of the complete OPM background investigation, PSB will adjudicate the case. A final letter will be issued by PSB to the COR and sponsoring office indicating approval or denial for BA.
- (ii) As determined by PSB, the applicant 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).

(d) Reinvestigation for Building Access (BA) and Childcare Contractor Cases

- (i) BA is valid for 10 years from the initial approval date, provided that the individual remains employed in accordance with an NRC contract, MOU, IAA, or similar arrangement. Each individual who is approved for unescorted BA must be recertified every 10 years from the date of the initial approval and each subsequent reinvestigation.
- (ii) Childcare BA approvals are valid for 5 years from the date of initial approval, provided the individual remains employed in accordance with the NRC Childcare Contract. Each individual who is approved for unescorted access in accordance with the NRC Childcare Contract must be recertified every 5 years from the date of the initial approval and each subsequent reinvestigation.
- (iii) For each subsequent recertification, the contractor will submit a new e-QIP SF-85 and two FD-258s to PSB, through the NRC headquarters or regional COR, for each individual who requires reinvestigation. With timely application and in the absence of any adverse information, the individual will maintain unescorted BA pending reinvestigation. If the contractor fails to submit a timely application, unescorted BA approval will expire at the end of the 5-year period and the individual will be denied unescorted access to NRC facilities.

(e) Resolving Questions of Eligibility

Any questions regarding the individual's final eligibility for continuous unescorted BA to NRC facilities on the basis of the OPM investigation will be resolved between the individual and PSB. PSB will contact the individual to obtain further information in an effort to mitigate any concerns that may affect the approval to continue the individual's unescorted access. The individual is provided an opportunity to give additional information and to appeal a denial of building access to the director of DFS.

3. A contractor employee or other individual requiring unescorted BA will not be provided unescorted access to NRC facilities until being approved for interim or final access in accordance with these procedures.
4. NRC CORs may be issued a security infraction, as described in MD 12.1 for situations in their which contractors do not follow the access procedures of MD 12.3. Examples may include when a contractor requires access for more than 30 calendar days and does not receive access approval from PSB, or when a contractor is denied access and is subsequently escorted into the building for work.
5. Any exception to the requirements of this section requires the approval of the Director of DFS. For example, the need to escort contractors to work within NRC space for more than 30 calendar days may warrant a possible exception. Other possible exceptions may include situations in which escort requirements could be relaxed if the escort would be subjected to hazardous conditions.

## **II. INVESTIGATIONS AND DETERMINING ELIGIBILITY FOR ACCESS AUTHORIZATION**

### **A. Investigations**

1. The hiring or employing office, in coordination with OCHCO and the Director, DFS, must determine the position sensitivity, using the criteria specified in Section I.B of this handbook, before requesting access authorization for the following individuals: NRC employees, applicants for employment, consultants, experts, and panel members. 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 the employee's classified access requirements; access to SGI, NRC IT systems, or sensitive information; or need for unescorted access to nuclear power facilities, NRC headquarters, or regional office facilities.
2. Instead of an OPM report of investigation, 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 have been granted to the individual on the basis of an investigation and report.

### **B. Reciprocity of "Q" and "L" Access Authorization**

1. 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, meets the required level of the clearance requested, and is linked with separation of employment of 2 years or less. An SF-86 may be required.



2. 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 will be accepted.

### **C. Reopening of Canceled Cases**

A canceled case is any request that is canceled before the investigation is completed. If more than 90 days have passed since the security forms originally submitted were signed, an individual will be required to update, re-sign, re-date, and resubmit the security forms to reopen the canceled case.

### **D. Pre-Appointment Investigation Waiver with No Access to Classified Information**

1. The DEDCM 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 while the required security investigation is pending.
2. All waivers must be submitted on NRC Form 236 and must meet the following criteria:
  - (a) The waiver must be requested by the office director, the deputy office director, or his or her designee; or by the regional administrator, the deputy regional administrator, or his or her designee.
  - (b) The waiver must 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.
  - (c) The waiver must indicate that the hiring office will establish administrative controls 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.
  - (d) The waiver must be concurred on by the CHCO, or his or her designee; the Director of DFS; and if regional personnel are involved, the Human Resources Branch.
3. OCHCO and PSB must process all Section 145b AEA requests under Exhibit 2 of this handbook. OCHCO or the regional Human Resources Branch, when applicable, must provide PSB with the results of pre-employment checks (reference checks)

conducted for NRC applicants who are being considered for employment under Section 145b of the AEA.

4. An exception to personal reference checking for consultants or experts may be recommended to OCHCO 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 on NRC Form 236.
5. In the case of students being considered for temporary summer appointments, personal reference checks must be conducted under the procedures specified in Exhibit 2 of this handbook.

