Security Access Authorization and Card Issuance Policies and Procedures

Office of Administration

Version 3.0

Security Access Authorization and Card Issuance Policies and Procedures

Nuclear Regulatory Commission

The Office of Administration

Issue Date: 12-02-2009

Effective Date: *MM-DD-YYYY*

WARNING: *This document is SENSITIVE BUT UNCLASSIFIED (SBU). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with NRC policy relating to SBU information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized NRC official.*

Nuclear Regulatory Commission

[This page left is intentionally left blank]

Table of Contents

Document Revision History			
Date	**Version**	**Description**	**Author**
07/29/2009	1.0	Draft	J. Sanchez K. Juris
09/04/2009	2.0	Incorporate DFS comments	J. Sanchez K. Juris
12/2/2009	3.0	Incorporate comments for 800-79 certification	J. Sanchez K. Juris

1.0 Introduction

This document provides the procedures to implement the Nuclear Regulatory Commission (NRC) Personnel Security Program policy concerning access authorization and clearance.

1.1 Purpose

As stated in Management Directive (MD) 12.3, it is the policy of NRC to establish a personnel security program to ensure that the NRC reviews and makes eligibility determinations in accordance with pertinent laws, Executive Orders, MDs, and applicable directives of other federal agencies in order to provide assurance that personnel (NRC employees, consultants, contractors, and licensees) are reliable and trustworthy to have access to:

- NRC facilities
- Classified information
- Safeguards information
- Sensitive NRC information and equipment
- Nuclear power facilities
- Special nuclear material

1.2 Scope

The scope of this document is limited to the access authorization and clearance procedures which are the responsibility of the Division of Facilities and Security, Office of Administration (DFS/ADM).

1.3 Audience

The audience for this document is current DFS personnel who will use this document as a reference for procedures, and NRC management officials who need to verify that proper procedures are documented in compliance with security requirements.

The DFS administers the NRC program for personnel security, including building access, IT access, access to safeguards information, and security clearances. They also manage the NRC drug testing program.

1.4 Approach

In order to ensure a comprehensive understanding of the access authorization and clearance process, chapters 2 through 5 provide introductory information - key concepts, authorities and references, Personal Identity Verification (PIV) per Federal Information Processing Standard (FIPS) 201, and an overview of the personnel access authorization and clearance process at NRC.

- **Section 2.0 Key Concepts**
  This section provides key concepts for understanding and performing the access authorization and clearance process.

- **Section 3.0 Authorities and References**
  This section provides the federal laws and regulations, Executive Orders, Presidential Directives, NIST standards, OMB guidance, and NRC MDs that govern the access authorization and clearance process.
- **Section 4.0 FIPS 201 Personal Identity Verification (PIV) Framework**
  This section discusses the PIV framework that provides the foundation for the access authorization and clearance process at NRC.
- **Section 5.0 Overview of the Access Authorization and Clearance Process**
  This section describes the security clearance process for NRC employees.

Chapters 6 through 17 provide the procedures applicable to the different types of applicants for access authorization and clearance, as well as requirements for special situations.

- **Section 6.0 The 145b Process**
  This section describes the requirements and procedures for adjudicating NRC employees, or applicants for employment at the NRC, for access authorization and/or clearance.
- **Section 7.0 The Consultants and Experts Process**
  This section describes the requirements and procedures for adjudicating consultants and experts engaged by the NRC for access authorization and/or clearance.
- **Section 8.0 The Information Technology (IT) Contractor Process**
  This section describes the requirements and procedures for adjudicating contractors providing IT services for access authorization.
- **Section 9.0 The Contractor with Clearance Process**
  This section describes the requirements and procedures for adjudicating contractors who require "need to know" access to sensitive or classified information for access authorization and/or clearance.
- **Section 10.0 The Building Access Process**
  This section describes the requirements and procedures for adjudicating workers who require only physical access to NRC facilities.
- **Section 11.0 The Daycare Worker Process**
  This section describes the requirements and procedures for adjudicating daycare worker who require either IT and physical access or only physical access to NRC facilities.
- **Section 12.0 The Licensee Process**
  This section describes the requirements and procedures for adjudicating licensees who require unescorted access to nuclear facility sensitive areas and/or access to sensitive or classified information for access authorization and/or clearance.
- **Section 13.0 The Foreign Assignee Process**
  This section describes the requirements and procedures for granting physical access authorization to Foreign Assignees.

- **Section 14.0 Special Situations Concerning Citizenship of Applicants**
  This section describes special situations where the access authorization and clearance process may require additional information or place limitations due to citizenship of the applicant or family members.
- **Section 15.0 The Renewal Process**
  This section describes the requirements and process for renewing an Applicant's PIV card.
- **Section 16.0 Changes to Access Authorizations**
  This section describes the requirements and process for: upgrades/downgrades based on "need to know", and terminations.
- **Section 17.0 Reciprocity of Access Authorization**
  This section describes the requirements and procedures for granting access authorization and/or clearance based on a previous investigation by another federal agency.
- **Section 18.0 The Reinvestigation Program**
  This section describes the requirements and procedures for performing reinvestigations as required by law.
- **Section 19.0 Reinstatement of Access Authorization**
  This section describes the requirements and procedures for reinstatement of access authorization for NRC employees who are returning to duty after a period of separation.
- **Section 20.0 Sensitive Compartmented Information (SCI) Access**
  This section briefly describes the procedures applicable to the PSB in the SCI access authorization process.

2.0 Key Concepts

It is advantageous to the users of this document to ensure that they understand certain key concepts and terms. The following information in this section should be considered "pre-requisites" for understanding and executing the access authorization and clearance process.

2.1 Terminology

2.1.1 Access Authorization and Clearance

An Access Authorization is a determination by an authorized adjudicative office granting an individual physical access to federally controlled facilities and logical access to federally controlled information systems as determined by role, responsibility, and need-to-know.

A Clearance is a formal security determination by an authorized adjudicative office that an individual is authorized access to classified information as determined by role, responsibility, and need-to-know.

The difference between an access authorization and a clearance is that an access authorization grants physical access and logical access to federal information. Only after one gets access authorization can he or she be granted access to classified information through the clearance process.

Background Investigation

A background investigation is a requirement to determine if an individual is reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States. Background investigations are performed in order to make suitability and security determinations for access authorization and/or clearance.

The requirement to be investigated applies to all access authorizations even if the position does not require a security clearance. The scope and type of a background investigation will vary, depending on the nature of the position and the degree of harm that an individual in that position could cause.

2.1.2 Classified Information

Classified information is information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

2.1.3 Physical Access Control System

Physical Access Control System (PACS), which controls physical access to NRC facilities using the PIV credentials created by PCI. Card readers installed at perimeter entrances and controlled areas will read the PIV cards and grant access to authorized personnel.

2.2 Personnel Security Principles

2.2.1 Access Control

Access Control means that authorized individuals must present identification and authentication in order to gain access to facilities, data, and/or systems.

Identification is the means by which a user provides a claimed identity.

Authentication is the means of establishing the validity of a claimed identity.

For example, when logging onto a computer, your username identifies you. Your private password is a means to authenticate that you are the owner of the username.

2.2.2 Least Privilege

Least privilege refers to the security objective of granting users only the access they need to perform their official duties. Application of this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources.

2.2.3 Separation of Duties

Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. Ensuring that such duties are well defined is the responsibility of management.

2.2.4 Need-to-Know

Need-to-know means that even if a person has been found eligible and granted access to classified information via the clearance process, access to the specific level of information will be determined by the need-to-know and according to a person's duties and responsibilities.

3.0 Authorities and References

This section provides important background information concerning the authorities which mandate and provide guidance for the access authorization and clearance process.

The structure of this section is:

- Federal Law and Regulations
- Executive Orders
- Presidential Directives
- Federal Information Processing Standards (FIPS)
- Office of Management and Budget (OMB) Memoranda
- NRC MDs

Additional references to federal law and Executive Orders applicable to the NRC personnel access authorization and clearance policy and procedures may be found in Section 7 of the NRC MD 12.3, *NRC Personnel Security Program*.

3.1 Federal Law and Regulations

The federal laws which pertain to the personnel access authorization and clearance policy and procedures are The Atomic Energy Act of 1954, the Energy Reorganization Act of 1974, and Section 145b of The Atomic Energy Act.

In addition, regulatory agencies like the NRC are empowered to create and enforce rules and regulations that carry the full force of a law.[1]

Regulations which pertain to the personnel access authorization and clearance policy and procedures are:

- 10 CFR Part 10--Criteria and Procedures for Determining Eligibility for Access to Restricted Data or National Security Information or an Employment Clearance
- 10 CFR Part 25--Access Authorization for Licensee Personnel

[1] Congress often grants broad authority to executive branch agencies to interpret the statutes which the agencies are entrusted with enforcing. Congress is not able to write statutes that cover the breadth of detail in broad areas that are the jurisdiction of regulatory agencies. For example, technical specialists at the NRC are best equipped to develop detailed rules applicable statutes affecting the regulation of nuclear energy.

Under the Administrative Procedure Act (APA), agencies must publish all proposed new regulations in the Federal Register at least 30 days before they take effect, and they must provide a way for interested parties to comment, offer amendments, or to object to the regulation.

Once a regulation takes effect, it is printed as a “final rule” in the Federal Register and codified in the Code of Federal Regulations (CFR).

- 10 CFR Part 73.5--Personnel Access Authorization Requirements for Nuclear Power Plants
- 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.

3.1.1 The Atomic Energy Act of 1954

The Atomic Energy Act of 1954 is the fundamental U.S. law covering both the civilian and the military uses of nuclear materials.

Under the Atomic Energy Act of 1954, a single agency, the Atomic Energy Commission, had responsibility for the development and safety regulation of the civilian uses of nuclear materials and for the development and production of nuclear weapons.

3.1.2 Energy Reorganization Act of 1974

Energy Reorganization Act of 1974 established the NRC.

The Act of 1974 split the civilian and military functions of the Atomic Energy Commission. The Department of Energy is assigned responsibility for the development and production of nuclear weapons, promotion of nuclear power, and other energy-related work. The NRC is assigned the regulatory work (not including regulation of defense nuclear facilities.)

3.1.3 Section 145b of the Atomic Energy Act

Section 145b is a key element of the security clearance and access authorization process, and it is unique to the NRC.

Section 145b of the Atomic Energy Act of 1954, as amended, requires that NRC applicants must undergo a background security investigation prior to employment. A waiver of this security clearance requirement is permitted under Section 145b to employ an individual before the completion of the investigation, with the assurance and security controls that the individual will not have access to classified information until the investigation is completed and a security clearance is granted.

