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

MD 12.3	NRC PERSONNEL SECURITY PROGRAM	DT-22-04
Volume 12:	Security	
Approved By:	Jennifer M. Golder, Director Office of Administration	
Date Approved:	July 18, 2022	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of Administration Division of Facilities and Security	
Contact Name:	Elizabeth Fowble	Lisa Nichols-Streck

EXECUTIVE SUMMARY

Management Directive (MD) 12.3, "NRC Personnel Security Program," is revised to reflect changes in the personnel security program, specifically—

- The removal of Section IV, "Assignment of Foreign Regulatory Employees to the NRC." This information is in MD 12.1, "NRC Facility Security Program."
- The addition of the Continuous Vetting (CV) Program information in Section II.L.
- Incorporating Security Executive Agent Directives (SEAD) updates such as SEAD 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position."
- Administrative changes to include organizational changes and hyperlink updates.

TABLE OF CONTENTS

I. POLICY....2

II. OBJECTIVE....3

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY....3

A. Commission....3

B. Executive Director for Operations (EDO)....3

For updates or revisions to policies contained in this MD that were published after the MD was signed, please see the Yellow Announcement to Management Directive index (YA-to-MD index).

C. Deputy Executive Director for Materials, Waste, Research, State, Tribal, Compliance, Administration, and Human Capital Programs (DEDM) 3
D. General Counsel (GC) 4
E. Office of the Inspector General (OIG) 4
F. Director, Office of Administration (ADM) 4
G. Director, Office of Investigations (OI) 5
H. Chief Human Capital Officer (CHCO) 5
I. Director, Office of Nuclear Security and Incident Response (NSIR) 5
J. Office Directors and Regional Administrators 5
K. Director, Division of Facilities and Security (DFS), ADM 6
IV. APPLICABILITY 6
V. DIRECTIVE HANDBOOK 6
VI. EXCEPTIONS OR DEVIATIONS 7
VII. REFERENCES 7

I. POLICY

A. It is the policy of the U.S. Nuclear Regulatory Commission (NRC) 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; and
8. Visits involving classified National Security Information (NSI), Restricted Data (RD), or Sensitive Compartmented Information (SCI).

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)

1. 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.
2. 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, Division of Facilities and Security (DFS), Office of Administration (ADM).

C. Deputy Executive Director for Materials, Waste, Research, State, Tribal, Compliance, Administration, and Human Capital Programs (DEDM)

1. Performs the functions assigned to the Deputy Executive for Materials, Waste, Research, State, Tribal, Compliance, Administration and Human Capital Programs (DEDM) in accordance with 10 CFR Part 10, including granting, suspending, denying, or revoking 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. 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.

5. Establishes in writing, in accordance with the authority in Section 145g of the AEA, standards and specifications 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 with information obtained in audits and investigations that is relevant to security issues consistent with the Inspector General (IG) Act, and 10 CFR 1.12, "Office of the Inspector General."

F. Director, Office of Administration (ADM)

1. Performs the functions assigned to the Office of Administration (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 and the DEDM relative to clearance, suspension, and denials.

2. Oversees the NRC personnel security program as carried out by DFS.

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

G. Director, Office of Investigations (OI)

1. Coordinates with DFS whenever information derived from DFS files alone and not corroborated by other means are used in OI reports.
2. Provides security-related information to DFS 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.

H. Chief Human Capital Officer (CHCO)

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

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

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

J. 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 of any information that indicates noncompliance with MD 12.3 or that is otherwise pertinent to the proper protection of classified information, Controlled Unclassified Information or NRC property.
4. Notify DFS of individuals under their jurisdiction who possess an access authorization, or for whom an access authorization has been requested, who are hospitalized or otherwise treated for an illness or mental condition that may cause defects in their judgment, trustworthiness, or reliability, and of any subsequent developments as discussed in the handbook to this directive.

5. Notify DFS 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 all alleged or suspected incidents of employee or contractor fraud, misconduct, unauthorized disclosure, or misuse of automated information systems.

K. 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, 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, Defense Counterintelligence and Security Agency (DCSA) and other investigative agencies on NRC personnel security matters.

4. Recommends to the EDO approval of Section 145b waiver of the AEA 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, Atomic Safety and Licensee Board Panel members, applicants for employment, other persons designated by the DEDM, and 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, and drug testing.

VI. EXCEPTIONS OR DEVIATIONS

Exceptions to or deviations from the NRC Personnel Security Program described in MD 12.3 may be granted by the Director of DFS in writing, except for those areas in which the responsibility or authority is vested solely with the Commission, the DEDM, or the Director of ADM, and is nondelegable, or for matters specifically required by law, 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 https://www.federalregister.gov/documents/2017/01/23/2017-00979/mandatory-guidelines-for-federal-workplace-drug-testing-programs.

SEAD 7, "Reciprocity of Background Investigations and National Security Adjudications."

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, “Recruitment, Appointments, and Merit Staffing.”

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.”

Memorandum from Joseph M. Hendrie, Chairman, to Lee V. Gossick, Executive Director for Operations, “Delegation of Authority to Approve Employment of an Individual by NRC Prior to Completion of Security Investigation,” dated January 24, 1979.(ML17286A476).

NRC Forms Library on SharePoint: https://usnrc.sharepoint.com/teams/NRC-Forms-Library/SitePages/Home.aspx.

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.

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 https://www.state.gov/09-106.

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.

Security Executive Agent Directives (SEADs)

SEAD 1, "Security Executive Agent Authorities and Responsibilities."

SEAD 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position."

SEAD 4, "National Security Adjudicative Guidelines."

SEAD 5, "Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications."

SEAD 6, "Continuous Evaluation."

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)

DH 12.3	NRC PERSONNEL SECURITY PROGRAM	DT-22-04
Volume 12:	Security	
Approved By:	Jennifer M. Golder, Director Office of Administration	
Date Approved:	July 18, 2022	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of Administration Division of Facilities and Security	
Contact Name:	Elizabeth Fowble	Lisa Nichols-Streck

EXECUTIVE SUMMARY

Management Directive (MD) 12.3, "NRC Personnel Security Program," is revised to reflect changes in the personnel security program, specifically—

- The removal of Section IV, "Assignment of Foreign Regulatory Employees to the NRC." This information is in MD 12.1, "NRC Facility Security Program."
- The addition of information about the Continuous Vetting (CV) Program.
- Incorporating Security Executive Agent Directives (SEAD) updates such as SEAD 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position."
- Administrative changes to update information within the MD.