#### **E. Circumstances Affecting Eligibility for Access Authorization**

1. The 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, "Criteria," and 32 CFR Part 147, "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information." These matters must be promptly reported to the Director of DFS by the person's designated employment official. In addition, the individual must adhere to the requirements of Section II.J of this handbook.
2. In the case of contractor personnel, the circumstances must be reported promptly to the Director of DFS by the contracting officer, the COR, or other person so designated.
3. The reporting requirements of Section II.J.11 of this handbook do not excuse an individual from the requirement to report to PSB an arrest as required by the QSP (SF-86), the security acknowledgment (NRC Form 176), or other forms signed by the individual. The arrest must be reported within 5 workdays.
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 national security.
5. NRC employees and designated management officials are encouraged to seek information and assistance available from the NRC Employee Assistance Program Manager in accordance with MD 10.122, "Employee Assistance and Wellness Services Program," 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.

**F. Determination of Eligibility for Access Authorization**

1. Except as provided for in Section II.I of this handbook, an NRC “L,” “L(H),” or “Q” access authorization (security clearance) will be granted only to employees and contractors who are U.S. 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.
2. 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,” (available from PSB) before the granting of the security clearance.
3. The SF-312 is executed in accordance with Executive Orders (E.O.s) 12968 and 13526. Additionally, 10 CFR 25.23 and 95.33 also apply to licensee personnel. 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 must attend a security briefing and execute an SF-312. The term “individual” refers to all NRC employees, contractors, licensees, and those who the Commission deems 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.
4. The determination of eligibility for contractor access will be consistent with 10 CFR Part 10. BA contractors will be afforded due process if derogatory information is developed that could result in BA being denied or revoked. The contractor employee must be provided written notification of the grounds for the denial or revocation by the Chief of PSB. The Director of DFS makes the final determination for BA in the best interest of NRC.

**G. Temporary Access to Classified Information**

1. Only the Commission may grant temporary access authorization for access to RD.
2. Requests for temporary access to classified information must be forwarded to PSB in the same manner as requests for access authorization and must include the forms and information specified in Section I.C of this handbook. 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.

3. OCHCO or the regional Human Resources Branch, as appropriate, must provide PSB with the results of the pre-employment checks on NRC applicants who are being considered for temporary access to classified information authorization (see Exhibit 2 to this handbook for the scope of the required pre-employment checks).
4. If PSB evaluation of the information developed on an individual is unfavorable, PSB will inform the requesting office and, if applicable, OCHCO of its determination in the matter.

#### **H. Access Authorization for Dual Citizens**

A dual citizen is a U.S. citizen who concurrently holds citizenship with a foreign country. When adequately supported, a dual citizen may be processed for an "L," "L(H)," or "Q" access authorization. In addition, the investigative coverage must be obtainable for the immediate 10-year retrospective period.

#### **I. Access Authorization for Non-U.S. Citizens**

1. 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 DEDCM, be granted an NRC "L," "L(H)," or "Q" access authorization with access to classified information limited to the specific programs, projects, contracts, licenses, certificates, or grants for which there is a need for access. These individuals will not be eligible for access to any greater level of classified information than the U.S. Government has determined may be releasable to the country of which the subject is currently a citizen, and 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.
2. An interview with the applicant will be conducted and include the following:
  - (a) The individual's statement and disclosure of national allegiance;
  - (b) The applicant's intent as to permanent residence in the United States;
  - (c) The applicant's general attitude toward the United States versus the other country of the applicant's citizenship;
  - (d) The applicant's eligibility and intention to maintain dual citizenship (if the applicant is a dual citizen);
  - (e) The applicant's previous civilian or military service with a foreign government, if any;
  - (f) The names of the applicant's family or other relatives who live abroad or are employed by a foreign government; and

- (g) The names and addresses of U.S. citizens who can furnish information as to the applicant's background and activities outside the United States.
- 3. A verbatim transcript or detailed summary of the interview will be maintained and provided to the applicant upon request.
- 4. If PSB 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.
- 5. If PSB concludes that there are significant issues in the case that will require further review, the NRC sponsor will be informed.

#### **J. Personnel Reporting Responsibilities**

- 1. All NRC employees, consultants, experts, panel members, contractors, and licensees are required to abide by the security reporting requirements; the responsibility is an important part of the "continuing evaluation" process to maintain eligibility for an NRC security clearance/access authorization. Individuals must report to PSB the following information 5 days of an event occurring. Failure to timely report the following information could result in disciplinary action and/or affect eligibility for a security clearance:
  - (a) Arrests, charges, or detentions;
  - (b) Involvement in civil court actions;
  - (c) Change in marital status (including legal separation);
  - (d) Change of name;
  - (e) Change in cohabitation;
  - (f) Outside employment that creates a conflict of interest;
  - (g) Foreign national contacts including business or personal contacts;
  - (h) Travel to a foreign country for which the U.S. Department of State has issued a travel warning (travel warnings can be found at <http://travel.state.gov/travel/>);
  - (i) Any arrests and detentions, issues with customs or law enforcement, or concerns that you were being followed or monitored while on official or unofficial travel;
  - (j) Travel to a foreign country where a passport other than a U.S. passport is used to enter or leave the country;
  - (k) Enrollment in a drug or alcohol treatment program;