3.1.4 10 CFR Part 10

Criteria and Procedures for Determining Eligibility for Access to Restricted Data or National Security Information or an Employment Clearance

The regulations in 10 CFR Part 10 establish criteria and procedures in this part shall be used in determining eligibility for NRC access authorization and/or employment clearance involving:

(a) Employees (including consultants), contractors, and agents of the NRC and applicants for employment;

(b) Licensees of the NRC and their employees (including consultants) and applicants for employment;

(c) Any other person designated by the Deputy Executive Director for Information Services and Administration and the Chief Information Officer of the NRC.

3.1.5 10 CFR Part 25

Access Authorization for Licensee Personnel

The regulations in 10 CFR Part 25 establish procedures for granting, reinstating, extending, transferring, and terminating access authorizations of licensee personnel, licensee contractors or agents, and other persons who may require access to classified information.

3.1.6 10 CFR Part 73.5

Personnel Access Authorization Requirements for Nuclear Power Plants

The regulations in 10 CFR Part 73, Section 56 direct Licensees to establish and maintain an access authorization program, and specify requirements for granting individuals unescorted access to protected areas. This section further specifies timelines, objectives, and requirements, and mandates the protection of personal information.

10 CFR Part 73.56 regulations which are pertinent to the personnel access authorization and clearance process are summarized as follows:

The licensee may accept an access authorization program, or part of the program, used by its contractors and substitute or supplement any portion of the program as necessary to meet NRC requirements.

The unescorted access authorization program must include a background investigation (as well as a psychological assessment and behavioral observation).

The licensee shall grant unescorted access authorization to all individuals who have been certified by the NRC as suitable for such access.

3.1.7 10 CFR Part 95

Facility Security Clearance and Safeguarding of National Security Information and Restricted Data

The regulations in 10 CFR Part 95 apply to licensees, certificate holders and others who may require access to classified National Security Information and/or Restricted Data and/or Formerly Restricted Data (FRD). They establish procedures for obtaining facility security clearance and for safeguarding National Security Information and Restricted Data.

3.2 Executive Orders

Executive Orders are legally binding orders given by the President of the United States, acting as the head of the Executive Branch, to federal administrative agencies. Executive Orders are generally used to direct federal agencies and officials in their execution of congressionally established laws or policies. Executive Orders do not require Congressional approval to take effect but they have the same legal weight as laws passed by Congress.

The Executive Orders which pertain to personnel access authorization and clearance policy and procedures are E.O. 10450, *Security Requirements for Government Employees*, and E.O. 12968, *Access to Classified Information*.

3.2.1 Executive Order 10450

Security Requirements for Government Employees

Executive Order 10450 was issued by President Eisenhower on Apr. 27, 1953. It established the requirement for a background investigation for federal employment and specifies that the investigation be inclusive of "a national agency check (including a check of the fingerprint files of the Federal Bureau of Investigation (FBI)), and written inquiries to appropriate local law enforcement agencies, former employers and supervisors, references, and schools."

> "…all persons seeking the privilege of employment or privileged to be employed in the departments and agencies of the Government [shall] be adjudged by mutually consistent and no less than minimum standards and procedures among the departments and agencies…"

3.2.2 Executive Order 12968

Access to Classified Information

Executive Order 12968 was issued by President Clinton on August 2, 1995. It established "a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information." This order provides the adjudication guidelines currently utilized for the determination of access eligibility.

3.3 Presidential Directive

A Presidential Directive is a form of executive order issued by the President of the United States with the advice and consent of the National Security Council.

The Presidential Directive which pertains to personnel access authorization and clearance policy and procedures is Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors.*

3.3.1 Homeland Security Presidential Directive 12 (HSPD-12)

Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, was issued by President George W. Bush on August 27, 2004. The Directive enhances security and protects personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

The Directive charges the Secretary of Commerce to promulgate a Federal standard for secure and reliable forms of identification.

3.4 Federal Information Processing Standards (FIPS)

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA) of 2002. The approving authority for FIPS publications is the Secretary of Commerce.

The FIPS publication which provides standards pertinent to personnel access authorization and clearance policy and procedures is FIPS 201, *Personal Identity Verification for Federal Employees and Contractors.*

3.4.1 FIPS 201

Personal Identity Verification for Federal Employees and Contractors

This Federal standard, FIPS 201, was released February 25, 2005 by the National Institute of Standards and Technology (NIST). An updated version, FIPS 201-1, was released on June 26, 2006.

FIPS 201 establishes a standard for a reliable, government-wide PIV based on secure and reliable forms of identification credentials issued by the federal government to its employees and contractors. These credentials are intended to authenticate individuals who require physical access to controlled facilities and logical access to controlled information systems.

Section 4.0 of this document discusses FIPS 201 in detail.

3.5 Office of Management and Budget

The Office of Management and Budget (OMB) is one of the offices within the Executive Office of the President.

OMB issues "management" instructions concerning Executive Orders or tasks required of federal agencies. The OMB Memorandum pertains to personnel access authorization and clearance policy and procedures is M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12.*

3.5.1 OMB Memorandum M-05-24

M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12*, was issued by the Office of Management and Budget (OMB) on August 5 2005. It provides instructions to federal agencies and departments for implementing the requirements in FIPS 201 and HSPD-12.

The NRC, like all federal agencies, is mandated to implement the PIV standards in FIPS 201 under Presidential Directive HSPD-12.

The NRC personnel access authorization and clearance processes are impacted by the standards and guidance provided by FIPS 201 and M-05-24 with regard to adjudication and background investigations. This subject is covered in more detail in section 4.0 of this document.

FIPS 201 and M-05-24 also impact the NRC badging process. However, the badging process is the responsibility of the Facilities Security Branch and is therefore outside of the scope of this document.

3.6 NRC Management Directives (MDs)

MDs contain the policies and procedures that govern the internal NRC functions necessary for the agency to accomplish its regulatory mission.

The NRC MD which provides policy and guidance for personnel access authorization and clearance is MD 12.3, *NRC Personnel Security Program*. Also, MD 10.6, *Use of Consultants and Experts* provides some agency policy and guidance which pertains to access authorization and clearance for consultants.

3.6.1 NRC Management Directive (MD) 12.3

The objective of MD 12.3, *NRC Personnel Security Program* is to provide assurance that NRC employees, consultants, contractors, and licensees are sufficiently reliable and trustworthy to have access to NRC facilities, classified information, sensitive NRC information and equipment, nuclear power facilities, and special nuclear material.

MD 12.3 sets forth NRC policy to ensure that personnel suitability determinations are made in accordance with pertinent laws, Executive Orders, MDs, and applicable directives of other federal agencies for an:

- NRC access authorization (i.e., security clearance)
- NRC employment clearance (i.e., pre-appointment investigation waiver, Section 145b of the Atomic Energy Act of 1954 (AEA), as amended)
- Unescorted access to nuclear power facilities for NRC employees or contractors
- Access to special nuclear material by NRC licensees
- Access to unclassified Safeguards Information (SGI)
- Access to sensitive NRC information, technology systems or data
- Unescorted access to NRC facilities
- Visits involving classified National Security Information (NSI), Restricted Data (RD), or Sensitive Compartmented Information (SCI)
- Providing information to foreign regulatory assignees

It is also NRC policy that its workplace be free from illegal use, possession, or distribution of controlled substances.

3.6.2 NRC Management Directive (MD) 10.6

MD 10.6, *Use of Consultants and Experts* sets forth NRC policy concerning the appointment and utilization of consultants and experts to assist in the accomplishment of its mission. MD 10.6 policy also ensures that the appointment of such individuals is in accordance with applicable statutory and regulatory requirements.

Of particular pertinence to the personnel access authorization and clearance procedures is the direction in MD 10.6 to employ the services of individual consultants and experts by hiring them under the *Personnel Appointment Process* (e.g. the 145b process for employees).

Note: When the services of consultants and experts must be employed by contract or interagency agreement, the policies and procedures specified in MD 11.1, "NRC Acquisition of Supplies and Services," must be followed.

4.0 FIPS 201 Personal Identity Verification (PIV) Framework

Authentication of an individual's identity is a fundamental component of physical and logical access control processes. When an individual attempts to access security-sensitive buildings, computer systems, or data, an access control decision must be made. An accurate determination of identity is needed to make sound access control decisions.

FIPS 201, *Personal Identity Verification for Federal Employees and Contractors* "Establishes a standard for a reliable, government-wide Personal Identity Verification (PIV) based on secure and reliable forms of identification credentials *(e.g., ID badges)* issued by the federal government to its employees and contractors. These credentials are intended to authenticate individuals who require access to federally controlled facilities, information systems, and applications."

FIPS 201 contains two parts to guide department and agency implementation. The requirements of Part 2 build upon the requirements of Part 1.

Part 1: PIV-I Common Identification, Security and Privacy Requirements

PIV-I establishes the minimum requirements for a federal personal identification system that meets the control and security objectives of HSPD-12, including personal identity proofing, registration, and credential issuance process for employees and contractors.

Part 2: PIV-II Government-wide Uniformity and Interoperability

PIV-II establishes "detailed specifications to support technical interoperability among departments and agencies, including card elements, system interfaces, and security controls required to securely store and retrieve data from the card."

The PIV-II technical implementation guidance is not applicable to these procedures.

4.1 PIV-I Applicability

PIV-I applies to all employees, contractors and "other applicable individuals."

"Department and Agency heads must conduct a background investigation, adjudicate the results, and issue identity credentials to their employees and contractors who require long-term access to federally controlled facilities and/or information systems."

4.2 PIV-I Requirements

4.2.1 Investigation Requirements

M-05-24 establishes tasks and deadlines for implementation of PIV-I. Two required tasks from the PIV-I standard are directly pertinent to the access authorization and clearance process:

1. Initiate the National Agency Check with Written Inquiries (NACI) or other suitability or national security investigation prior to credential issuance
2. Verify and/or complete background investigations for all employees, contractors and other applicable individuals

4.2.2 Privacy Requirements

HSPD-12 explicitly states that protecting personal privacy is a requirement of the PIV system. As such, all departments and agencies must implement the PIV system in accordance with the spirit and letter of all privacy controls specified in the FIPS 201 standard, as well as those specified in federal privacy laws and policies including but not limited to the E-Government Act of 2002, the Privacy Act of 1974, and Office of Management and Budget (OMB) Memorandum M-03-22, as applicable.

4.3 Audit Records

The Personnel Security Branch (PSB) is responsible for the maintenance of all records related to the access authorization and clearance process.

The authorities requiring the maintenance of audit records include (but are not limited to) HSPD-12, FIPS 201, and FISMA. The primary justification for the maintenance of audit records includes:

- Protection of privacy
- Forensics and accountability
- Compliance with required security controls for federal information systems
- Independent, objective annual review and annual independent assessment by the Office of the Inspector General (OIG), as required by FISMA

4.3.1 Protection of Privacy

To ensure the privacy of applicants, agencies are required to assure that the technologies used in the department or agency's implementation of the PIV system allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program.