TABLE OF CONTENTS

I. NRC ACCESS TYPES 4

A. Introduction 4
B. Position Sensitivity Criteria 4
C. Special Sensitive Positions of a High Degree of Importance or Sensitivity for Sensitive Compartmented Information (SCI) 4
D. Positions of a Critical-Sensitive Designation that Require a "Q" Clearance 5

E. Positions of High Public Trust that Require an "L(H)" Clearance....5
F. "L" Positions of a Noncritical-Sensitive Designation....5
G. Access Authorization Requests....6
H. Contractual Language for Unescorted Access by NRC Contractors....9
I. Access to Controlled Unclassified Information//Specified (CUI//SP)-Safeguards Information (SGI) by NRC Contractors....11
J. Contractors or Consultants Requiring Access Authorizations ("Q," "L(H)," or L Clearances)....11
K. Contractors or Consultants Requiring Access to NRC Information Technology (IT) Systems or Controlled Unclassified Information (CUI) (formerly SUNSI)....14
L. Contractors or Consultants Requiring Building Access (BA) to NRC Facilities....17
M. Removing a Contractor or Consultant from a Contract and/or Task Order....20
N. Adding Another Contract and/or Task Order to an Existing NRC Contractor or Consultant....20
O. Transferring an NRC Contractor or Consultant....21
P. Upgrading an NRC Contractor or Consultant....21
Q. Downgrading an NRC Contractor or Consultant....22

II. INVESTIGATIONS AND DETERMINING ELIGIBILITY FOR ACCESS AUTHORIZATION....23

A. Investigations....23
B. Reciprocity of "Q," "L(H)," and "L" Access Authorization....23
C. Reopening of Canceled Cases....24
D. Pre-Appointment Investigation Waiver with No Access to Classified Information....24
E. Circumstances Affecting Eligibility for Access Authorization....26
F. Determination of Eligibility for Access Authorization....26
G. Temporary Access to Classified Information....27
H. Access Authorization for Dual Citizens....28
I. Access Authorization for Non-U.S. Citizens....28
J. Personnel Reporting Responsibilities....29
K. Reinvestigation Program....33
L. Continuous Vetting (CV) Program....34
M. Termination of Access Authorization....35
N. Clearance Suspension and Revocation....35

O. Termination of Contractor Unescorted Building Access (BA), Controlled Unclassified Information, and Power Reactor Access 36
P. Badging Requirements in Homeland Security Presidential Directive-12 (HSPD-12) 36
III. CONTROL OF VISITS INVOLVING CLASSIFIED INFORMATION 36
A. Introduction 36
B. General 37
C. Outgoing Visits by NRC Employees, Contractors, and Licensees 38
D. Incoming Visitors 39
E. Visits Involving Access to Sensitive Compartmented Information (SCI) 40
F. Visits Involving Access to Classified Information by Foreign Nationals Sponsored by Foreign Governments or International Organizations 41
G. Visits to Foreign Governments or Activities by NRC Personnel 41
H. Records of Visit Requests 42
I. Withdrawal of Active Visit Request 42
IV. NRC'S DRUG-FREE WORKPLACE PLAN 42
A. General 42
B. NRC's Drug Testing Program 43
C. Deferral of Drug Testing 43
D. Drug Testing When an Employee is Working Under the NRC's Telework Program 43
E. Positive Drug Test Result 44

EXHIBITS

Exhibit 1 Security Orientation Briefing for New NRC and Contractor Employees 45
Exhibit 2 Standard Operating Procedures for Pre-Employment Screening of NRC Applicants 46
Exhibit 3 "Q," "L(H)," and "L" Reinvestigation Program Requirements 48
Exhibit 4 Security Clearances/Access Types 49

I. NRC ACCESS TYPES

A. Introduction

1. The U.S. Nuclear Regulatory Commission (NRC) reviews and makes eligibility determinations for NRC access authorization and 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 Controlled Unclassified Information//Specified (CUI//SP)-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. 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 (as described in 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 Notices; NRC-39, “Personnel Security Files and Associated Records-NRC”; and NRC-35, ”Drug Testing Program Records.”

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 based on a Tier 5 (T5) investigation by the agency’s investigation service provider, or the equivalent conducted by other Federal agencies, or an “L” security clearance, as a minimum, based on a Tier 3 (T3) investigation or equivalent.

C. 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 a T5 or equivalent in accordance with Section 145f of the Atomic Energy Act of 1954 (AEA), as amended. These positions include—

1. The Chairman,

2. An NRC Commissioner,

3. The Inspector General, and

4. Any person who requires access to sensitive compartmented information.

D. 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 a T5 or equivalent. Functions considered critical-sensitive and requiring a "Q" clearance have one or more of the following characteristics:

1. Access to Secret or Top Secret-Restricted Data or Top Secret National Security Information.

2. Access to Confidential Restricted Data involving broad naval nuclear propulsion program policy or direction.

   (a) 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.

   (b) 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.

E. 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 a T5 or equivalent. The types of functions considered to be of high public trust include—

1. Final approval of plans, policies, or programs that directly affect the overall operations and direction of the NRC.

2. 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.

3. Duties performed by resident inspectors.

4. Other duties requiring high public trust as determined, on an as-needed basis, by the Deputy Executive Director for Materials, Waste, Research, State, Tribal, Compliance, Administration, and Human Capital Programs (DEDM).

F. "L" Positions of a Noncritical-Sensitive Designation

People in any NRC position not covered by Sections I.B.1-3 of this handbook require an NRC "L" access authorization based on a T3 investigation or equivalent.

G. 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), NRC experts, Atomic Safety and Licensee Board Panel members, and consultants must be submitted through the Office of the Chief Human Capital Officer (OCHCO) or the Office of the Inspector General (OIG), Human Resources staff, as appropriate, to the Office of Administration (ADM).

(b) An NRC OCHCO or OIG Human Resources officer is responsible for submitting NRC Form 236, "Personnel Security Clearance Request and Notification," available in the NRC Forms Library in SharePoint at https://usnrc.sharepoint.com/teams/NRC-Forms-Library/SitePages/Home.aspx 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 the submitting office 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 OIG, Human Resources officer.

(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.

(i) For "Q" and "L(H)" clearances, the applicant must meet the immediate 10-year U.S. residency coverage requirement.

(ii) For "L" clearances, the requirement is the immediate 7-year U.S. residency coverage period.

(d) 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 a background 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 its investigation service provider or another Federal agency, provides the basis for granting a clearance.

(e) Applicants living overseas for extensive periods (1 year or more, excluding for 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 are not eligible for temporary access

authorization due to the difficulty in obtaining investigative coverage overseas. Therefore, the 145b waiver will not be approved for such applicants. An applicant's overseas history may also result in the investigation service provider's delay or inability to conduct a background investigation in a timely manner, thus affecting the NRC's ability to process the final access authorization approval or clearance.

(f) A security orientation briefing must be given to NRC employees, NRC experts, Atomic Safety and Licensee Board Panel (ASLBP) members, and consultants requiring access authorizations when they enter duty status. This briefing will normally be given by a representative of DFS, ADM, 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) requiring access to the local area network (LAN) and/or unescorted building access (BA) must submit a request for access using NRC Form 850, "Request for Contractor Assignment(s)." A request for a contractor requiring a national security clearance is processed using NRC Form 850 and NRC Form 188, "Drug Testing Criteria Document." The requester must forward both forms electronically to PSB. See Section I.C.3 of this handbook, "Security Forms Packet for an Access Authorization Request."

(b) At contractor facilities where the 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 a personnel security clearance. A 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.") 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 a temporary access authorization approval. A background investigation conducted by its investigation service provider 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 are not eligible for temporary 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.

(d) Foreign nationals (non-U.S. citizens) are not eligible for a national security clearance. However, at the discretion of the DEDM ,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).

(e) A security orientation briefing must be given to NRC contractors granted national security clearances. This briefing normally will 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) Applicants must electronically certify Standard Form (SF)-86, “Questionnaire for National Security Positions” (QSP) (initiated by PSB), except BA applicants who are required to complete SF-85, "Questionnaire for Non-Sensitive Positions.”