- (l) Changes in financial status (notice of debt collection, bankruptcy, collection activity, foreclosure, Federally guaranteed loans, tax liens, or failure to file or pay Federal or State taxes); or
  - (m) Treatment for emotional, mental, or personality disorders (except marriage, grief, or family counseling). NOTE: Employees are encouraged to seek help for mental health and/or addictions issues. This treatment is not automatically adverse to maintaining a national security clearance.
2. Employees will be required to acknowledge these reporting requirements annually to encourage compliance.
  3. In addition, employees have an obligation to promptly report any information that raises doubts as to whether someone's continued eligibility for access to classified information is clearly consistent with national security. In addition to the items listed above, reportable information includes, but is not limited to—
    - (a) Use of intoxicating beverages habitually to excess without evidence of rehabilitation or reformation or being hospitalized or treated for alcohol abuse.
    - (b) Use of, trafficking in, sale, transfer, or possession of a drug or other substance listed in the Controlled Substances Act, Title II of the Comprehensive Drug Abuse Prevention 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.
    - (c) Commission of, attempted commission of, or conspiracy to commit any act of sabotage, treason, or sedition.
    - (d) Holding membership in, with the intention of furthering the aims of, or actively participating in any foreign or domestic organization or group that advocates the commission of illegal acts by force or violence.
    - (e) 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 this support will further the goals of the group or organization.
    - (f) Renouncing U.S. citizenship or representing a foreign nation in activities that may be contrary to national security of the United States.
    - (g) Parent(s), brother(s), sister(s), spouse, or offspring living in a nation whose interests may be adverse to the interests of the United States, or in satellite states or occupied areas.

- (h) Observing or having knowledge of another individual who willfully violates or disregards security or safeguards regulations.
  - (i) 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.
  - (j) 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.
  - (k) Any criminal conduct including arrests, charges (including charges that are dismissed), allegations or admissions of criminal conduct, and/or detentions by Federal, State, or other law enforcement authorities for any violation of any Federal, military, State, county, or municipal law, regulation, or ordinance other than minor traffic violations for which a fine of \$300 or less was imposed, occurring during any period in which they hold an NRC security clearance.
  - (l) 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 condition that may cause a significant defect in judgment or reliability.
  - (m) Any employment or association or change in employment or association with a foreign or foreign-owned interest or representatives.
  - (n) Contact with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information.
  - (o) Effort by any individual to obtain or gain unauthorized access to classified information or special nuclear material.
  - (p) Any financial considerations that indicate an inability or an unwillingness to satisfy debts. Examples include—
    - (i) Not meeting financial obligations, such as a mortgage foreclosure, bankruptcy, debt collections, charge-offs, or failure to pay State and Federal taxes;
    - (ii) Financial problems linked to gambling, drug abuse, alcoholism; or
    - (iii) Other financial issues.
4. Not all reportings are deemed derogatory and affect a security clearance.
5. Individuals who marry or cohabitate in a spouse-like relationship after they have submitted an SF-86 must furnish PSB with an original NRC Form 354, "Data Report on Spouse," available on the NRC Forms Library on SharePoint.

**K. Reinvestigation Program**

1. 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—
  - (a) NRC employees, consultants, experts, and panel members;
  - (b) 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 NRC's activities;
  - (c) Congressional staff members cleared by the NRC;
  - (d) Employees and consultants of NRC contractors and licensees; and
  - (e) All others who possess an NRC access authorization.
2. PSB must re-evaluate the continued eligibility of those individuals cleared (see Exhibit 3 to this handbook for “Q” and “L” reinvestigation requirements).
3. PSB will initiate a reinvestigation every 5 years for “Q” and “L(H)” (high public trust) clearances and every 10 years for “L” clearances. PSB will notify the individuals who are to be reinvestigated and the dates by which they are to complete the security forms in e-QIP. In addition, PSB will advise the former Chairman and Commissioners who have retained their NRC security clearances, congressional staff members, and contractor organizations directly.
4. Each individual must complete the security forms in e-QIP and return the forms to PSB by the specified date. If a Government employee or contract employee fails to submit the forms by the specified date, PSB will take additional steps to further notify the individual, up to and including notification to the division director, who may be administratively terminated.
5. Upon favorable review of the investigation, PSB will provide OCHCO with an Official Personnel Folder copy of the certification of investigation to be retained in the employee's personnel file.
6. Individuals approved for access authorizations are subject to continuous monitoring requirements as set forth by OPM criteria which is subject to change at OPM's discretion.