4.3.2 Forensics and Accountability

"All actions taken for approval/denial of requests by all participants in the PIV identity proofing and badge issuance process shall have an auditable trail that can support both forensic and system management capabilities. This audit trail shall provide a critical control component for the chain of trust for PIV issuance and management."

4.3.3 Compliance with Security Control Requirements for Federal Information Systems

Agencies are required to ensure audit and accountability security controls (described in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems)* are implemented on any federal information systems utilized for the PIV process. One example of a federal information system that is required to comply with audit and accountability security control guidance is the Integrated Personnel Security System (IPSS).

4.3.4 Independent and Objective Annual Review under FISMA

FISMA outlines the information security management requirements for agencies, including the requirement for an annual review and annual independent assessment. The annual assessments provide agencies with information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security including privacy of personnel data.

4.4 The PIV Role-Based Model

Sections 2.2 and 5.2 of the FIPS 201 standard require the adoption and use of an approved identity proofing and registration process. All identity proofing and registration systems must satisfy the PIV objectives and requirements stated in Sections 2.2 and 5.2 in order to be approved.

Identity Proofing is the process of providing sufficient information (e.g., identity history, credentials, documents) to a PIV Registrar when attempting to establish an identity.

Identity Registration is the process of making a person's identity known to the PIV system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.

Section 2.3 and 5.3 of the FIPS 201 standard requires the adoption and use of an approved *credential* issuance and management process. All credential issuance and management systems must satisfy the PIV objectives and requirements stated in sections 2.3 and 5.3 in order to be approved.

A **Credential** is evidence attesting to one's right or authority; in this standard, it is the "PIV Card" (e.g., the NRC ID badge).

The heads of federal departments and agencies may approve other identity proofing, registration, and issuance process sets that are accredited as satisfying the requisite PIV objectives and requirements.

4.4.1 Identity Proofing and Registration

For compliance with the PIV-I control objectives, the identity proofing and registration process must meet the following requirements when issuing identity credentials (e.g., ID badges).

The process shall begin with initiation of a NACI or other Office of Personnel Management (OPM) or National Security community investigation required for federal employment. This requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI. At a minimum, the FBI National Criminal History Check (fingerprint check) shall be completed before credential issuance.

Identity credentials issued to individuals without a completed NACI or equivalent must be electronically distinguishable from identity credentials issued to individuals who have a completed investigation.

The applicant must appear in-person at least once before the issuance of a PIV credential.

During identity proofing, the applicant shall be required to provide two forms of identity source documents in original form. The identity source documents must come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*. At least one document shall be a valid State or Federal government-issued picture identification (ID).

The PIV identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.

4.4.2 Roles and Responsibilities

The critical roles associated with the PIV identity proofing, registration and issuance process are the *Applicant*, *Sponsor*, *Registrar*, and *Issuer*. These roles may be ancillary roles assigned to personnel who have other primary duties.

The **Applicant** is the individual to whom a PIV credential needs to be issued. At the NRC, the Applicant may be an employee, consultant, or contractor.

The **Sponsor** is the individual who substantiates the need for, and makes the request for, a PIV credential to be issued to the Applicant. The Sponsor provides sponsorship to the Applicant. At the NRC, the Sponsor for an employee Applicant may be Human Resources; the Sponsor for a consultant or contractor may be an Office Director or Project Officer. For the PCI system, the Security Processing Unit within the PSB will serve as the electronic sponsor.

The **Registrar** is the entity responsible for identity proofing of the Applicant and ensuring the successful completion of the background checks. The PIV Registrar provides the final approval for the issuance of a PIV credential to the Applicant. At the NRC, the Registrar role is performed by two distinct operating groups within the PSB, the Security Processing Unit, and the Personnel Security Specialists (Adjudicators).

The **Issuer** is the entity that performs credential personalization operations and issues the identity credential to the Applicant after all identity proofing, background checks, and related approvals have been completed. At the NRC, the Issuer role is filled by the Facilities Security Branch.

The roles of PIV Applicant, Sponsor, Registrar, and Issuer, while not mutually exclusive, do contain the following provisions:

- Applicant cannot serve any other role in their personal access authorization and clearance process.
- Sponsor cannot serve as an Issuer.
- Registrar cannot serve as an Issuer.

Table 4.1: Example of the Role-based PIV Process for a New NRC Employee

PIV Role	Applicant	Sponsor	Registrar	Issuer
NRC Role	Employee Applicant	Human Resources (HR)	Personnel Security Branch (PSB)	Facilities Security Branch (FSB)
Responsibilities / Tasks	Provides two identity source documents and required background information	Begins the hiring process; requests PIV credential for Applicant	Completes background checks, adjudicates, and approves or denies PIV credential	Issues PIV credential after verifying Applicant's identity

5.0 Overview of the Access Authorization and Clearance Process

The access authorization and clearance process is a role-based model for identity proofing and registration contained in FIPS 201 PIV-I, involving roles and responsibilities of Sponsor, Applicant, Registrar, and the credential Issuer.

5.1 Roles and Responsibilities

The access authorization and clearance process incorporates the principle of separation of duties - the roles of PIV Applicant, Sponsor, Registrar, and Issuer, while not mutually exclusive, do contain the following provisions:

- Applicant cannot serve any other role in their personal access authorization and clearance process.
- Sponsor cannot serve as an Issuer.
- Registrar cannot serve as an Issuer.

5.1.1 Sponsor

The Sponsor is responsible for substantiating the need for access and makes the security clearance request on behalf of the Applicant. The Sponsor must assure the Applicant provides identification using at least two forms of approved certificates of identity per the I-9 documents list (i.e., Drivers License, Birth Certificate, Passport). The Sponsor also provides security forms to the Applicant.

In the case of new employees, the Sponsor's role is usually fulfilled by Human Resources in cooperation with an NRC Office Director or Deputy Office Director.

In the case of new contractors, the Sponsor's role is usually fulfilled by the designated NRC Project Officer.

5.1.2 Applicant

The Applicant is the employee/contractor (or prospective employee/contractor) who requires a clearance or appropriate access authorization in order to be able to perform their assigned duties. The Applicant completes the security forms and returns them to the Sponsor, who checks the forms for completeness and forwards them to the Registrar.

5.1.3 Registrar

The Registrar role is filled by two distinct operating groups within the PSB: the Security Processing Unit analysts and the Personnel Security Specialists (Adjudicators).

The Security Processing Unit analysts' responsibilities and tasks are:

- Verify the completeness of the Applicant's PIV security forms
- Establish an account for the Applicant on e-QIP;
- Provide notification to the Applicant to begin using e-QIP
- Enter Applicant data into IPSS and PCI

- Enroll Applicant, including capturing Applicant's photo, I-9 documents, and biometrics
    - Ensure that fingerprint images retained by the agency are formatted according to SP 800-76-1
        - Fingerprint templates stored on the PIV card are prepared from images of the primary and secondary fingers where the choice of fingers is based on the order of priority, as provided in FIPS 201-1, Section 4.4.1
        - Acquires fingerprint images in accordance with Table 2 in 800-76-1
    - Collect facial images that conform to SP 800-76-1
    - Capture the biometrics (fingerprints and facial image) that are used to personalize the PIV Card during the enrollment/identity proofing process
    - Capture the Applicant's fingerprints in accordance with the rolled live imaging mode

The Personnel Security Specialists' (Adjudicators) responsibilities and tasks are:

- Review the Applicant's PIV credentials, Standard Form 86 (SF-86) or Standard Form 85P (SF-85P), and initial security check results to render a 145b security clearance or access authorization interim approval or denial recommendation
- Initiate background investigation by OPM
- Review the OPM background investigation
- Resolve issues, if any, identified in the investigation process
- Render a recommendation for approval or denial of access
- If favorable, adjudicate Applicant in PCI

5.1.4 Credential Issuer

Upon notification by the Registrar of successful clearance or an interim approval, the Applicant reports to the *Issuer* to be issued a PIV card. The Issuer role is filled by the Facilities Security Branch. The Issuer's responsibilities and tasks are:

- Verify that the individual who collects the identity credential is indeed the Applicant by validating the individual's I-9 documents and establishing a 1:1 biometric match
- Produce and activate the PIV card
- Issue PIV card to Applicant after obtaining Applicant's acceptance of the PIV credential and the related responsibilities

5.2 Summary of the Access Authorization and Clearance Process

The primary activities of the access authorization and clearance process are:

- Request an access authorization or clearance
- Initial screening
- Suitability determination
- Interim access authorization (if applicable)
- Issuance of credential (PIV card)
- Background investigation by OPM (if applicable)
- Final approval

5.2.1 Request an Access Authorization or Clearance

The Sponsor is responsible for substantiating the need for access and requests the access authorization or clearance on behalf of the Applicant.

The Sponsor must assure the Applicant provides two forms of approved certificates of identity per the I-9 documents list (e.g., Drivers License, Birth Certificate, or Passport) and provides a package of security forms to the Applicant. The Sponsor also ensures that the security forms are completed by the Applicant.

5.2.2 Initial Screening

The Sponsor will receive the completed security forms package from the Applicant. The Applicant's security package is then submitted to the Registrar (PSB) for a determination.

5.2.3 Suitability Determination

When the Registrar (PSB) receives the completed security package, a Security Processing Unit Analyst begins a pre-screening process to verify completeness and accuracy of the package. Upon confirmation that the package is complete, the Analyst will enroll the Applicant and initiate preliminary checks that will help determine the Applicant's suitability for access authorization and/or clearance. IPSS and PCI are updated accordingly and the Applicant's folder is provided to a Personnel Security Specialist (Adjudicator).

5.2.4 Interim Access Authorization (if applicable)

Upon a favorable suitability determination by the Adjudicator and concurrence by appropriate management officials, interim approval for access authorization and credentials (i.e., PIV card) is granted. The Applicant must not have access to any classified information until the OPM background investigation is completed adjudicated, and the security clearance or access authorization is granted.

The PSB notifies the Sponsor and Facilities Security Branch.

5.2.5 Issuance of Credential (PIV Card)

The Applicant will be notified that they must pick up their PIV card. The Applicant must bring identifying credentials per the I-9 documents list. The FSB will verify the Applicant's identity and compare the Applicant's information to the data provided by the Registrar. The Issuer will conduct a 1:1 biometric match to check that the fingerprint of

the individual matches the biometric credential embedded in the PIV credential. The Issuer shall produce and activate the PIV credential. The physical access to NRC facilities on the PIV credential will be activated through PACS. The Issuer will issue the Applicant an electro-magnetically opaque sleeve or other protection technology to protect against any unauthorized contactless access to information stored on a PIV credential.