(ii) Applicants need to submit electronic fingerprint images at an NRC facility. If an individual is not within 25 miles of an NRC facility, the applicant can inform OCHCO or PSB of their location. Then OCHCO or PSB will mail to the individual two applicant fingerprint cards (SF-87 for Federal employee applicants or FD-258, “FBI Fingerprint Card,” for contractors). Completed fingerprint cards must be returned to PSB.

(iii) NRC Form 176A, “Security Acknowledgment.”

(iv) Résumé (for NRC applicants; not required for contractors).

(v) NRC Form 236 (for NRC employees) and NRC Form 237 (for NRC licensees).

(vi) OF-306, “Declaration for Federal Employment,” provided by 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).

(b) PSB will reject 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) The forms are illegible.

(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 CUI//SP-SGI, or access to sensitive NRC IT systems, data, or facilities.

4. Canceled or Withdrawn Request

When a request for an applicant's access authorization is to be withdrawn or canceled, PSB should be notified immediately by email 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 canceled.

H. 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 CUI//SP-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 CUI//SP-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) Sponsoring office must include the NRC Form 187, “Contract Security and/or Classification Requirements,” available in 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 MD 11.1.)

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) Temporary Approval

Temporary approvals may be obtained by two methods.

(i) The contractor employee must submit a completed personnel security forms packet to PSB through the NRC contracting officer's representative (COR), including an SF 86. PSB will conduct criminal history and credit checks. Based on the result of these checks, DFS will determine the contractor employee's eligibility for temporary access and will indicate "objection" or "no objection" to the sponsoring office, pending completion of the required background investigation.

(ii) 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 licensee 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 that results 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 temporary 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 PSB.

(c) Resolving Questions of Eligibility

The investigation described in Exhibit 4 of this handbook may involve a Tier 3 or another investigation as PSB deems necessary. PSB 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 temporary or final unescorted access to nuclear power facilities or access to CUI//SP-SGI are subject to the reporting requirements set forth in Section II.J.1 of this handbook. The security officer or designee must promptly report the circumstances to PSB.

I. Access to Controlled Unclassified Information//Specified (CUI//SP)-Safeguards Information (SGI) by NRC Contractors

The NRC sponsoring office must decide whether performance in accordance with an NRC contract will involve access to CUI//SP-SGI. This access may require a National Agency Check with Inquiry (NACI) or other investigation as PSB deems necessary. Based on the review of the applicant's security forms by PSB, and/or the receipt of adverse information by the NRC, the individual may be denied access to CUI//SP-SGI until a final determination of eligibility for access is made. CUI//SP-SGI access for contractor employees may be granted in accordance with licensee programs. See MD 12.6, “NRC Controlled Unclassified Information (CUI) Program,” for more information.

J. Contractors or Consultants Requiring Access Authorizations (“Q,” “L(H),” or L Clearances)

1. Foreign nationals (non-U.S. citizens) are not eligible for a national security clearance.
2. Access to national security information requires a favorably adjudicated background investigation, a national security clearance, and the “need-to-know” justification.
3. CORs may be reported for a security infraction as described in MD 12.1 for situations in which their contractors or consultants do not follow the access procedures of MD 12.3.
4. Contractors or consultants for NRC security clearances at the "L," "L(H)," or "Q" level will be required to attend a security orientation briefing, given by a representative of PSB, and sign an SF 312, "Classified Information Nondisclosure Agreement," (available from PSB) before they are granted a security clearance.

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

Contractors or consultants in certain critical-sensitive positions must have an NRC "Q" clearance based on a Tier 5 background investigation. Functions considered critical-sensitive and requiring a "Q" clearance have one or more of the following characteristics:

(i) Access to Top Secret/Secret/Confidential National Security Information or Top Secret/Secret/Confidential Restricted Data.

(ii) Access to Confidential Restricted Data involving broad naval nuclear propulsion program policy or direction.

(b) Positions of High Public Trust That Require an “L(H)” Clearance

Contractors or consultants in positions of high public trust require an “L(H)” clearance based on a Tier 5 background investigation. Functions considered to be of high public trust and requiring an “L(H)” clearance have one or more of the following characteristics:

(i) Access to Secret/Confidential National Security Information.

(ii) Access to Confidential Restricted Data.

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

(iv) 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.

(v) Other duties requiring high public trust as determined on an as-needed basis by the DEDM.

(c) Positions of Noncritical-Sensitive Designation that require an “L” Clearance

Contractors or consultants in positions of Non-critical Sensitive designation require an "L" clearance based on a Tier 3 background investigation. Functions considered to be of Noncritical-Sensitive and requiring an "L" clearance have either or both of the following characteristics:

(i) Access to Secret/Confidential National Security Information.

(ii) Access to Confidential Restricted Data not related to broad naval nuclear propulsion program policy or direction.

5. Temporary Access Approval

(a) The COR will need to complete and submit a security package to the Personnel Security Branch (PSB). The security package consists of NRC Form 850, “Request for Contractor Assignment(s),” and the NRC Form 188, “Drug Testing Criteria,” which should be emailed to PSB_ContractorResourceInbox@nrc.gov.

(b) PSB will review the security package and make one of the following security decisions:

(i) The contractor or consultant has a background investigation that meets or exceeds the investigative requirement for the clearance (either Q, L(H), or L) and qualifies for contract performance through reciprocity; or the contractor or

consultant does not qualify for reciprocity and will be required to undergo a background investigation.

(ii) If PSB determines the contractor or consultant qualifies for reciprocity, then they will be granted the clearance (Q, L(H), or L). PSB will email the COR the clearance memo and any additional instructions. Note that as stated on the NRC Form 188, "Drug Testing Criteria," a contractor or consultant requiring a clearance needs pre-employment drug testing. PSB must wait for the results before granting the clearance.

(c) PSB will review the Standard Form (SF) 86, "Questionnaire For National Security Positions"; FBI fingerprint record check; credit check; and pre-employment drug test results to grant temporary IT-II Access and send the COR the temp IT access approval memo by email. PSB will forward the SF 86 to its investigation service provider for a full background investigation, which will be reviewed when it is completed. PSB does not grant temporary or interim security clearances (i.e., interim L or interim Q clearance).

6. Resolving Questions of Eligibility

(a) If there is a non-favorable initial review of the SF 86, FBI fingerprint check, credit check, and pre-employment drug test results, PSB will contact the COR, by email, and notify them that the contractor or consultant will not be granted temporary IT-II access. The COR should note that the contractor or consultant cannot support the contract and/or task order if they were not approved for temporary IT-II access and may not be escorted to support the contract. The COR will then be asked if they wish to continue processing the contractor, or consultant, or discontinue processing the security package and submit a new contractor or consultant. If the COR requests to continue processing the contractor or consultant, then the SF 86 will be forwarded its investigation service provider for a full background investigation. Furthermore, reviewing the investigation, potentially obtaining additional information from the contractor or consultant and/or third parties, and rendering an adjudicative determination may require additional time to complete. Based on the response from the COR, one of the following actions will happen.