**L. Termination of Access Authorization**

1. Access authorization will be terminated and a security termination statement (NRC Form 136, "Security Termination Statement") must be signed when—
  - (a) An NRC employee, consultant, or contractor is separated from employment with NRC.
  - (b) A non-NRC employee is separated for a period of over 90 calendar days or more from activities for which he or she was granted an access authorization.
  - (c) Access authorization is no longer required.
2. Upon the voluntary or involuntary separation (for example, death) from employment or the revocation of clearance of a person who holds an NRC access authorization, the employing office at headquarters or the regional office or facility (for example, an NRC contractor) must, at a minimum—
  - (a) Provide prompt notification of the termination of employment to PSB.
  - (b) Ensure that all classified and sensitive unclassified documents charged to the person are accounted for and properly disposed of.
  - (c) Arrange for the immediate return of badges, passes, and other forms of official identification to the responsible NRC security point of contact.
  - (d) Notify PSB to remove the individual's name from all access lists.
  - (e) Ensure that combinations to which the person had access are changed.
  - (f) Arrange for the person's name to be removed from access permissions to critical or sensitive areas, such as telephone closets and computer rooms.
3. The completed and signed security termination statement must be forwarded to PSB for retention.
4. 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, the sponsoring office or COR must promptly notify PSB. Measures similar to those specified in Sections II.L.2(b) through (f) of this handbook, determined on a case-by-case basis, must be used.

**M. Clearance Suspension and Revocation**

The process for clearance suspension and/or revocation is contained in 10 CFR Part 10.

1. An NRC employee whose clearance has been suspended is subject to indefinite suspension pending a final determination on eligibility for continuance of his or her security clearance.

2. A contractor whose clearance has been suspended will be removed from the NRC contract pending the outcome of the suspension review and the final determination.
3. When a licensee employee's clearance is suspended, the licensee is notified of the suspension. Continued employment of the individual is at the licensee's discretion, barring any access to classified information.
4. Any individual whose clearance has been suspended may not access any level of classified information or NRC sensitive information until a final determination is reached.
5. In accordance with Presidential Policy Directive (PPD) 19, "Protecting Whistleblowers with Access to Classified Information," signed by President Obama on October 10, 2012, the U.S. Nuclear Regulatory Commission (NRC) has instituted a review process that permits employees to appeal actions affecting eligibility for access to classified information (i.e., adversely affecting their security clearance) that they allege have been taken in retaliation for protected disclosures (whistleblowing).

**N. Termination of Contractor Unescorted Building Access (BA), Information Technology (IT) Access, Power Reactor Access, and Safeguards Information (SGI) Access**

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

**O. Badging Requirements in Homeland Security Presidential Directive-12 (HSPD-12)**

As a condition of being issued an NRC Personal Identity Verification Badge (PIV), Homeland Security Presidential Directive 12 (HSPD-12) requires new employees and contractor employees to provide two forms of identification at the time of fingerprinting and photo collection for the NRC badge. More detailed information can be found on the NRC internal Web site at <http://www.internal.nrc.gov/ADM/index.html>.

### **III. CONTROL OF VISITS INVOLVING CLASSIFIED INFORMATION**

**A. Introduction**

This section provides standards and procedures 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.

**B. General**

1. Before disclosing classified information to any visitor, the sponsoring office must confirm the visitor's identity, need-to-know, and level of access authorization.
2. NRC or contractor officials (for example, supervisors) must ensure that visit requests are submitted at least 7 workdays before the visit to allow for timely notification of the person or facility to be visited.
3. Continuing visit approval for 1 year or less may be granted for repeated visits to the NRC, the U.S. 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 (for example, Secret), and the same type of classified information (for example, RD).
4. Visit requests of an unusual or emergency nature for which timely notification cannot be given may be transmitted to PSB by facsimile, telephone, or e-mail. Telephone arrangements must be immediately confirmed with PSB in writing. Visit requests that are not in writing or that do not provide timely notification may not be accepted at some facilities.
5. Classified information must not be given to individuals who possess a no clearance (NC) HSPD-12 badge.
6. 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.
7. The NRC office, NRC contractor, or other NRC activity visited must establish appropriate administrative controls over the activity of approved visitors to ensure that they are given access only to the authorized classified information.
8. 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.
9. If appropriate, the visitor should confirm in advance with the facility to be visited that necessary approvals have been received.
10. Access to RD requires a "Q" or "L" access authorization, depending on the classification level of the RD, except as provided in Section I.D.1 of this handbook.
11. Visits to NRC offices or divisions, except as indicated in Section I.C.1(a) of this handbook, 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 Access Approval," or in an appropriate written request containing the following information:

- (a) Identity of each visitor, including full name, social security number, citizenship, date of birth, place of birth, and organization with which the visitor is affiliated.
  - (b) Access classification level and type of information (for example, RD or NSI).
  - (c) Access authorization level ("Q," "L," Top Secret, Secret, or Confidential) and the need-to-know of each person certified by an appropriate official.
  - (d) Purpose of the visit.
  - (e) Name and location of facility(ies) to be visited.
  - (f) 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.)
  - (g) Name, title of position, organization, and telephone number of the person who prepared the request.
12. Requests for visits to the NRC, NRC contractors, or other NRC facilities by individuals outside NRC should be faxed to (301) 415-0245 or sent to the following address:
- U.S. Nuclear Regulatory Commission  
Chief, Personnel Security Branch  
Division of Facilities and Security  
11555 Rockville Pike  
Rockville, MD 20852
13. 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 concerning a conference or other such activity, the express permission of the person responsible for the activity must be obtained. Also, records that are released must be protected in accordance with MD 12.2, "NRC Classified Information Security Program," and the Freedom of Information Act of 1966 (5 U.S.C. 522).