5.2.6 Background Investigation by OPM (if applicable)

An Adjudicator submits the request for a background investigation to OPM with specific instructions about the type and extent of investigation to be performed.

5.2.7 Final Approval

The Registrar receives the Report of Investigation with a Certification of Investigation, Case Closing Transmittal, and Form 79A from OPM with the completed background investigation. The Adjudicator reviews the investigation from OPM along with the Applicant's security folder and grants (or denies) final determination of the clearance. The Facilities Security Branch is notified of the final determination and issues a PIV Credential (PIV card), if favorable.

5.3 Applicant Badge Issuance Qualifications

HSPD-12 credentials will not be provided contractors or temporary employees working less than 6 months at the NRC, nor will HSPD-12 credentials be provided to credit union or daycare center workers or patrons. Foreign assignees and licensees will not be issued an HSPD-12 credential. Even though these individuals will not receive an HSPD-12 credential, their security packets will be processed in the same manner as PIV Applicants.

5.4 Truncated Names

According to FIPS 201-1, Zone 2 on the PIV card's front face will contain the Applicant's name. Specifically, FIPS 201-1 mandates that, "the full name shall be printed directly under the photograph in capital letters. The font shall be a minimum of 10 point." FIPS 201-1 Zone 2 specifications, in accordance with the Nuclear Regulatory Commission's (NRC) approved topology for the PIV card face and FIPS 201-1 approved printing capabilities, restrict both lines of the zone to 20 characters each.

The first line of the zone will include the Applicant's legal last name followed a comma. If the Applicant has a suffix on their name, the first line of the zone will include the Applicant's legal last name followed by a space, the suffix, a period, and a comma.

The second line of the zone will include the Applicant's legal first name and their middle initial followed by a period (if applicable).

If the contents of zone 2 exceed the space available, then the first or last name shall be truncated to fit the first 20 characters.

5.5 1-1 Biometric Match Fails

If three attempts have not been completed, the Issuer will recapture the Applicant's fingerprint and reattempt to match the fingerprint to the biometric credential embedded in the PIV credential.

After three attempts, in the event that the Applicant's fingerprint does not match the biometric embedded in the PIV credential at the time of activation; the Issuer will use a card profile that does not require biometric verification.

5.6 Regional Offices

Regional office Applicants or Applicants with access to a regional office will be directed by DFS to enroll for their PIV credentials at the regional office. The PIV card enrollment and issuance process will be the same as that for Headquarters Applicants. However, the printed PIV card with no active certificates will be sent to the regional office via certified mail. Once received by the regional office, the Applicant will be notified to appear in person for issuance and the Issuer will put the digital certificates on the PIV card at that time.

5.7 PIV Card Chain of Custody

ADM will serve as the primary custodian for blank and printed cardstock. The Security Officers and Issuers are permitted access to blank and printed cardstock held in the TWFN vault. The FSB Branch Chief delegates the roles of Security Officer and Issuer to the designated role holders. These role holders currently maintain a minimum of an 'L' clearance. Only authorized individuals are permitted access to the blank and printed cardstock. The Security Officers and Issuers use the HSPD-12 Badge Check-In/Check-Out Log to manage the cardstock.

The blank and printed cardstock is mailed to a security specialist within FSB and he/she checks-in the badges and stores them in the vault located on TWFN floor 6. The Security Officers and Issuers use the HSPD-12 Badge Check-In/Check-Out Log to manage the cardstock being stored in the vault.

Security Officers and Issuers are authorized to remove the cardstock from the vault at the time of activation. The Security Officers and Issuers use the HSPD-12 Badge Check-In/Check-Out Log to manage the cardstock being removed from the vault.

FSB stores inactive PIV cards with suspended physical access controls and deactivated logical access controls in the FSB vault located on TWFN floor 6 upon a cardholder's termination or separation from the agency in preparation for card destruction.

6.0 The 145b Process

This section describes the requirements and procedures for conducting pre-employment processing and adjudication of NRC Applicants for employment.

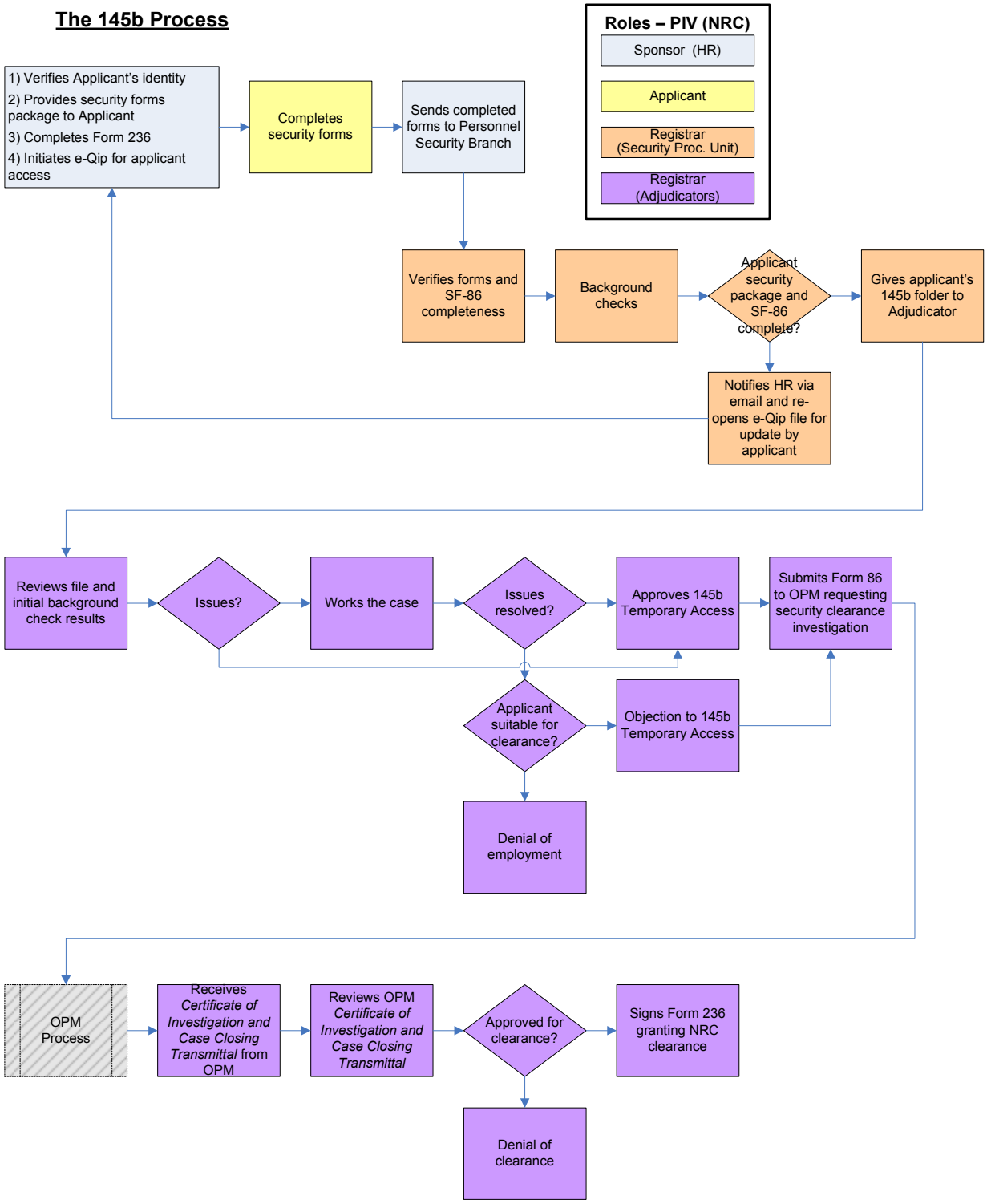
6.1 Overview

All federal employees are required to be investigated per Executive Order 10450.

The 145b Program is a waiver of the pre-appointment clearance investigation. This enables NRC employees to begin work prior to the completion of a background investigation. However, these employees may not have access to classified information until they have had a background investigation completed, adjudicated favorably, and been granted a security clearance.

Access authorization and clearance investigations for NRC employees are requested using the NRC Form 236, *Personnel Security Clearance Request and Notification*. The 145b requests are submitted through the Office of Human Resources or the Regional Personnel Office.

The 145b Process is illustrated on the following page.


The 145b Process
Roles – PIV (NRC)
Sponsor (HR)
Applicant
Registrar (Security Proc. Unit)
Registrar (Adjudicators)
1) Verifies Applicant's identity
2) Provides security forms package to Applicant
3) Completes Form 236
4) Initiates e-Qip for applicant access
Completes security forms
Sends completed forms to Personnel Security Branch
Verifies forms and SF-86 completeness
Background checks
Applicant security package and SF-86 complete?
Gives applicant's 145b folder to Adjudicator
Notifies HR via email and re-opens e-Qip file for update by applicant
Reviews file and initial background check results
Issues?
Works the case
Issues resolved?
Approves 145b Temporary Access
Submits Form 86 to OPM requesting security clearance investigation
Applicant suitable for clearance?
Objection to 145b Temporary Access
Denial of employment
OPM Process
Receives Certificate of Investigation and Case Closing Transmittal from OPM
Reviews OPM Certificate of Investigation and Case Closing Transmittal
Approved for clearance?
Signs Form 236 granting NRC clearance
Denial of clearance

6.2 Request for Access Authorization and Clearance for Employees

Prior to a request for personnel security clearance, HR will: (a) assure the Applicant's identity using at least two forms of approved certificates of identity (e.g., Drivers License, Birth Certificate, or Passport) and provide a security forms package; (b) perform education verification and employment reference checks on the Applicant; (c) send an authorized conditional offer of employment to the Applicant; and (d) initiate e-QIP access for the Applicant.

The Applicant will (a) complete, certify, and submit his/her SF-86, *Questionnaire for National Security Positions* via e-QIP, and print and sign any required forms; (b) obtain fingerprints from an authorized source; (c) read, complete, and sign all required forms in the security forms package; and, (d) return completed signed forms and fingerprint cards to HR, unless enrollment will occur prior to EOD at headquarters.

NRC Form 236, *Personnel Security Clearance Request and Notification* is used to request the appropriate level of security clearance and to request a 145b waiver of the pre-appointment clearance investigation. Part I is completed by the Applicant's employing office. The section which specifies the justification for the 145b employment request requires signature by the Office Director or Deputy Director of the employing office. The section which specifies the applicable position sensitivity criterion (i.e., "Q", "L (H)", or "L") requires signature by the Division Director (or designated delegate)

6.2.1 Sponsor Sends Applicant's forms to the Personnel Security Branch

HR submits the 145b package to the PSB. The 145b package delivered to PSB by HR should contain:

- Form 236, *Personnel Security Clearance Request and Notification*
- OF-612, *Application for Federal Employment* (or a resume)
- OF-306, *Declaration for Federal Employment*
- SF-87, OPM Fingerprint Card (2 copies)
- NRC Form 176, *Security Acknowledgement*
- Fair Credit Reporting Act Release
- Signed forms printed from e-QIP
- Pre-employment reference checks and education verification (completed by HR)
- Drug Testing Results (for designated positions)

Supplemental material may be sent with the Applicant's security package, as needed. For example: Foreign National Questionnaire, Naturalization Certificate, bankruptcy disposition papers, documentation of paid accounts, etc.