(i) Discontinue processing – The COR notifies PSB to discontinue processing the contractor or consultant and submits a new security package for another contractor or consultant for the contract and/or task order.

(ii) Continue processing – The COR notifies PSB of their request to continue processing the contractor or consultant, even though temporary IT-II access will not be granted. PSB will forward the SF 86 to its investigation service provider and wait for the full background investigation to be completed. While the background investigation is pending, the COR is required to notify PSB if the contractor or consultant is no longer needed on the contract. Once the investigation is complete, PSB will review it; obtain additional information from

the contractor, or consultant, and/or third parties (if necessary); and render one of the following adjudicative determinations:

- If PSB makes a favorable adjudicative determination, then PSB will email the COR with the clearance memo (either Q, L(H), or L) and any additional instructions.
- If PSB does not make a favorable adjudicative determination, then PSB will advise the contractor or consultant of their appeal rights and notify the COR of the clearance denial.

(b) Final Approval or Disapproval - Upon receipt of the complete background investigation, PSB will then review it; obtain additional information from the contractor or consultant, and/or third parties (if necessary); and render one of the following adjudicative determinations:

(i) If PSB makes a favorable adjudicative determination, then PSB will email the COR with the clearance memo (either Q, L(H), or L) and any additional instructions.

(ii) If PSB does not make a favorable adjudicative determination, then PSB will advise the contractor or consultant of their appeal rights and notify the COR of the clearance denial.

K. Contractors or Consultants Requiring Access to NRC Information Technology (IT) Systems or Controlled Unclassified Information (CUI) (formerly SUNSI)

1. The Executive Director for Operations (EDO) approves the sensitivity criteria to be used in determining whether a contractor requires IT Level I or IT Level II approval for access to NRC IT systems or other CUI regardless of contractor's physical work location. An IT Level I or IT Level II approval requires a favorably adjudicated background investigation. Before a contractor or consultant requiring IT access (either Level I or Level II) can begin working, they must be granted either a temporary access or final access based on a background investigation.
2. A pre-employment review of an applicant's background is conducted by PSB to provide the basis for temporary access. A completed background investigation covering the last 7 years provides the basis for granting final access.
3. 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 ability 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. Additionally, IT Level I includes all the access and responsibilities under IT Level II Access and Building Access. These positions may involve—

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

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

(c) 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.

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

(i) Dollar amounts of $10 million per year or greater; or

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

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

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

4. IT Level II Access includes all other contractors or consultants with access to IT systems or CUI regardless of physical work location, including those needing an NRC LAN account.

5. Contractors and consultants requiring IT access will be approved in accordance with the following procedures.

(a) Temporary Approval

(i) The COR will need to complete and submit a security package to PSB. The security package consists of NRC Form 850 and NRC Form 188, which should be emailed to PSB_ContractorResourceInbox@nrc.gov. (See Section I.C.3 of this handbook for specific instructions on how to complete a security package for temporary approval.)

(ii) PSB will review the security package and make one of the following security decisions:

- The contractor or consultant has a background investigation that meets or exceeds the investigative requirement for IT access (either IT Level I or IT Level II) and qualifies for contract performance through reciprocity; or
- The contractor or consultant does not qualify for reciprocity and will be required to undergo a background investigation.

(iii) If PSB determines the contractor or consultant qualifies for reciprocity, then they will be granted final IT access (either IT Level I or IT Level II). PSB will email the COR the final IT access memo and any additional instructions. Note that if the NRC Form 188, "Drug Testing Criteria," indicates the contractor requires pre-employment drug testing, then PSB will need to wait for the results before granting final IT access.

(iv) PSB will review the Standard Form (SF) 86, "Questionnaire For National Security Positions," FBI fingerprint record check, credit check, and drug test results (if applicable) to grant temporary IT Access (either IT Level I or IT Level II) and send the COR the temp IT access approval memo by email. PSB will forward the SF 86 to its investigation service provider for a full background investigation that will be reviewed when it is completed.

(b) Resolving Questions of Eligibility

After non-favorable review of the SF 86, FBI fingerprint check, credit check, and drug test results (if applicable), PSB will email the COR and notify them that the contractor or consultant will not be given temporary IT access. The COR should note that the contractor or consultant cannot support the contract and/or task order if they were not approved for temporary IT access and may not be escorted to support the contract. The COR will then be asked if they wish to continue processing the contractor, or consultant, or discontinue processing the security package and submit a new contractor or consultant. If the COR requests to continue processing the contractor or consultant, then the SF 86 will be forwarded to its investigation service provider for a full background investigation. Furthermore, reviewing the investigation, potentially obtaining additional information from the contractor or consultant and/or third parties, and rendering an adjudicative determination may require additional time to complete. Based on the response from the COR, one of the following will happen—

(i) Discontinue processing – The COR notifies PSB to discontinue processing this contractor or consultant and will submit a new security package for another contractor or consultant for the contract and/or task order.

(ii) Continue processing – The COR notifies PSB of their request to continue processing the contractor or consultant, even though temporary IT access will not be granted. PSB will forward the SF 86 to its investigation service provider and wait for the full background investigation to be completed. While the background investigation is pending, the COR is required to notify PSB if the contractor or consultant is no longer needed on the contract. Once the investigation is complete, PSB will review it; obtain additional information from the contractor, or consultant, and/or third parties (if necessary); and render one of the following adjudicative determinations:

- If PSB makes a favorable adjudicative determination, then PSB will email the COR with the final IT access approval memo (either IT Level I or IT Level II) and any additional instructions.
- If PSB does not make a favorable adjudicative determination, then PSB will provide the contractor or consultant with their appeal rights and notify the COR of the IT access denial.

(c) Final Approval or Disapproval

Upon receipt of the completed background investigation, PSB will then review it; obtain additional information from the contractor, or consultant, and/or third parties (if necessary); and render one of the following adjudicative determinations:

(i) If PSB makes a favorable adjudicative determination, then PSB will email the COR with the final IT access approval memo (either IT Level I or IT Level II) and any additional instructions.

(ii) If PSB does not make a favorable adjudicative determination, then PSB will advise the contractor or consultant of their appeal rights and notify the COR of the IT access denial.

L. Contractors or Consultants 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-issued, HSPD-12 PIV card (NRC badge) for access to the NRC headquarter buildings or regional office facilities.
2. If the COR determines that the work will take more than 30 calendar days, or that the work requires an HSPD-12 PIV card, then approval for unescorted BA must be granted 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.
3. CORs may be reported for a security violation, as described in MD 12.1, for situations in which their contractors or consultants do not follow the access procedures of MD 12.3. Examples may include when a contractor or consultant is denied access (temporary or final) and is subsequently escorted into NRC facilities for work.
4. An NRC contractor, subcontractor, or other individual who is not an NRC employee (for example, other Government agency personnel or licensee) requiring unescorted BA will be approved in accordance with the following procedures.

(a) Temporary Building Access Approval

(i) Before a contractor or consultant requiring BA can begin working, they must be granted either temporary access or final access based on a background investigation. A pre-employment review of a contractor's or consultant's background is conducted by PSB to provide the basis for temporary access. A more thorough investigation covering the last 10 years, conducted by its investigation service provider, provides the basis for granting final BA. Contractors or consultants must have resided in the United States for the immediate and previous 2 years. Contractors or consultants living overseas for extensive periods may have difficulty obtaining investigative coverage overseas. This may also result in a delay or the inability to process the BA approval.