### **C. Outgoing Visits by NRC Employees, Contractors, and Licensees**

- 1. For visits by NRC employees, contractors, and licensees to NRC headquarters, regional offices, and the Technical Training Center, a request for visit or access approval (NRC Form 277) is not necessary. The NRC cleared individual's HSPD-12 photo-identification badge will serve to identify the individual and the access authorization held.
- 2. For visits to NRC contractors, licensees and their related facilities, and other Government agencies or their contractors, NRC cleared individuals should submit NRC Form 277 to PSB at least 7 workdays before the initial date of the visit. When acting as representatives of the Federal Government in their official capacities, NRC

regional inspectors, Office of Investigations (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.

3. 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, NRC Form 277 should be submitted to PSB at least 15 workdays before the initial visit date.
4. For visits to facilities performing work on naval reactors for DOE, NRC Form 277 should be received at least 15 workdays before the initial visit date, especially for visits that do not involve inspections.
5. For visits to non-NRC facilities, an NRC Form 277 or other written request for visit or access approval should be completed by the NRC office or division establishing the individual's need-to-know and purpose of the visit, then submitted to PSB for verification of access authorization. PSB forwards the visit request to the facility to be visited. At those contractor or licensee facilities at which the NRC is not the CSA, the visit control procedures of the CSA will be followed.
6. NRC consultants who plan to visit NRC employees directing or monitoring their consultant interests will not be required to submit 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.

#### **D. Incoming Visitors**

##### **NOTE: THE NRC DOES NOT ACCEPT INTERIM CLEARANCES.**

##### 1. Required Information

The information listed below must be provided to the NRC from the visitor's employing agency on that agency's letterhead or on a form signed by that agency's security officer. The following information is required for incoming visitors:

- (a) The visitor's full name,
- (b) The visitor's social security number,
- (c) The visitor's date of birth,
- (d) The visitor's place of birth, including the city and state,
- (e) The visitor's agency affiliation,
- (f) The purpose of the visit,

- (g) The date of the visit,
- (h) The name of the person to be visited,
- (i) The type of access required,
- (j) The level of clearance, and
- (k) The last investigation date and type.

2. Restricted Data (RD)

RD in the possession of the NRC, its contractors, or in NRC facilities must not be released to an individual unless the individual has the appropriate NRC or DOE access authorization, and the need for access has been properly certified by the security office.

3. National Security Information (NSI)

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 program office to be visited.

4. Other Classified Information

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 PSB for processing and approval.

5. Representatives of Other Agencies

If authorized by the Director of DFS, representatives of other agencies (for example, the FBI or OPM) acting in their official capacities may, upon presentation of proper credentials, be granted access to classified information. In case of doubt about identity or the level of access authorized, PSB will verify these credentials or the level of access by contacting a security official of the agency or activity involved.

6. Members of Congress and Congressional Staff

Visits to the NRC, NRC contractors, or other activities associated with NRC programs involving access to RD or other classified information by members of Congress may be approved by headquarters office directors, headquarters division directors, or by regional administrators. The identity of the visitors and their need-to-know 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 NRC Director of the Office of Congressional Affairs.

**E. Visits Involving Access to Sensitive Compartmented Information (SCI)**

1. Visitors to the NRC must have their SCI access authorization and need-to-know forwarded to the special security officer in NSIR. At a minimum, the information required for these visits should include the full name of the visitor, agency affiliation, purpose and date of the visit, name of the person to be visited, and the SCI compartments involved. This information may be provided by secure fax, telephone call from 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.
2. NRC employees visiting other Government agencies or departments, or their contractors, must 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 with the request for SCI or may be processed separately in accordance with the procedure specified in Section III.C.2 of this handbook.

**F. Visits Involving Access to Classified Information by Foreign Nationals Sponsored by Foreign Governments or International Organizations**

1. Requests for foreign nationals to visit the NRC, NRC contractors, or other activities associated with NRC programs must be forwarded to the Director of DFS by NSIR, Division of Security Operations (DSO). Any foreign national possessing a security assurance (i.e., clearance) from his or her government must be officially certified to NSIR/DSO by an authorized official of the foreign government sponsoring the visit, with the assistance of the Office of International Programs (OIP), if necessary
2. If the foreign nationals do not possess security assurance, OIP will request NSIR/DSO, conduct investigative checks. For further guidance on the disclosure of classified information to foreign nationals refer to MD 12.2.
3. Representatives of the International Atomic Energy Agency (IAEA) who are authorized to make visits to or inspect NRC-licensed facilities in accordance with the Agreement Between the United States of America and the International Atomic Energy Agency for the Application of Safeguards in the United States (and Protocol Thereto), November 18, 1977, available at <http://www.state.gov/t/isn/5209.htm>, 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.

**G. Visits to Foreign Governments or Activities by NRC Personnel**

1. For visits to foreign governments or activities by NRC personnel, NRC Form 277 should be submitted to PSB for processing and coordination with OIP when classified information is involved. If NRC Form 277 is not available, the information listed in Section III.D.1 of this handbook should be submitted to PSB.
2. These visit requests should be submitted at least 30 calendar days in advance of the initial visit date.