6.3 Initial Screening

The Applicant's 145b package undergoes initial screening for a determination for access authorization and/or clearance.

6.3.1 Registrar Processes the Applicant's forms

The Security Processing Unit analyst will:

1. Date stamp the back of each item in the 145b package
2. Verify that all required forms have been received
   - **If any required forms are missing or incomplete**, return them to HR. HR will contact the Applicant if necessary
   - **If the original Form 306, *Declaration of Federal Employment* is received,** make a copy for the Applicant's 145b folder and send the original back to HR
3. Via e-QIP, check the SF-86, Part I, "Agency Usage Block" to verify that HR entered the correct coding for NRC investigations and clearances
4. Print a copy of the Applicant's SF-86 from e-QIP
5. Create an NRC Form 225, *File Summary Sheet* from INFORMS
6. Assemble the Applicant's 145b folder
   a. Use light green folder
   b. Affix a label with the Applicant's SSN and name to the folder tab
   c. Affix a coversheet for Privacy Act Info to the front outer cover of the folder
   d. Arrange forms in the Applicant's 145b folder as follows:

Left Side (Sleeve 1), Top to Bottom	***Right Side (Sleeve 2), Top to Bottom***	***Left side (Sleeve 3)***	***Right Side (Sleeve 4), Top to Bottom***
NRC Form 225	SF-86 (from e-QIP)	Reciprocity request	NRC Form 176 – Security Acknowledgment
NRC Form 236	OF-306	Emails, Mail	Drug Test Results
Processing Unit checklist	Resume (or OF_612)	Internal (within NRC) requests	Zero Tolerance Statement (if provided)
PIV/ID documents	Fair Credit Reporting Act	Records of telephone calls	Education Verification
	<u>Pre-employment checks:</u> FBIF record Credit Report PIPS JPAS CPCI	Notes	NRC Form 212
	1 SF-87	Supplemental documents	1 SF-87

Supplemental Information

To print the NRC Form 225, File Summary Sheet in INFORMS:

a. Select Master List and select Form 225
b. Enter the applicant's name and DOB
c. Select the type of clearance to be processed
d. Date: enter the date clearance was requested
e. Select Investigative Agency to perform the investigation
f. Type the date the Fingerprint Cards were received
g. On the remarks section, type applicant's SSN and place of birth
h. Office Symbol: "HQ"
i. For 145b cases: Type Clearance = None
j. For 145b cases: Action: 145b
k. Type Clearance: "Q", "LH", or "L" (Form 236, "Clearance Requested" section)
l. Action: Grant
m. Employer Code: 1NRC (for employee applicants), 1NRC RI (for Region I employee applicants), 1NRC RII (for Region II employee applicants), etc.

6.3.2 Pre-screen the 145b Package

The pre-screening process is a series of preliminary checks to verify completeness and accuracy.

The Security Processing Unit analyst will perform the following checks and procedures:

1. Are all required forms in the 145b security package?
2. Are the forms complete?
3. Has the Applicant signed all of the forms?
4. Do the signatures on all the forms match?
5. Is the Applicant using his/her name as it reads on his/her official ID: Birth Certificate or Social Security Card?
6. Ensure that the information provided in the resume matches the information provided in the SF-86. If the person has provided information which has not been accounted for in the SF-86, ensure that the provided information is complete (e.g., any employment data that has not been listed in the SF-86 must include complete address, phone number and supervisor's name).
7. If the Applicant is not enrolled at HQ prior to EOD, ensure that data entered on SF-87, *Fingerprint Cards*, matches the Applicant data in the resume and the SF-86.
8. Ensure that data in the OF-306, *Declaration of Federal Employment*, matches the Applicant data in the resume and the SF-86.
9. Review the OF-306 for a positive response ("Yes") to questions 9-13. If there is a "Yes" response to any question, flag the information for the Adjudicator.
10. Review the Applicant's SF-86 and flag items that reflect derogatory information.
11. Has the Applicant signed the SF-86 signature forms?

12. Has the Applicant signed the Authorization for Release of Medical Information? (It must be signed if the Applicant answered "yes" to question 21 on the SF-86).

If there are any paper forms which are missing a signature, they must be sent back to HR for the Applicant's signature.

If there is a problem with the Applicant's SF-86, it must be corrected by the Applicant in e-QIP. To release e-QIP back to the Applicant for corrections:

1. Login to e-QIP
2. In the Applicant's record, select Review
3. Under Rejection Comments section, in the box labeled "Reject To Applicant Comments", provide a detailed record of which sections need corrections and what information is required
4. Scroll down and select "Reject to Applicant"
5. Email HR to notify that the Applicant needs to make corrections to his/her SF-86 in e-QIP

Supplemental Guidance (Sleeve 3 of 145b Folder)

Security Processing Unit analysts should retain all correspondence (e-mail, mail, or notes/records of telephone conversations) in the applicant's 145b folder.

Internal (within NRC) requests for information should be sent via e-mail.

Print all e-mail correspondence – both sent and received.

Keep record of all phone calls, including dates and times.

Date stamp any additional documents received and retain them in the applicant's 145b folder.

6.3.3 Create a Record in the Integrated Personnel Security System (IPSS)

The Security Processing Unit analyst will:

1. Login to IPSS
2. Under "Create a New Person", enter the Applicant's SSN and full name as it appears on the SF-86. If there is no middle name, enter "nmn"
3. Select "Create" to begin entering the Applicant's personnel security record. Ensure that the fields in the following sections pertaining to an individual's personnel security record are completed. (See Appendix D for details on the fields in each IPSS section)
   - Personal Data
   - Aliases
   - Employment Data
   - INS Info
   - Documents & Forms
   - Clearances/Access

- Security checks
- Investigation Data

6.4 Create a record in the PCI system (prior to EOD)

For those Applicants able to come to HQ for enrollment purposes prior to EOD, the Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

6.5 Perform Pre-Employment Checks

Upon confirmation that the package is complete, the Security Processing Unit analyst will perform preliminary checks that will help determine the Applicant's suitability for access authorization and clearance. These preliminary checks are:

- Credit check
- FBI Fingerprint and FBI Name checks
- PIPS (Personnel Investigations Processing System) check, which includes;
  - the SII (Security/Suitability Investigations Index)
  - the CVS (Clearance Verification System)
  - the JPAS (Joint Personnel Adjudication System)
- CPCI (Central Personnel Clearance Index)

See Appendix E for detailed information about PIPS, SII, CVS, JPAS, CPCI.

IPSS is then updated and the Applicant's folder is provided to a Personnel Security Specialist (Adjudicator).

6.5.1 Perform Preliminary Checks

The Security Processing Unit analyst will:

1. Perform preliminary checks that will help determine the Applicant's suitability for access authorization and clearance
2. Retain all background check reports in the Applicant's 145b folder, on the right side (Sleeve 2), between the Fair Credit Reporting Act and the SF-87 Fingerprint Cards. (See chart in 6.2.1)
3. Update the Applicant's Security Checks record in IPSS

When all required pre-screening and checks are complete, the Applicant's 145b folder should be up-to-date and ready for the Adjudicator to review. The Security Processing Unit analyst will then file the 145b folder on the Adjudicators' shelf, and notify the Personnel Security Specialist (e.g., the Adjudicator) by e-mail.

6.5.1.1 Credit Check

To perform a credit check on the Applicant, the Personnel Security Processing Unit analyst will:

1. Open Internet Explorer, and navigate to www.experian.com/esolutions/index.html
2. Login

   Select: ***Consumer Credit***

   Access Sub code: Select **TBD3 1487040 Rockville MD**

   Product: ***Employment Insight***
3. **Primary Applicant Box:** Enter the Applicant's name, SSN, date of birth, and phone number.

4. **Address Box:** Enter Applicant's current address. Click Submit.
5. Print the report

6.5.1.2 FBI Fingerprint and Name check

The Security Processing Unit analyst will send the Applicant's fingerprints to OPM via PIPS. Results usually come back via PIPS within a few business days.

6.5.1.3 PIPS - SII, CVS, and JPAS checks

The Personnel Security Processing Unit analyst will:

1. Login to PIPS
2. Select #2 CVS Menu
3. Select #1 SII/CVS/JPAS
4. Enter Applicant's SSN and last name and submit.
5. A report screen will display Applicant's data. Scroll to the bottom of the page to view further screen options. Screens containing data will be flagged with a "Y".
6. Select the number of the desired screen to view.
7. Print the desired reports and log out of PIPS

6.5.1.4 CPCI (Central Personnel Clearance Index)

The Personnel Security Processing Unit analyst will:

1. Login to CPCI. Open Internet Explorer and navigate to: https://cpci.doe.gov/loginPage.faces
2. Enter either the SSN or name of the Applicant
3. Print the report
4. Log out of the CPCI

6.6 Interim Access Authorization

Upon a favorable determination by the Adjudicator, and concurrence by appropriate management officials, a145b interim access authorization will be granted.

The PSB notifies HR and the Facilities Security Branch.

6.6.1 Favorable Eligibility Determination

The Adjudicator reviews the Applicant's 145b folder to determine eligibility for access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the eligibility determination for 145b access authorization is favorable, the following actions are performed:

1. The Adjudicator will:

(a) Write a 145b approval summary stating that the Applicant's 145b request has been adjudicated with no issues and is recommended for approval

(b) Deliver the 145b folder to the PSB Chief for review and consent to the approval recommendation

2. The Branch Chief will review the 145b folder, confirm consent by initialing the 145b approval summary, and forward the folder to the Division of Facilities Security Director.
3. The Division Director will review the 145b folder, confirm consent, check the "No security objection" box and sign Part III of the Form 236. The Applicant's 145b folder is returned to the Adjudicator to release the investigation request to OPM (See 6.6) then forwarded to the Security Processing Unit.
4. The Adjudicator will enter favorable adjudication for Applicant in PCI
   - Login to PCI
   - Click "Adjudicate Person" and search the Applicant to be adjudicated
   - Click the Applicant's name to open the Applicant's record
   - Set the NACI status to "Approved"
   - On the Personal tab, click "Card Issuance Approved"
   - Click "Save" and then click "Yes" to confirm adjudication
   - Select the appropriate card profile and click "Accept"
5. The Security Processing Unit analyst will:

   (a) Send a copy of the Form 236 to HR

   (b) Update the Applicant's Clearances/Accesses record in IPSS with the date the interim access was approved

   (c) Place the 145b folder on the EOD shelf

Supplemental Information

The Executive Director of Operations (EDO) is the official approver of 145b access authorizations. HR sends a list of Applicants who have been recommended for 145b interim access to the EDO for approvals. When the Applicant enters on duty he/she must not have access to any classified information until the OPM security background investigation is completed and a security clearance is granted.