(ii) The COR will complete and submit a security package to PSB. The security package consists of NRC Form 850 and the NRC Form 188 which should be forwarded to PSB_ContractorResourceInbox@nrc.gov.

(iii) PSB will review the security package and make one of the following security decisions.

- The contractor or consultant has a background investigation that meets or exceeds the investigative requirement for BA and qualifies for contract performance through reciprocity, or
- The contractor or consultant does not qualify for reciprocity and will be required to undergo a background investigation.

(iv) If PSB determines the contractor or consultant qualifies for reciprocity, then they will be granted final BA. PSB will email the COR the final BA memo and any additional instructions. Note that if the NRC Form 188 indicates the contractor or consultant requires pre-employment drug testing, then PSB will wait for the results before granting final BA.

(v) PSB will review the SF 85, FBI fingerprint record check, credit check, and drug test results (if applicable) to grant temporary BA and email the COR the temporary BA approval memo. PSB will forward the SF 85 to the investigation service provider for a full background investigation that will be reviewed when it is completed.

(b) Resolving Questions of Eligibility

After non-favorable review of the SF 85, FBI fingerprint check, credit check, and drug test results (if applicable), PSB will email the COR and notify them that the contractor or consultant will not be given temporary BA. The COR should note that the contractor or consultant cannot support the contract and/or task order if they were not approved for temporary BA and may not be escorted to support the contract. The COR will then be asked if they wish to continue processing the

contractor or consultant, or discontinue processing the security package and submit a new contractor or consultant. If the COR requests to continue processing the contractor or consultant, then the SF 85 will be forwarded to its investigation service provider for a full background investigation. Furthermore, reviewing the investigation, potentially obtaining additional information from the contractor or consultant and/or third parties, and rendering an adjudicative determination may require additional time to complete. Based on the response from the COR, one of the following actions will happen:

(i) Discontinue processing – The COR notifies PSB to discontinue processing this contractor or consultant and will submit a new security package for another contractor or consultant for the contract and/or task order.

(ii) Continue processing – The COR requests that PSB continue processing the contractor or consultant even though temporary BA will not be granted. PSB will forward the SF 85 to its investigation service provider and wait for the full background investigation to be completed. While the background investigation is pending, the COR is required to notify PSB if the contractor or consultant is no longer needed on the contract. Once the investigation is complete, PSB will review it; obtain additional information from the contractor, or consultant, and/or third parties (if necessary); and render one of the following adjudicative determinations:

- If PSB makes a favorable adjudicative determination, PSB will email the COR with the final BA approval memo and any additional instructions.
- If PSB does not make a favorable adjudicative determination, PSB will advise the contractor or consultant of their appeal rights and notify the COR of the BA denial.

(c) Final Approval or Disapproval

Upon receipt of the complete background investigation, PSB will review it; obtain additional information from the contractor, or consultant, and/or third parties (if necessary), and render one of the following adjudicative determinations:

(i) If PSB makes a favorable adjudicative determination, PSB will email the COR with the final BA approval memo and any additional instructions.

(ii) If PSB does not make a favorable adjudicative determination, then PSB will advise the contractor or consultant of their appeal rights and notify the COR of the BA denial.

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.

M. Removing a Contractor or Consultant from a Contract and/or Task Order

Follow this process when a contractor or consultant needs to be removed from a contract or task order. CORs should understand that the termination of the contractor is only for the specified contract or task order.

1. The COR will need to complete and email the NRC Form 851, "Contractor Closeout Form," to PSB at PSB_ContractorResourceInbox@nrc.gov.
2. PSB will review the NRC Form 851 and terminate the contractor from the contract and/or task order.

N. Adding Another Contract and/or Task Order to an Existing NRC Contractor or Consultant

Follow this process, when adding a contractor that is already supporting a contract at the NRC, or when adding one or more task orders for a contractor who is already supporting the corresponding NRC Enterprisewide Contract (EWC), Blanket Purchase Agreement (BPA), Interagency Agreement (IAA), or Delivery/Task Order.

1. The COR completes and emails the NRC Form 847, "Request for Addition of Contract or Task Order(s)," and the NRC Form 188 to PSB at PSB_ContractorResourceInbox@nrc.gov.
2. PSB reviews the NRC Form 847 and the NRC Form 188 and makes one of the following security decisions:

   (a) The contractor has a background investigation that meets or exceeds the investigative requirement for the position being submitted and qualifies for contract performance through reciprocity. If PSB determines the contractor qualifies for reciprocity, the contractor or consultant will be granted the requested final access or clearance. PSB will email the COR the final access or clearance memo and any additional instructions. Note that if the NRC Form 188 indicates the contractor requires pre-employment drug testing, then PSB will wait for the results before granting a final access or clearance.

   (b) The contractor does not qualify for reciprocity and will be required to undergo a background investigation. If PSB determines the contractor or consultant does not qualify for reciprocity, then they will need to be processed as a new contractor. The COR will need to follow the instructions in Section I.G.3 of this handbook. Note: A background investigation is only necessary when the contractor does not qualify for reciprocity and is being submitted for a higher position requiring a higher background investigation. The COR will be emailed with this decision.

O. Transferring an NRC Contractor or Consultant

Follow this process when a contractor or consultant needs to be removed from one contract and/or task order and transferred to another contract and/or task order. For example, a contract is expiring, and current support staff need to be transferred to a newly awarded contract.

1. The COR needs to complete and email the NRC Form 848 and the NRC Form 188 to PSB at PSB_ContractorResourceInbox@nrc.gov.
2. PSB will review the NRC Form 848 and the NRC Form 188 and make one of the following two security decisions:
   (a) The contractor or consultant has a background investigation that meets or exceeds the investigative requirement for the position being submitted and qualifies for contract performance through reciprocity. If PSB determines the contractor qualifies for reciprocity, the contractor will be granted either a final access or clearance, depending on what the request, to the new contract and/or task order. PSB will email the COR with the final access memo or clearance memo with any additional instructions. PSB will then terminate the access or clearance from the contract and/or task order from which they are being removed. Note that if the contractor or consultant requires pre-employment drug testing, determined by the COR's responses on the NRC Form 188, PSB will wait for the results before granting a final access or clearance.
   (b) The contractor does not qualify for reciprocity and will be required to complete the appropriate security questionnaire. If PSB determines the contractor or consultant does not qualify for reciprocity, then they will need to be processed as a new contractor or consultant. Please note that this only happens when the contractor or consultant is being submitted for a higher position requiring a higher background investigation. PSB will email the decision to the COR.

P. Upgrading an NRC Contractor or Consultant

Follow this process when a contractor's or consultant's access or clearance level for a contract and/or task order needs to be upgraded.

1. The COR will need to complete and submit a security package to the Personnel Security Branch (PSB). The security package consists of NRC Form 850 and the NRC Form 188, which should be emailed with the upgrade information to PSB at PSB_ContractorResourceInbox@nrc.gov.
2. PSB will review the security package and make one of the following security decisions:
   (a) The contractor has a background investigation that meets or exceeds the investigative requirement for the position being submitted and qualifies for reciprocity. If PSB determines the contractor or consultant qualifies for

reciprocity, then they will be granted either a final access or clearance, depending on the request. PSB will email the COR with the final access or clearance memo and any additional instructions. Note that if the contractor or consultant requires pre-employment drug testing, determined by the COR's responses on the NRC Form 188, then PSB will wait for the results before granting a final access or clearance.