**H. Records of Visit Requests**

Records of visit requests consisting of 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.

**IV. ASSIGNMENT OF FOREIGN REGULATORY EMPLOYEES TO THE NRC****A. Introduction**

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 OIP; ADM, DFS; supervisors; and employees are outlined below.

**B. Activity Plans**

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.

**C. Assignments**

1. Consideration for assignments will be given in the following order:
  - (a) Nationals from developing countries building or operating U.S.-type light-water reactors.
  - (b) Nationals from other countries with which the NRC has entered into information exchange and cooperation arrangements.
  - (c) Nationals from the IAEA member states sponsored in accordance with the IAEA Fellowship Program, if different from Sections IV.C.1(a) and IV.C.1(b) of this handbook.
  - (d) Other foreign nationals as decided on a case-by-case basis.



2. Within each of these categories, preference will be given, in general, to nationals from countries that are parties 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.
3. All personnel accepted for NRC assignments of should—
  - (a) Be fluent in English;
  - (b) Have successfully completed an NRC-approved English language foreign competency examination;
  - (c) Have professional training, experience, or education; and
  - (d) 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.
4. 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 to minimize the impact on NRC employees. 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 the assignee's institution. Assignees will normally be given duties similar to those of NRC employees, without special "diverse experience" assignments (i.e., the assignment will not be tailored diversify the assignee's skills, but rather, duties will be similar to NRC employees who have the same position), except when convenient to the NRC.
5. 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 by the staff and at least 5 workdays 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.
6. OIP will forward all formal NRC letters of invitation accepting proposed assignments to the U.S. Department of State 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.

7. OIP approves or disapproves the assignment of a foreign national to the 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.
8. Foreign nationals will not be assigned to the Commission, the Office of the Secretary, the Office of the Executive Director for Operations, office directors, or 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.

#### **D. Background Check**

Before inviting the foreign regulatory employee to join the NRC, OIP will obtain the required background and biographical data and submit the data to PSB with a request that the appropriate indices checks be conducted by the appropriate agencies (the Central Intelligence Agency, the FBI, and the U.S. Department of State). Information that creates a question as to whether assignment of the foreign national is consistent with national interest will be evaluated by PSB and forwarded with a recommendation to OIP.

#### **E. Assignee Agreements**

Foreign assignees will be required to sign a commitment patterned after the agreement signed by 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 employees receive and use this information. The signing of the confidentiality agreement by the assignee is a condition of the assignment in accordance with the terms of the agency-to-agency agreement that both the NRC and the foreign regulatory agency sign. Specific procedures are as follows:

1. 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 will ensure that all documents on the assignee's list are returned.
2. Access to special classes of information, including details of facility security plans, material control and accounting information, and SGI that is subject to 10 CFR 73.21, must not be granted unless approved by NSIR.

**F. Security Plans**

1. 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 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:
  - (a) Description of the physical location of the assignment within NRC, a licensee facility, or another facility.
  - (b) Identification of specific areas to which the assignee is to be given unescorted access to perform essential responsibilities. (The assignee's access should be consistent with the requirements of DFS and the assignments of the host office.)
  - (c) Explanation of special badging required and associated restrictions.
  - (d) Explanation of restrictions on the use of, or connection to, NRC computing resources such as LANs, other NRC computing systems, document management systems, and sensitive data.
  - (e) Discussion of the ways in which commercial or foreign proprietary information must be protected if the assignment requires access to this information. (Assignments should normally be tailored so that they do not require access to this information.)
  - (f) 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.
  - (g) Assignment of a supervisor and an alternate to monitor the assignee's day-to-day activities.
  - (h) 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.)
  - (i) 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.)
2. 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.

3. 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.
4. Co-workers and other NRC employees in the assignee's area also will be made aware of the requirement for the assignee to wear the 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.
5. 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.

#### **G. Assignee Responsibilities**

1. Assignees will not authorize visits by other individuals to the NRC, NRC contractors, or other NRC facilities.
2. Assignee duties are to be limited to those that do not require representing the NRC in public or acting as an official representative in meetings with NRC licensees.
3. 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.

#### **H. Evaluation of Assignees**

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

### **V. NRC'S DRUG-FREE WORKPLACE PLAN**

#### **A. General**

1. NRC's Drug-Free Workplace Plan sets forth objectives, policies, procedures, and implementation guidelines to achieve a drug-free Federal workplace consistent with the following:
  - (a) Executive Order 12564 and

- (b) Section 503 of the Supplemental Appropriations Act of 1987 (Public Law 100-71).
2. NRC's program consists of the following:
    - (a) An Employee Assistance Program,
    - (b) Supervisory training,
    - (c) Employee education, and
    - (d) Random drug testing.
  3. NRC's drug testing follows procedures specified in the Department of Health and Human Services (HHS) Mandatory Guidelines for Federal Workplace Drug Testing Programs (available at <http://www.internal.nrc.gov/announcements/yellow/2010/2010-122.html>). Current HHS guidelines supersede all previous issues of guidance.