6.6.2 Unfavorable Eligibility Determination

The Adjudicator reviews the Applicant's 145b folder to determine eligibility for access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the determination for 145b access authorization is unfavorable, the Adjudicator will inform HR that a determination is pending the completed OPM background investigation and favorable adjudication.

In most cases, the following actions are performed:

1. The Adjudicator will:
   (a) Write a 145b denial memorandum stating that the Applicant is not eligible for a 145b access authorization, including a brief summary of the cause. (If the Adjudicator's findings indicate that the Applicant is not suitable for employment, this determination and justification is included in the denial memorandum)
   (b) Write a letter to the Applicant, providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*.
   (c) Deliver the 145b folder to the PSB Chief for review and consent to the denial recommendation
2. The Branch Chief will review the 145b folder, confirm consent by initialing the 145b denial memorandum, and forward the folder to the Division of Facilities and Security Director
3. The Division of Facilities and Security Director will review the 145b folder, confirm consent, check the "Denied" box, sign Part III of the Form 236, and forward the folder with the letter to the Applicant to the Office of Administration Director for signature (as required by 10 CFR 10.22).
4. The Office of Administration Director reviews the 145b folder and signs the letter to the Applicant. The Applicant's 145b folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the Applicant
2. Retain 1 set of copies in the Applicant's security folder
3. Send a copy of the 236 and the original denial memo to HR
4. Send the original signed letter to the Applicant
5. Update the Applicant's record in IPSS
6. File the Applicant's security folder to the "Denied" shelf

HR will notify the employee that 145b has been denied.

The Applicant may appeal the decision with PSB and the Office of the General Counsel, per 10 CFR Part 10.

6.7 Background Investigation by OPM (if applicable)

The Adjudicator will:

1. Login to e-QIP
2. Double-check the accuracy of the information Agency Usage Block, Part I of the Applicant's SF-86
3. Print a final copy of the Applicant's SF-86 from e-QIP, and stamp it with the investigation type and the date requested
4. Add the new copy of the Applicant's SF-86 to the 145b folder
5. Purge the old copy from the folder.

   Note: Any printed information containing sensitive personal information must be shredded or destroyed according to NRC media destruction procedure.
6. Select "Release From Agency" (to submit the Applicant's information to OPM for a clearance investigation). Update the 225 File Summary with the date to OPM.

   Note: The Adjudicator might have already requested a valid prior investigation from another agency (see Reciprocity procedure.) In this case there will be a note on the right side of the folder stating that that an OPM clearance investigation will not be requested
7. Return the Applicant's 145b folder to the Security Processing Unit

The Security Processing Unit analyst updates the Applicant's record in IPSS with the current investigation type and the date requested and files the 145b folder on the "Entry on Duty" (EOD) shelf.

6.8 Entry on Duty

HR maintains Entry on Duty (EOD) information for each Applicant. Once confirmation is received that the Executive Director of Operations has approved the Applicant's 145b interim access authorization, HR notifies the Applicant of their employment start date.

HR sends an EOD list to the PSB each Friday.

The Security Processing Unit analyst will:

1. Remove the Applicant's file from the EOD shelf
2. Give the folder to the Adjudicator.

The Adjudicator will:

1. Sign the NRC Form 236 Part III and add the date of EOD
2. Update the NRC Form 225, *File Summary Sheet* with the EOD date.

The 145b folder is then returned to the Security Processing Unit for the following steps:

1. Update IPSS with EOD date
2. Make copies of 236 for badge.
3. Place file on Active shelf.

6.9 Issuance of Credential (NRC ID Badge)

On the first day that the Applicant reports to work, he/she is now an employee with 145b interim access authorization (i.e., no access to classified information). New employees meet in the lobby and are escorted to their security orientation briefing where they sign SF-312, *Classified Information Nondisclosure Agreement.* New employees not previously enrolled for their PIV card will report to PSB for enrollment.

6.9.1 Create a record in the PCI system (if applicable)

HR directs the new employees, who were not previously enrolled, to the PSB. The Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents

13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

The employee must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

Employees (145b) receive a temporary badge until their PIV card is ready for issuance.

6.9.2 Day 1 - Security Orientation Briefing

The PSB Adjudicators conduct a mandatory security orientation briefing for new employees where the employees are required to sign an SF-312, *Classified Information Nondisclosure Agreement.* At this time, the employee has 145b access which does not allow access to classified information. However, once the employee's OPM background investigation is completed and clearance is approved, the employee will receive a new badge indicating their clearance based on their "need-to-know."

A Security Processing Unit analyst will retain the SF-312 in the SF-312 security binder and update IPSS with the date of the SF-312 signature.

6.9.3 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

6.9.4 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally,

the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.

- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall ensure that the Applicant's PIV credential has "Employee" in Zone 8: Employee Affiliation.

The Issuer shall ensure that the Applicant's PIV credential has their correct office location (i.e. HQ, RI, RII, etc.) in Zone 17.

In the event the Applicant is a first responder, the Issuer shall ensure that the Applicant's PIV credential has a red line in Zone 12 indicating that the Applicant is a first responder.

The Issuer shall ensure that the Applicant (145b) receives a badge with NC in Zone 4: Clearance Designation, indicating that the individual has no clearance and he/she must have no access to classified information.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request
- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

6.9.5 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

6.10 Final Approval

Once the background investigation has been completed, OPM sends a package containing the results of the investigation to the PSB, with a *Certification of Investigation, Case Closing Transmittal,* and a Form 79A, *Report of Agency Adjudicative Action*.

The Security Processing Unit analyst will:

1. Stamp the back of the Certification of Investigation and Case Closing Transmittal (CCT) with the date received.
2. Update the IPSS investigation record to reflect the date received from OPM, the closed investigation date, and the date forwarded for adjudication.

3. Attach the Certificate and Form 79A, and any additional investigation reports (in the order they were received) to the top, right side of the folder.
4. Place the folder on the closed initial investigation shelf for adjudication.

The Adjudicator will review the employee's SF-86 and the background investigation report results in order to make a final determination for a clearance.

<u>If the employee is approved for clearance</u>:

The Adjudicator will:

1. Sign and date the Certification of Investigation, and stamp the CCT "Reviewed and Approved"; the Certification of Investigation is retained in the folder, and a copy is sent to HR for the employee's official personnel file (OPF)
2. Complete the Form 79A with the adjudicative action, sign, and date the form; a copy of the Form 79A is retained in the folder, and the original is sent to OPM
3. Update and sign the Form 225, *File Summary Sheet* with the grant date.
4. Update and sign Part IV of the NRC Form 236, including investigative agency and type of investigation; the NRC Form 236 is retained in the folder, and a copy is sent to the Facilities Security Branch Badge Office to initiate the creation of a new badge (Blue for Q clearance; Yellow for L clearance) for the employee
5. The Adjudicator will enter favorable adjudication for Applicant in PCI
    - Login to PCI
    - Click "Adjudicate Person" and search the Applicant to be adjudicated
    - Click the Applicant's name to open the Applicant's record
    - Set the NACI status to "Approved"
    - On the Personal tab, click "Card Issuance Approved"
    - Click "Save" and then click "Yes" to confirm adjudication
    - Select the appropriate card profile and click "Accept"

Note: The employee will receive an e-mail notification when the new badge is ready for pickup at the Badging Office.

The Security Processing Unit analyst will:

1. Update the employee's clearance record in IPSS to reflect the 145b terminated with a termination date.
2. Create a clearance record with the clearance designated on the NRC Form 236, make the action "active", and add the grant date reflected on the NRC Form 236.
3. File the folder on the active shelf

6.10.1 Create a record in the PCI system (Final Badge Issuance)

DFS directs the employee to the PSB. The Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

The employee must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

6.10.2 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

6.10.3 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.
- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall ensure that the Applicant's PIV credential has "Employee" in Zone 8: Employee Affiliation.

The Issuer shall ensure that the Applicant's PIV credential has their correct office location (i.e. HQ, RI, RII, etc.) in Zone 17.

In the event the Applicant is a first responder, the Issuer shall ensure that the Applicant's PIV credential has a red line in Zone 12 indicating that the Applicant is a first responder.

The Issuer shall ensure that the Applicant's PIV credential has their correct clearance designation (i.e. L, LH, Q) in Zone 4.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request

- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

6.10.4 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

If the employee is not approved for clearance:

The Adjudicator will:

1. Sign and date the Certificate of Investigation, stamp the CCT "Denied", and retain it in the employee's security folder
2. Sign and date the Form 79A, retain a copy in the employee's security folder, and send the original to OPM
3. Update and sign the Form 225, *File Summary Sheet*
4. Write a denial memorandum stating that the employee is not eligible for an access authorization, including a brief summary of the cause
5. Write a letter to the employee, providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*
6. Deliver the employee's security folder to the PSB Chief for review and consent to the denial recommendation

The Branch Chief will review the consultant-employee's security folder and confirm consent by signing the denial memorandum. The letter to the employee and the folder will then be forwarded to the Division of Facilities and Security Director for review and concurrence. The file is then forwarded to the Office of Administration Director for signature (as required by 10 CFR 10.22).

The Office of Administration Director reviews the employee's security folder and signs the letter to the employee. The security folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the employee
2. Retain 1 set of copies in the employee's security folder
3. Send the original denial memorandum to HR
4. Send the original signed letter to the employee
5. Update the employee's record in IPSS

6. File the employee's security folder to the "TERM" shelf

HR will notify the employee that the clearance has been denied.

The employee will be given appeal rights according to 10 CFR Part 10.

If the situation cannot be resolved and the employee cannot be granted a clearance, the employee will be terminated per NRC HR procedures and a Form 136; *Security Termination Statement* must be completed.

7.0 The Consultants and Experts Process

This section describes the requirements and procedures for adjudicating consultants and experts engaged by the NRC for access authorization and/or clearance.

7.1 Overview

From MD 10.6, *Use of Consultants and Experts*:

"*It is the policy of the NRC to appoint and utilize consultants and experts to assist in the accomplishment of NRC's mission and to appoint such individuals in accordance with applicable statutory and regulatory requirements.*"

"It is also the policy of the NRC to employ the services of individual consultants and experts by hiring them under the personnel appointment process, which establishes an employee-employer relationship with the NRC, whenever possible."