(b) The contractor does not qualify for reciprocity and will be required to complete the appropriate security questionnaire. If PSB determines the contractor or consultant does not qualify for reciprocity, then, depending on the position they are being submitted for, additional forms, digital fingerprinting and a security questionnaire will need to be submitted. PSB will email the COR and tell them what is needed. After all the required forms and digital fingerprints are submitted, and a drug test is conducted (if applicable), PSB will forward the SF 85/SF 86 to its investigation service provider for a full background investigation, which will be reviewed when it is completed. The contractor or consultant will remain at their current access or clearance level until the investigation is favorably adjudicated. Once the investigation is complete, PSB will review it, obtain additional information from the contractor and/or third parties (if necessary), and render one of the following adjudicative determinations:

(i) If PSB makes a favorable adjudicative determination, then PSB will email the COR with the final approval memo and any additional instructions.

(ii) If PSB does not make a favorable adjudicative determination, then PSB will advise the contractor or consultant of their appeal rights, and notify the COR of the access denial.

Q. Downgrading an NRC Contractor or Consultant

Follow this process when a contractor's or consultant's access or clearance level for a contract and/or task order needs to be downgraded.

1. The COR will complete and email the NRC Form 849, "Contractor Downgrade Form," and the NRC Form 188 with the downgrade information to PSB at PSB_ContractorResourceInbox@nrc.gov.
2. PSB will review the NRC Form 849 and process the downgrade. Note that if the contractor or consultant requires pre-employment drug testing, determined by the COR's responses on the NRC Form 188, PSB will need to wait for the results before granting a final access or clearance downgrade.
3. PSB will send the COR a new memo with all the downgraded information.

II. INVESTIGATIONS AND DETERMINING ELIGIBILITY FOR ACCESS AUTHORIZATION

A. Investigations

1. The hiring or employing office, in coordination with OCHCO or OIG Human Resources officer 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:

   (a) NRC employees,

   (b) Applicants for employment,

   (c) Consultants,

   (d) Experts, and

   (e) Atomic Safety and Licensee Board Panel members.

2. For NRC contractor and subcontractor employees, the access authorization (security clearance) or access level required should be determined based on the employee's classified access requirements; access to CUI//SP-SGI, NRC IT systems, or sensitive information; or need for unescorted access to nuclear power facilities, NRC headquarters, or regional office facilities.

3. Instead of a report of investigation from its investigation service provider, the NRC may accept an investigation from another Federal department or agency that conducts personnel security investigations that is within scope and has not been previously adjudicated by another agency.

B. Reciprocity of "Q," "L(H)," and "L" Access Authorization

1. Security Executive Agent (SecEA) Directive 7, "Reciprocity of Background Investigations and National Security Adjudications," states that "background investigations and national security eligibility adjudications, conducted by an authorized investigative agency or authorized adjudicative agency, respectively, shall be reciprocally accepted for all covered individuals."

2. The NRC may request an individual to identify any changes since the last SF 86 submission. The NRC may also "conduct the appropriate personnel security interview or inquiry pertaining to the changes."

3. When new information of national security adjudicative relevance has been reported, developed, or made known to agency officials since the last background investigation indicating the individual may no longer satisfy the eligibility standards for an NRC access authorization, the individual's background investigation and eligibility determination conducted by other Federal authorities may not be reciprocally 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 EDO 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 (Memorandum from Joseph M. Hendrie, Chairman, to Lee V. Gossick, Executive Director for Operations, "Delegation of Authority to Approve Employment of an Individual by NRC Prior to Completion of Security Investigation," dated January 24, 1979.(ML17286A476)). 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 justification 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 Inspector General, office director, the deputy office director, or their designee or by the regional administrator, the deputy regional administrator, or his or her designee.
   (b) The waiver must justify why an applicant should begin employment before the completion of the appropriate background investigation. The Form 236 should clearly demonstrate how 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 OCHCO, the Director of DFS; or OIG, if OIG Human Resources officer is involved.
3. All AEA Section 145b waiver requests will be processed as described in Exhibit 2 of this handbook. An OCHCO or OIG Human Resources officer 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. (See Exhibit 2 for more details.)

4. An exception to personal reference checking for consultants or experts may be recommended to OCHCO by the office director, the regional administrator, or OIG Human Resources staff 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 listed 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 CUI//SP-SGI, or access to NRC IT systems or sensitive information are listed in 10 CFR 10.11, "Criteria"; 32 CFR Part 147, "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information"; and SecEA Directive 4, "National Security Adjudicative Guidelines." These matters must be reported promptly to PSB 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 Personnel Security Branch by the contracting officer, the COR, or other person so designated. In addition, the contractors with an NRC national security clearance must adhere to the requirements of Section II.J of this handbook.

3. The reporting requirements outlined in Section II.J.1 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 required 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. The EAP is only available to NRC employees. 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 discussed 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 made consistent with

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

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 clearance is granted.

3. The SF 312 is executed in accordance with E.O. 12968 and E.O. 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 need 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 IT-I and IT-II access will be consistent with 10 CFR Part 10. BA contractors (including daycare providers) 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 can authorize temporary 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 listed 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. The OCHCO or OIG Human Resources officer, 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 OCHCO, if applicable) 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 applicant’s other country of 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. A Tier 5 investigation will be required for an “L,” “L(H),” 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, Atomic Safety and Licensee Board Panel members, cleared contractors, cleared licensees, cleared licensee contractors, and other cleared persons designated by the EDO are required to abide by the security reporting requirements listed below. 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 planned or actual involvement in any of the activities listed below before participating in such activities, or within 5 days following the start of their involvement. Individuals can email their report to PSBReporting.Resource@nrc.gov. Depending on the nature of the report, a personnel security specialist may contact you to obtain additional information and/or clarification. Failure to comply with reporting requirements and/or agency security inquiries may result in an administrative action that may include, but is not limited to, revocation of national security eligibility or access authorization:

   (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) Application for, possession of, or use of a foreign passport or identity card for travel;

   (h) Unofficial contact with a known or suspected foreign intelligence entity;

   (i) Foreign national contacts including business or personal contacts, and continuing association with a known foreign national(s) or foreign national roommate(s);

   (j) Direct involvement in a foreign business;

   (k) Foreign bank accounts;

   (l) Ownership of foreign property;

   (m) Foreign citizenship;

   (n) Voting in a foreign election;

   (o) Adoption of non-U.S. citizen child;

(p) Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure;

(q) Media contacts (not for official duties), where the media seeks access to classified or otherwise “protected” information (specifically prohibited by law from disclosure), whether or not the contact results in an authorized disclosure. Media contacts related to the fulfillment of official duties of the position held by the individual need not be reported;

(r) Unofficial foreign travel to countries for which the U.S. Department of State has issued a Level 3 or 4 travel advisory (https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html);

(s) 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;

(t) Travel to a foreign country where a passport other than a U.S. passport is used to enter or leave the country;

(u) Enrollment in a drug or alcohol treatment program;

(v) Financial issues and anomalies including, but not limited to, bankruptcy, foreclosure, tax liens, failure to pay Federal or State taxes, garnishment, being over 120 days delinquent on any debt, and any unusual infusion of $10,000.00 or greater such as an inheritance, winnings, or similar financial gain;

(w) Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified or other "protected" information (specifically prohibited by law) from disclosure regardless of means;

(x) Unofficial media contacts where the media seeks access to classified or otherwise "protected" information (specifically prohibited by law from disclosure), whether the contact results in an unauthorized disclosure. Media contacts related to the fulfillment of official duties of the position held by the individual need not be reported; and

(y) Treatment for emotional, mental, or personality disorders (except marriage, grief, or family counseling not related to violence by you or strictly related to adjustments from service in a military combat environment). Victims of sexual assault who have consulted with a health care professional regarding an emotional or mental health condition strictly in relation to the sexual assault are not required to report. Court-ordered counseling must be reported.