#### **B. NRC's Drug Testing Program**

1. NRC's Drug Testing Program, which is administered by PSB includes the following types of testing:
  - (a) Random,
  - (b) Applicant,
  - (c) Reasonable suspicion,
  - (d) Post-accident,
  - (e) Voluntary, and
  - (f) Followup.
2. All NRC employees and any individuals who are tentatively selected for employment at the NRC and who have not, immediately before selection, been subject to random drug testing, are included in the random drug testing pool.
3. Specific policies and procedures are reflected in the following:
  - (a) NRC Drug-Free Workplace Plan, available at NUREG/BR-0134, Rev. 2, dated March 2007, and at Yellow Announcement 08-040, "General Notice of NRC Drug Testing Program Changes and Notice of Employee Awareness Sessions," as the revised NRC Drug-Free Workplace Plan, dated August 2007, and
  - (b) NRC Drug Testing Manual, NUREG/BR-0136, August 2008.

**C. Deferral of Drug Testing**

According to the NRC Drug-Free Workplace Plan, an employee randomly selected for drug testing may be deferred from testing that day if the employee meets one of the following criteria:

1. The employee is in a prior approved leave status.
2. The employee is in official travel status away from the test site.
3. The employee is about to embark on official travel which was scheduled before testing notification.

**D. Drug Testing when an Employee is Working under the NRC's Flexiplace Program**

1. When an employee is working from a non-NRC worksite under the NRC's Flexiplace Program, they continue to be subject to random drug testing. If notified, the employee is required to report to the designated drug testing office on the day of notification. A reasonable timeframe will be established and agreed upon by the Drug Testing Program manager and the donor's supervisor.
2. Employees working full-time under the NRC's Flexiplace Program may be directed to report to a preapproved subcontractor drug testing facility. Usually, the subcontractor drug testing facility is within a 2-hour drive from the employee's duty location.

**E. Positive Drug Test Result**

1. An employee who tests positive for illegal drugs shall be subject to the provisions of Part VIII of the NRC's Drug-Free Workplace Plan.
2. A contractor who tests positive for illegal drugs is immediately physically removed from NRC-controlled space. The contractor's badge shall be de-activated and LAN access denied, and he/she may not work on any NRC contract for a period of not less than 1 year from the date of the failed drug test. In addition, the contractor will not be considered for reinstatement unless the NRC's Medical Review Officer (MRO) determines there is evidence of rehabilitation.

**Exhibit 1 Security Orientation Briefing for New NRC and Contractor Employees**

A security orientation briefing must be given to NRC national security information (Q, L(H), L) 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), Office of Administration (ADM), or in a regional office by a regional security representative. The briefing will include the following:

1. Information about the type of security clearances and access approvals granted by the NRC and the access those clearances and approvals afford after an official need-to-know has been established.
2. Information about the personnel security reporting responsibilities of each individual.
3. Prescribed procedures for the storage and handling of classified information and sensitive but unclassified information and the importance of protecting this information.
4. Information about physical security aspects, the importance of visitor control, and the types of procedures of the particular facility for protecting Government property. Contractors are not allowed to escort visitors unless prior approval has been granted by DFS.
5. Notification to all NRC employees in regard to the random drug testing pool and the requirements to comply with the NRC's Drug-Free Workplace Plan.
6. Notification of the responsibilities associated with the issuance of a government photo identification badge (HSPD-12).
7. Information on where to obtain further guidance or assistance.

Those individuals granted access authorizations are required to complete SF-312, "Classified Information Non-Disclosure Agreement," which is maintained by the Personnel Security Branch, DFS, ADM.

**Exhibit 2 Standard Operating Procedures for Pre-Employment Screening of NRC Applicants**

- A.** The headquarters Office of the Chief Human Capital Officer (OCHCO) specialist or the regional HR Officer (HRO) will obtain a current resumé and the following security forms:
1. Signature pages from the Questionnaire for National Security Positions (e-QIP, SF- 86, "Questionnaire for National Security Positions" (QSP)) (initiated by the Office of Administration (ADM), Division of Facilities and Security (DFS), Personnel Security Branch (PSB) in e-QIP);
  2. Two fingerprint charts;
  3. NRC Form 236, "Personnel Security Clearance Request and Notification";
  4. NRC Form 176, "Security Acknowledgement/Access Authorization";
  5. OF-306, "Declaration for Federal Employment" (available from OCHCO or PSB); and
  6. The Fair Credit Reporting Act (FCRA) release.
- B.** The OCHCO specialist or the regional HRO will ensure that appropriate reference checks are conducted using the resumé as the source document. Once the security package is complete, OCHCO will forward it to PSB for processing.
- C.** The following additional requirements apply and will be conducted by OCHCO and submitted to PSB:
1. All personnel conducting reference checks must be thoroughly familiar with the reference check process and appropriate reference check techniques.
  2. In all cases, OCHCO will verify dates of attendance at the educational institution, the highest educational level attained, and the type and year of degree.
  3. In cases where applicants are naturalized citizens, include a legible copy of the Naturalization or Citizenship Certificate.
- D.** The OCHCO specialist or the HRO will review the results of all the reference checks to determine acceptability of the applicant. If either the OCHCO specialist or the HRO has any doubt as to the applicant's suitability, then OCHCO and the program or regional office will render a determination that will be forwarded to PSB along with the rest of the security forms.
- E.** Upon receipt of the security forms, PSB will—
1. Request fingerprint and credit checks on the selectee.
  2. Conduct applicable database checks of the selectee.