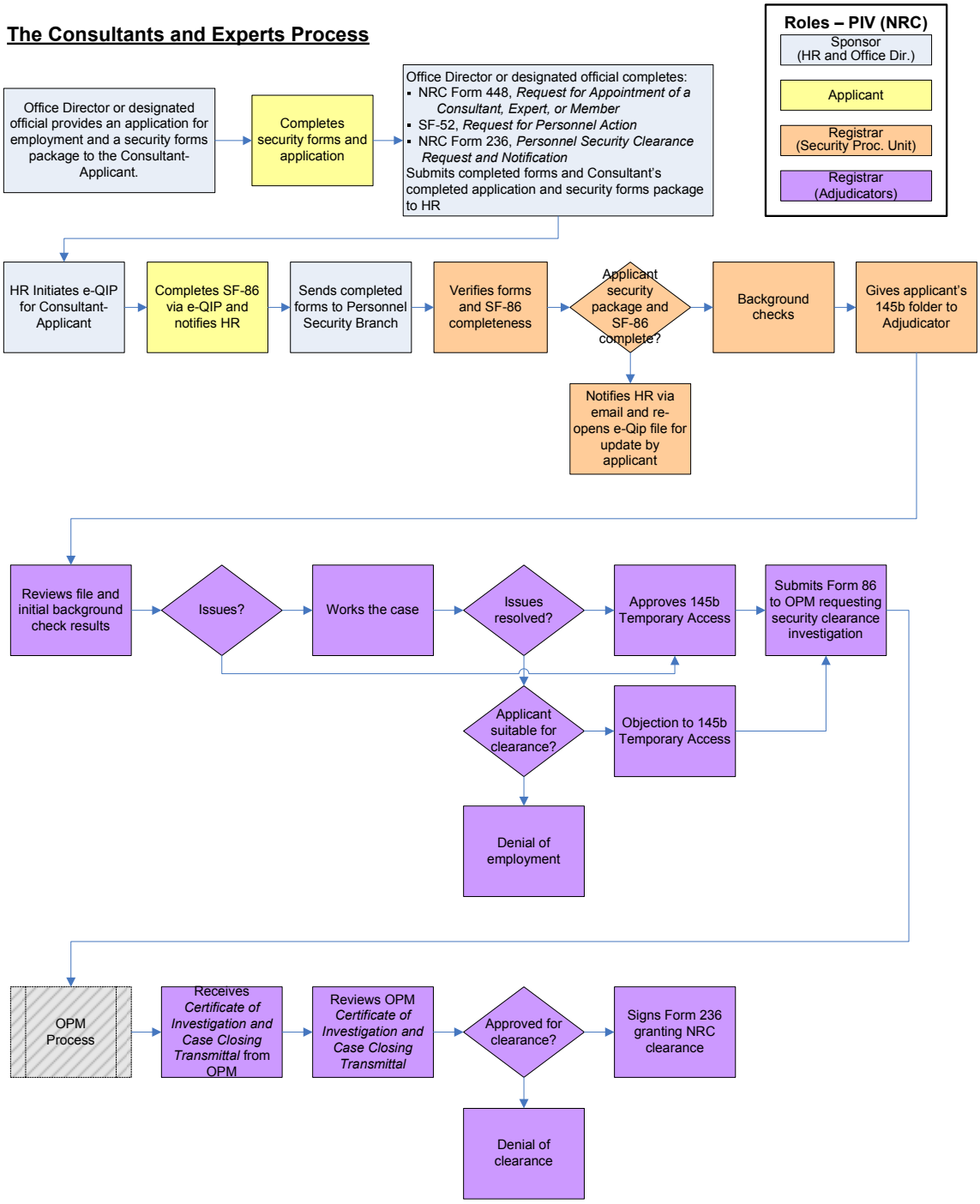
Consultants and experts whose services are employed through the appointment process are subject to the security clearance requirements applicable to all employees pursuant to the policy and guidance in MD 12.3, *NRC Personnel Security Program*. Therefore, most consultants are granted interim access and clearance according to the 145b Process.

When the services of consultants and experts must be employed by contract or interagency agreement, the policies and procedures specified in MD 11.1, *NRC Acquisition of Supplies and Services* must be followed. These consultants would be granted interim access and clearance according to the contractor with clearance process.

The consultants and experts process begins with a formal request for access authorization and clearance.

The consultants and experts process is illustrated on the following page.

The Consultants and Experts Process



7.2 Request for Access Authorization and Clearance

Prior to a request for security clearance, an Office Director or designated official will:

1. Determine the proposed consultant's qualifications and availability to serve
2. Send the individual a letter enclosing an application for employment and a security forms package
3. Complete the following forms:
   - NRC Form 448, *Request for Appointment of a Consultant, Expert, or Member*
   - SF-52, *Request for Personnel Action*
   - NRC Form 236, *Personnel Security Clearance Request and Notification*

NRC Form 236, *Personnel Security Clearance Request and Notification* is used to request the appropriate level of security clearance and to request a 145b waiver of the pre-appointment clearance investigation. Part I is completed by the Applicant's employing office. The section which specifies the justification for the 145b employment request requires signature by the Office Director or Deputy Director of the employing office. The section which specifies the applicable position sensitivity criterion (i.e., "Q", "L (H)", or "L") requires signature by the Division Director (or designated delegate).

After the prospective consultant completes the application for employment and the security forms package (including obtaining fingerprints), he or she will return them to the official.

The official then submits the internal forms and the Applicant's completed paperwork to Human Resources (HR).

HR will:

1. Perform education verification and employment reference checks on the Applicant
2. Send an authorized conditional offer of employment to the Applicant
3. Initiate e-QIP access for the Applicant.

The Applicant will complete, certify, and submit his/her SF-86, *Questionnaire for National Security Positions* via e-QIP; print and sign any required forms; and return completed, signed forms to HR.

7.2.1 Sponsor Sends Applicant's forms to the Personnel Security Branch

HR submits the 145b package to the PSB. The 145b package delivered to PSB by HR should contain:

- Form 236, *Personnel Security Clearance Request and Notification*
- OF-612, *Application for Federal Employment* (or a resume)
- OF-306, *Declaration for Federal Employment*
- SF-87, OPM Fingerprint Card (2 copies)
- NRC Form 176, *Security Acknowledgement*
- Fair Credit Reporting Act Form
- Signed forms printed from e-QIP

- Pre-employment reference checks and education verification (completed by HR)
- Drug Testing Results (for designated positions)

Supplemental material may be sent with the Applicant's security package, as needed. For example: Foreign National Questionnaire, Naturalization Certificate, bankruptcy disposition papers, documentation of paid accounts, etc.

7.3 Initial Screening

The Applicant's 145b package undergoes initial screening for an eligibility determination for access authorization and clearance.

7.3.1 Registrar Processes the Applicant's forms

The Security Processing Unit analyst will:

1. Date stamp the back of each item in the 145b package.
2. Verify that all required forms have been received.
   - **If any required forms are missing or incomplete**, return them to HR. HR will contact the Applicant if necessary.
   - **If the original Form 306, *Declaration of Federal Employment* is received,** make a copy for the Applicant's 145b folder and send the original back to HR.
3. Via e-QIP, check the SF-86, Part I, "Agency Usage Block" to verify that HR entered the correct instructions for NRC investigations and clearances.
4. Print a copy of the Applicant's SF-86 from e-QIP
5. Create an NRC Form 225, *File Summary Sheet* from INFORMS.
6. Assemble the Applicant's 145b folder
   a. Use light green folder
   b. Affix a label with the Applicant's SSN and name to the folder tab
   c. Affix a coversheet for Privacy Act Info to the front outer cover of the folder
   d. Arrange forms in the Applicant's 145b folder as follows:

Left Side (Sleeve 1), Top to Bottom	***Right Side (Sleeve 2), Top to Bottom***	***Left side (Sleeve 3)***	***Right Side (Sleeve 4), Top to Bottom***
NRC Form 225	SF-86 (from e-QIP)	Reciprocity request	NRC Form 176 – Security Acknowledgment
NRC Form 236	OF-306	Emails, Mail	Drug Test Results
NRC Form 448	Resume (or OF_612)	Internal (within NRC) requests	Zero Tolerance Statement (if provided)

Processing Unit checklist	Fair Credit Reporting Act	Records of telephone calls	1 SF-87
PIV/ID documents	Pre-employment checks: FBIF record Credit Report PIPS JPAS CPCI	Notes	
	1 SF-87	Supplemental documents	

Supplemental Information

To print the NRC Form 225, File Summary Sheet in INFORMS:

a. Select Master List and select Form 225
b. Enter the applicant's name and DOB
c. Select the type of clearance to be processed
d. Date: enter the date clearance was requested
e. Select Investigative Agency to perform the investigation
f. Type the date the Fingerprint Cards were received
g. On the remarks section, type applicant's SSN and place of birth
h. Office Symbol: "HQ"
i. For 145b cases: Type Clearance = None
j. For 145b cases: Action: 145b
k. Type Clearance: "Q", "LH", or "L" (Form 236, "Clearance Requested" section)
l. Action: Grant
m. Employer Code: 2NRC (for employee applicants), 2NRC RI (for Region I employee applicants), 2NRC RII (for Region II employee applicants), etc.

7.3.2 Pre-screen the 145b Package

The pre-screening process is a series of preliminary checks to verify completeness and accuracy.

The Security Processing Unit analyst will perform the following checks and procedures:

1. Are all required forms in the 145b security package?
2. Are the forms complete?
3. Has the Applicant signed all of the forms?
4. Do the signatures on all the forms match?
5. Is the Applicant using his/her name as it reads on his/her official ID: Birth Certificate or Social Security Card?
6. Ensure that the information provided in the resume matches the information provided in the SF-86. If the person has provided information which has not been accounted

for in the SF-86, ensure that the provided information is complete (e.g., any employment data that has not been listed in the SF-86 must include complete address, phone number and supervisor's name).

7. Ensure that data entered on SF-87, *Fingerprint Cards*, matches the Applicant data in the resume and the SF-86.
8. Ensure that data in the OF-306, *Declaration of Federal Employment*, matches the Applicant data in the resume and the SF-86.
9. Review the OF-306 for a positive response ("Yes") to questions 9-13. If there is a "Yes" response to any question, flag the information for the Adjudicator.
10. Review the Applicant's SF-86 and flag items that reflect derogatory information.
11. Has the Applicant signed the SF-86 signature forms?
12. Has the Applicant signed the Authorization for Release of Medical Information? (It must be signed if the Applicant answered "yes" to question 21 on the SF-86).

If there are any paper forms which are missing a signature, they must be sent back to HR for the Applicant's signature.