Note: Employees are encouraged to seek help for mental health and/or addictions issues and such treatment is not automatically adverse to maintaining a national security clearance. Employees do not have to report contacts with the Employee Assistance Program (EAP) where EAP merely provides an

assessment of the employee's condition, or simply provides a referral to another provider of health care services. Counseling/treatment from a third party mental health care provider/counselor, beyond EAP services, must be reported unless it falls within the non-reportable exceptions listed above.

Note: Though some states, U.S. territories and the District of Columbia permit the recreational and/or medical use of marijuana under state or district law, marijuana still remains illegal under Federal law and is identified as a Schedule I drug under the Controlled Substances Act.

2. Employees will be required to acknowledge these reporting requirements annually to encourage voluntary compliance.

3. In addition, employees are required 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) Habitual use of intoxicating beverages 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 the 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 activity that raises doubts as to whether another covered individual's continued national security eligibility is clearly consistent with the interests of national security.

(l) 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 a 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.

(m) 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.

(n) Apparent or suspected mental health issues where there is a reason to believe it may impact the covered individual's ability to protect classified information or other information specifically prohibited by law from disclosure.

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

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

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

(r) Misuse of U.S. Government property or information systems.

(s) An unwillingness to comply with rules and regulations or to cooperate with security requirements.

(t) Unexplained affluence.

(u) 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, or alcoholism; or

(iii) Other financial issues.

4. Not all reports 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 in the NRC Forms Library on SharePoint. If both parties are affiliated with the NRC, each party must submit their own NRC Form 354 to PSB.

K. Reinvestigation Program

1. The NRC reinvestigation program is designed to ensure the continued eligibility for access authorization of individuals affiliated with the NRC. The program applies to all those who possess "Q," "L(H)," or "L" access authorization, including—

   (a) NRC employees, consultants, experts, Atomic Safety and Licensee Board Panel (ASLBP) members, contractors, and licensees;

   (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," "L(H)," 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, if applicable. Continuous vetting will reduce the number of periodic reinvestigations required to be performed and will limit the need for reinvestigations to event- or risk-based rather than the traditional calendar-driven model (see Section L). PSB will notify the individuals who are to be reinvestigated and the dates by which they are to complete the security forms. 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 (see Section K.1) must complete and return the security 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. This may result in being 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 vetting requirements as set forth by Office of the Director of National Intelligence (ODNI) criteria, which is subject to change at ODNI's discretion.

L. Continuous Vetting (CV) Program

1. Continuous Vetting is the review of the background of an individual at any time during the period of eligibility to determine whether the individual continues to meet the requirements for eligibility for access to classified information or to hold a sensitive position to mitigate the risk posed by insiders who potentially represent a threat to national security.

2. CV implementation and business process must be consistent with SecEA Directive 6 (SEAD 6), "Continuous Evaluation"; the 2012 Federal Investigative Standards (FIS); Executive Order (E.O.) 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," as amended by E.O 13741; and E.O. 13764, "Amending the Civil Service Rules," Executive Order 13488, and Executive Order 13467, "To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters"; and 5 U.S.C 11001, "Enhanced Personnel Security Programs."

3. The CV applies to all NRC employees, consultants, experts, ASLBP members, contractors, and licensees with access to National Security Information.

4. SF 86 certification forms obtained from individuals within the last 5 years permit the agency to conduct CV checks.

5. PSB must conduct prescribed record checks on a random or continuous basis between otherwise established Federal Investigative Standards investigative cycles (see Exhibit 4).

6. The collection, transmission, and storage of information obtained through CV will be—

   (a) Limited to information lawfully available to security officials,

   (b) Relevant to security eligibility determinations, and

   (c) Compliant with all applicable civil liberties and privacy laws, directives, regulations, and policy.

M. Termination of Access Authorization

1. When an individual with an NRC security clearance no longer needs access to NSI, PSB will terminate the access authorization. The individual must receive a security debriefing and the debriefing portion of the SF 312 and NRC Form 176C, "Security Debriefing Acknowledgement," must be signed by the individual when—

   (a) An NRC employee, consultant, or contractor is separated from employment with the NRC.

   (b) A non-NRC employee (i.e., contractor) 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) An individual no longer requires access to NSI for the performance of their job.

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) Immediately return badges, passes, and other forms of official identification to the responsible NRC security point of contact.

   (d) Request that PSB remove the individual's name from all access lists.

   (e) Ensure that combinations to which the person had access are changed.

   (f) Remove the person's name 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 and any action taken will be determined on a case-by-case basis.

N. Clearance Suspension and Revocation

Title 10 CFR Part 10, "Criteria and Procedures for Determining Eligibility for Access to restricted Data or National Security Information or an Employment Clearance," outlines the process for clearance suspension and/or revocation.

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. The individual is not permitted access to classified information.
4. Any individual whose clearance has been suspended may not access any level of classified information or CUI 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 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).

O. Termination of Contractor Unescorted Building Access (BA), Controlled Unclassified Information, and Power Reactor Access

The NRC sponsoring office or COR must immediately notify PSB in writing, by submitting NRC Form 851, "Contractor Closeout Form," when a contractor employee no longer requires unescorted access to nuclear power facilities, NRC headquarters, or regional office facilities; or access to CUI.

P. 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 website at https://intranet.nrc.gov/ocio/catalog/25134.

III. CONTROL OF VISITS INVOLVING CLASSIFIED INFORMATION

A. Introduction

This section provides standards and procedures for the protection of classified information during visits to the 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 all incoming and outgoing 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 email to DFS_PSB_Request_for_Visit.Resource@nrc.gov. 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 PIV card (NRC 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 facilities 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, to NRC contractors, to other NRC facilities, or to other Government agencies except as indicated in Section I.C.1(a) of this handbook, involving classified information must be requested on NRC Form 277, "Request for Visit," or in a written request on agency/company letterhead 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, emailed to DFS_PSB_Request_for_Visit.Resource@nrc.gov, or sent to the following address:

    U.S. Nuclear Regulatory Commission
    Personnel Security Branch
    Division of Facilities and Security
    Mailstop: TWFN -07D04M
    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. A request for visit or access approval (NRC Form 277) is not necessary for NRC employees and contractors who are visiting NRC headquarters, regional offices, and the Technical Training Center. The NRC-cleared individual's HSPD-12 PIV card (NRC badge) identifies 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 all other non-NRC facilities, an NRC Form 277 or other written request for visit or access approval should be completed by the individual's NRC office or division establishing the individual's need-to-know and purpose of the visit, then emailed to PSB for verification of access authorization at DFS_PSB_Request_for_Visit.Resource@nrc.gov. PSB forwards the visit request to the facility to be visited. At those contractor or licensee facilities at which the NRC is not the cognizant security authority (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 7 workdays before the initial date of the visit. 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-to-know for access has been properly certified by the individual's home agency security office.