3. 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.
4. Evaluate the eligibility of the applicant for a Section 145b of the Atomic Energy Act (AEA) 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.
5. If the result of the pre-employment review does not warrant a Section 145b approval, OCHCO is notified to take appropriate action to determine whether to rescind the offer or authorize PSB to continue processing the request to OPM for the background investigation. Upon receipt of the report of investigation, PSB will review the report to mitigate any security concerns identified during the pre-employment review and determine the outcome of the clearance request.

**Exhibit 3 “Q,” “L(H),” and “L” Reinvestigation Program Requirements****A. “Q” and Sensitive Compartmented Information (SCI) Reinvestigation Requirements**

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

1. Each individual to be reinvestigated must submit a new Questionnaire for National Security Positions (QSP) (e-QIP, Standard Form 86) and related forms. These forms will be the basis for an investigation as specified below.
2. An Office of Personnel Management (OPM) single-scope background investigation or a periodic reinvestigation (SSBI-PR or a Phased Periodic Reinvestigation (PPR)) will be conducted for “Q” cleared individuals other than the following:
  - (a) The Chairman,
  - (b) The Commissioners, and
  - (c) The Inspector General.
3. The Chairman, the Commissioners, and the Inspector General are subject to a Federal Bureau of Investigation (re)investigation concerning their Presidential appointment.
4. Further investigative coverage may be undertaken on a case-by-case basis if the scheduled coverage is insufficient to obtain the required information.

**B. “L(H)” and “L” Reinvestigation Program Requirements**

Each individual to be reinvestigated must submit a new QSP via e-QIP and related forms. These forms will be the basis for an investigation as follows:

1. A national agency check with law and credit (NACLC) will be conducted. The investigation may be expanded as necessary to determine if access is clearly consistent with national security.
2. Further investigative coverage may be undertaken on a case-by-case basis if the scheduled coverage is insufficient to obtain the required information.

**C. OPM Reinvestigation Requirements**

Individuals approved for access authorizations are subject to continuous monitoring requirements as set forth by OPM criteria which is subject to change at OPM's discretion.

**D. Fingerprints Requirement**

Although not normally required for “Q,” “L(H),” or “L” reinvestigations, a new set of fingerprint cards will be requested every 10 years or on a case-by-case basis.

**Exhibit 4 Security Clearances/Access Types**

<b>SECURITY CLEARANCES/ ACCESS TYPES</b>	<b>INVESTIGATION REQUIRED</b>	<b>AUTHORIZES ACCESS TO THE FOLLOWING INFORMATION (WITH AN ESTABLISHED NEED-TO-KNOW)</b>
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/Confidential (C) National Security Information, Restricted Data
L- High Public Trust (L(H)) (Secret)	OPM SSBI, with National Agency Check with law and credit (NACLC) every 5 years	S/C National Security Information  C - Restricted Data
L - Secret (S)	Access National Agency Check with Inquiry (ANACI) and 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
Information Technology (IT) Level I Access	Minimum Background Investigation (MBI), with NACLC reinvestigations every 10 years	NRC Sensitive IT Systems or Data for the development, direction, implementation, and administration of NRC computer programs

<b>SECURITY CLEARANCES/ ACCESS TYPES</b>	<b>INVESTIGATION REQUIRED</b>	<b>AUTHORIZES ACCESS TO THE FOLLOWING INFORMATION (WITH AN ESTABLISHED NEED-TO-KNOW)</b>
IT Level II Access	NACLCL, with NACLCL reinvestigations every 10 years	NRC Sensitive IT Systems or Data, including those individuals needing an NRC Local Area Network (LAN) account
Building Access	NACI, with NACLCL reinvestigations every 10 years	Unescorted access to NRC facilities for vendors, health unit, housekeeping personnel
Child Care Access	NACI, with NACLCL reinvestigations every 5 years	Unescorted access to NRC facilities for childcare staff
Atomic Energy Act, Section 145b, pre-appointment investigation waiver	Standard Form (SF)-86, "Questionnaire for National Security Positions" (QSP), Federal Bureau of Investigations Fingerprint, credit, employment references, and education check conducted	Safeguards Information, Proprietary Information, and Official Use Only information
Unescorted Access to Power Plants	Access National Agency Check with Inquiry (ANACI) and NACLCL for reinvestigations every 10 years	Unescorted access to protected and vital areas of nuclear power facilities; access to safeguards information; and unescorted access to NRC facilities.