3. National Security Information (NSI)

   Classified information, other than RD, may be furnished to individuals when they have the required access authorization and their need-to-know 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 the individual's home agency security office representative should be submitted to PSB for processing and approval.

5. Representatives of Other Agencies

   If authorized by the Director, 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, DFS, to certify access authorization and with NRC's Director, Office of Congressional Affairs (OCA).

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-to-know for this access must be certified and the required access authorization must be verified by PSB.

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 Chief, PSB, by the Division of Security Operations (DSO), NSIR. Any foreign national possessing a security assurance (i.e., clearance) from his or her government must be officially certified to 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 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 https://www.state.gov/09-106, 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 before 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 authorized visit by the requesting office and the office of the facility visited.

I. Withdrawal of Active Visit Request

1. If an individual has an active visit request with another agency that is no longer needed, PSB needs to be informed immediately by email to DFS_PSB_Request_for_Visit.Resource@nrc.gov so the visit authorization can be terminated.
2. If an incoming visitor has an active visit request that is no longer needed, PSB needs to be informed immediately by email to DFS_PSB_Request_for_Visit.Resource@nrc.gov so the visit authorization can be terminated.

IV. 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, "Drug-free Federal Workplace," 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 https://www.federalregister.gov/documents/2017/01/23/2017-00979/mandatory-guidelines-for-federal-workplace-drug-testing-programs). 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. 3, dated December 2021, 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 an 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 that was scheduled before testing notification.

D. Drug Testing When an Employee is Working Under the NRC's Telework Program

1. When an employee is working from a non-NRC worksite under the NRC's Telework 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 Telework Program may be directed to report to a preapproved subcontractor drug testing facility. Usually, the subcontractor drug testing facility is within 50 miles 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 they 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) (PSB) 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. 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.
4. Notification of the responsibilities associated with the issuance of a Government photo identification badge (HSPD-12). Information about physical security aspects, the importance of visitor control, and the types of procedures of the particular facility for protecting Government property.
5. 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 OIG Human Resources staff will obtain a current resumé and the following security forms:

1. Signature pages from the Questionnaire for National Security Positions (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));
2. NRC Form 236, "Personnel Security Clearance Request and Notification";
3. NRC Form 176A, "Security Acknowledgement/Access Authorization";
4. OF-306, "Declaration for Federal Employment" (available from OCHCO or PSB);
5. The Fair Credit Reporting Act (FCRA) release;
6. NRC Form 212, Qualifications Investigation Professional, Technical, and Administrative Positions;
7. NRC Federal Employee Applicant Clearance Status Checklist;
8. I-9 or PIV; and
9. Offer Letter.

B. The OCHCO specialist or OIG Human Resources staff will ensure that appropriate reference checks are conducted using the resumé as the source document. Once the security package is complete, OCHCO or OIG Human Resources staff will forward it to PSB for processing and ensure a pre-employment drug test has been requested

C. The following additional requirements apply and will be conducted by OCHCO or OIG Human Resources staff 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 OIG Human Resources staff will review the results of all the reference checks to determine acceptability of the applicant. If either the OCHCO or OIG specialist or the HRO has any doubt as to the applicant's suitability, then OCHCO and the program or regional office or OIG 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 for clarification of the answers provided on the SF 86 or any other matters of security concern.
4. Evaluate the eligibility of the selectee for a Section 145b of the Atomic Energy Act (AEA) employment waiver after reviewing the security package and the results of the applicable checks and recommend approval or disapproval.
5. If the result of the pre-employment review does not warrant a Section 145b approval, OCHCO or OIG is notified to take appropriate action to determine whether to rescind the selectee’s conditional offer of employment or authorize PSB to continue processing the select’s complete background investigation. Upon receipt of the report of investigation, PSB will adjudicate the report, 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, Atomic Safety and Licensee Board 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 Standard Form (SF) 86 "Questionnaire for National Security Positions" (QSP) and related forms. These forms will be the basis for an investigation as specified below.
2. A Department of Defense, Defense Counterintelligence and Security Agency (DCSA) Tier 5 (T5) initial investigation or a Tier 5 reinvestigation (T5R) 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 SF 86 and related forms. These forms will be the basis for an investigation as follows:

1. A Tier 3 reinvestigation (T3R) 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. ODNI and/or DCSA Reinvestigation Requirements

Individuals approved for access authorizations are subject to continuous monitoring requirements as set forth by the Office of the Director of National Intelligence (ODNI) and/or DCSA criteria, which is subject to change at ODNI's and/or DCSA discretion.

Exhibit 4 Security Clearances/Access Types

SECURITY CLEARANCES/ACCESS TYPES	INVESTIGATION REQUIRED	AUTHORIZES ACCESS TO THE FOLLOWING INFORMATION (WITH AN ESTABLISHED NEED-TO-KNOW)
Q - Top Secret (TS)	Tier 5 investigation (T5), with Tier 5 Reinvestigation (T5R) every 5 years (if applicable). Subject to Continuous Vetting.	TS/S/Confidential (C) National Security Information, Restricted Data
L- High Public Trust (L(H)) (Secret)	T5, with Tier 3 Reinvestigation (T3R) every 5 years (if applicable). Subject to Continuous Vetting.	S/C National Security Information C - Restricted Data
L - Secret (S)	T3, with T3R every 10 years (if applicable). Subject to Continuous Vetting.	S/C National Security Information C - Restricted Data
U - Top Secret	T5, with T5R every 5 years (if applicable). Subject to Continuous Vetting.	Special Nuclear Material in support of the Material Access Authorization Program (MAAP)
R – Secret	T3, with T3R every 10 years (if applicable). Subject to Continuous Vetting.	Special Nuclear Material in support of the MAAP
Information Technology (IT) Level I Access	Tier 3 (T3), with Tier 3 Reinvestigation (T3R) every 10 years.	NRC Sensitive IT Systems or Data for the development, direction, implementation, and administration of NRC computer programs

SECURITY CLEARANCES/ACCESS TYPES	**INVESTIGATION REQUIRED**	**AUTHORIZES ACCESS TO THE FOLLOWING INFORMATION (WITH AN ESTABLISHED NEED-TO-KNOW)**
IT Level II Access	T3, with T3R every 10 years.	NRC Sensitive IT Systems or Data, including those individuals needing an NRC Local Area Network (LAN) account
Building Access	Tier 1 (T1) investigation.	Unescorted access to NRC facilities for vendors, health unit, housekeeping personnel
Child Care Access	T1 investigation.	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	T3, with T3R every 10 years (if applicable). Subject to Continuous Vetting.	Unescorted access to protected and vital areas of nuclear power facilities, access to safeguards information, and unescorted access to NRC facilities