If there is a problem with the Applicant's SF-86, it must be corrected by the Applicant in e-QIP. To release e-QIP back to the Applicant for corrections:

1. Login to e-QIP
2. In the Applicant's record, select Review
3. Under Rejection Comments section, in the box labeled "Reject To Applicant Comments", provide a detailed record of which sections need corrections and what information is required.
4. Scroll down and select "Reject to Applicant"
5. Email HR to notify that the Applicant needs to make corrections to his/her SF-86 in e-QIP.

Supplemental Guidance (3rd sleeve of 145b folder)

Security Processing Unit analysts should retain all correspondence (e-mail, mail, or notes/records of telephone conversations) in the applicant's 145b folder.

Internal (within NRC) requests for information should be sent via e-mail.

Print all e-mail correspondence – both sent and received.

Keep record of all phone calls, including dates and times.

Date stamp any additional documents received and retain them in the applicant's 145b folder.

7.3.3 Create a Record in the Integrated Personnel Security System (IPSS)

The Security Processing Unit analyst will:

1. Login to IPSS

2. Under “Create a new person”, enter the Applicant’s SSN and full name as appears on the SF-86. If there is no middle name, enter “nmn”
3. Select “Create” to begin entering the Applicant’s personnel security record. Ensure that the fields in the following sections pertaining to an individual’s personnel security record are completed. (See Appendix D for details on the fields in each IPSS section)
   - Personal Data
   - Aliases
   - Employment Data
   - INS Info
   - Documents & Forms
   - Clearances/Access
   - Security checks
   - Investigation Data

7.4 Create a record in the PCI system (prior to EOD)

For those Applicants able to come to HQ for enrollment purposes prior to EOD, the Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant’s information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position” tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the “Sponsor” tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click “Save” and then click “Yes” to confirm sponsorship

7. Click “Enroll Person” and search the Applicant
8. Click on the Applicant’s name to open the Applicant’s record
9. Click the "Biometrics" tab
10. Capture the Applicant’s biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant’s two I-9 documents
13. Upon verifying all the required information is both captured and valid, click “Save” and then click “Yes” to confirm enrollment

7.5 Perform Pre-Employment Checks

Upon confirmation that the package is complete, the Security Processing Unit analyst will perform preliminary checks that will help determine the Applicant’s suitability for access authorization and clearance. These preliminary checks are:

- Credit check
- FBI Fingerprint and FBI name checks
- Personnel Investigations Processing System (PIPS) check, which includes
  - the SII
  - the CVS and
  - the JPAS
- CPCI

See Appendix E for detailed information about PIPS, SII, CVS, JPAS, CPCI.

IPSS is then updated and the Applicant’s folder is provided to a Personnel Security Specialist (Adjudicator).

7.5.1 Perform Preliminary Checks

The Security Processing Unit analyst will:

1. Perform preliminary checks that will help determine the Applicant’s suitability for access authorization and clearance
2. Retain all background check reports in the Applicant’s 145b folder, on the right side (Sleeve 2), between the Fair Credit Reporting Act and the SF-87 Fingerprint Cards. (See chart in 7.3.1)
3. Update the Applicant’s Security Checks record in IPSS

When all required pre-screening and checks are complete, the Applicant’s 145b folder should be up-to-date and ready for the Adjudicator to review. The Security Processing Unit analyst will then file the 145b folder on the Adjudicators’ shelf, and notify the Personnel Security Specialist (e.g., the Adjudicator) by e-mail.

7.5.1.1 Credit Check

To perform a credit check on the Applicant, the Personnel Security Processing Unit analyst will:

1. Open Internet Explorer, and navigate to www.experian.com/esolutions/index.html
2. Login

   Select: **Consumer Credit**

   Access Subcode: Select **TBD3 1487040 Rockville MD**

   Product: **Employment Insight**
3. **Primary Applicant Box:** Enter the Applicant's name, SSN, date of birth, and phone number.
4. **Address Box:** Enter Applicant's current address. Click submit
5. Print the report

7.5.1.2 FBI Fingerprint and Name check

The Security Processing Unit analyst will scan the fingerprint card and send the file to OPM via PIPS. Results usually come back via PIPS after a few business days.

7.5.1.3 PIPS - SII, CVS, and JPAS checks

The Personnel Security Processing Unit analyst will:

1. Login to PIPS
2. Select #2 CVS Menu
3. Select #1 SII/CVS/JPAS
4. Enter Applicant's SSN and last name and submit.
5. A report screen will display Applicant's data. Scroll to the bottom of the page to view further screen options. Screens containing data will be flagged with a "Y".
6. Select the number of the desired screen to view.
7. Print the desired reports and log out of PIPS

7.5.1.4 CPCI (Central Personnel Clearance Index)

The Personnel Security Processing Unit analyst will:

1. Login to CPCI. Open Internet Explorer and navigate to: https://cpci.doe.gov/loginPage.faces
2. Enter either the SSN or name of the Applicant
3. Print the report
4. Log out of the CPCI

7.6 Interim Access Authorization

Upon a favorable suitability determination by the Adjudicator, and concurrence by appropriate management officials, a145b interim access authorization will be granted.

The PSB notifies HR, the Facilities Security Branch, and the OIS. An OIS IT Coordinator requests an account to be created in the NRC Enterprise Directory Services, and coordinates with the Facilities Security Branch to enable the basic physical and logical access required by the Applicant. Badge data is entered into the Access Control System, and IPSS data is verified and updated.

7.6.1 Favorable Eligibility Determination

The Adjudicator reviews the Applicant's 145b folder to determine eligibility for access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the eligibility determination for 145b access authorization is favorable, the following actions are performed:

1. The Adjudicator will:
   (a) Write a 145b approval summary stating that the Applicant's 145b request has been adjudicated with no issues and is recommended for approval
   (b) Deliver the 145b folder to the PSB Chief for review and consent to the approval recommendation
2. The Branch Chief will review the 145b folder, confirm consent by initialing the 145b approval summary, and forward the folder to the Division of Facilities Security Director.
3. The Division Director will review the 145b folder, confirm consent, check the "No security objection" box and sign Part III of the Form 236. The Applicant's 145b folder is returned to the Adjudicator to release the investigation request to OPM (See 7.6) then forwarded to the Security Processing Unit.
4. The Adjudicator will enter favorable adjudication for Applicant in PCI
   - Login to PCI
   - Click "Adjudicate Person" and search the Applicant to be adjudicated
   - Click the Applicant's name to open the Applicant's record
   - Set the NACI status to "Approved"
   - On the Personal tab, click "Card Issuance Approved"
   - Click "Save" and then click "Yes" to confirm adjudication
   - Select the appropriate card profile and click "Accept"
5. The Security Processing Unit analyst will:
   (a) Send a copy of the Form 236 to HR
   (b) Update the Applicant's Clearances/Accesses record in IPSS with the date the interim access was approved

(c) Place the 145b folder on the EOD shelf.

Supplemental Information

The Executive Director of Operations (EDO) is the official approver of 145b access authorizations. HR sends a list of Applicants who have been recommended for 145b interim access to the EDO for approvals. When the Applicant enters on duty he/she must not have access to any classified information until the OPM security background investigation is completed and a security clearance is granted.

7.6.2 Unfavorable Eligibility Determination

The Adjudicator reviews the Applicant's 145b folder to determine eligibility for access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the eligibility determination for 145b access authorization is unfavorable, the Adjudicator can make a determination of suitability for employment pending completion of the OPM security background investigation resulting in the approval of a security clearance. However, this is very rare.

In most cases, the following actions are performed:

1. The Adjudicator will:
   (a) Write a 145b denial memorandum stating that the Applicant is not eligible for a 145b access authorization, including a brief summary of the cause. (If the Adjudicator's findings indicate that the Applicant is not suitable for employment, this determination and justification is included in the denial memorandum)
   (b) Write a letter to the Applicant, providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*.
   (c) Deliver the 145b folder to the PSB Chief for review and consent to the denial recommendation
2. The Branch Chief will review the 145b folder, confirm consent by initialing the 145b denial memorandum, and forward the folder to the Division of Facilities Security Director
3. The Division of Facilities Security Director will review the 145b folder, confirm consent, check the "Denied" box, sign Part III of the Form 236, and forward the folder with the letter to the Applicant to the Office of Administration Director for signature (as required by 10 CFR 10.22).
4. The Office of Administration Director reviews the 145b folder and signs the letter to the Applicant. The Applicant's 145b folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the Applicant
2. Retain 1 set of copies in the Applicant's security folder
3. Send a copy of the 236 and the original denial memo to HR
4. Send the original signed letter to the Applicant
5. Update the Applicant's record in IPSS
6. File the Applicant's security folder to the "Denied" shelf

If the Applicant has been denied employment, the Adjudicator will ensure that the 145b folder is updated with all documentation required for closure and returned to the Security Processing Unit for placement in 'TERM' files.

If the Applicant has not been denied employment, the clearance process continues. The OPM clearance investigation must be completed, favorably adjudicated, and clearance granted before the Applicant can enter on duty.

7.7 Background Investigation by OPM (if applicable)

The Adjudicator will:

1. Login to e-QIP
2. Double-check the accuracy of the information Agency Usage Block, Part I of the Applicant's SF-86
3. Print a final copy of the Applicant's SF-86 from e-QIP, and stamp it with the investigation type and the date requested
4. Add the new copy of the Applicant's SF-86 to the 145b folder
5. Purge the old copy from the folder.

   Note: Any printed information containing sensitive personal information must be shredded or destroyed according to NRC media destruction procedure.
6. Select "Release From Agency" (to submit the Applicant's information to OPM for a clearance investigation). Update the 225 File Summary with the date to OPM.

   Note: The Adjudicator might have already requested a valid prior investigation from another agency (see Reciprocity procedure.) In this case there will be a note on the right side of the folder stating that that an OPM clearance investigation will not be requested
7. Return the Applicant's 145b folder to the Security Processing Unit

The Security Processing Unit analyst updates the Applicant's record in IPSS with the current investigation type and the date requested and files the 145b folder on the "Entry on Duty" (EOD) shelf.

7.8 Entry on Duty

HR maintains EOD information for each Applicant. Once confirmation is received that the Executive Director of Operations has approved the Applicant's 145b interim access authorization, HR notifies the Applicant of their employment start date.

HR sends an EOD list to the PSB each Friday.

The Security Processing Unit analyst will:

1. Remove the Applicant's file from the EOD shelf
2. Give the folder to the Adjudicator.

The Adjudicator will:

1. Sign the NRC Form 236 Part III and add the date of EOD
2. Update the NRC Form 225, *File Summary Sheet* with the EOD date.

The 145b folder is then returned to the Security Processing Unit for the following steps:

1. Update IPSS with EOD date
2. Make copies of 236 for badge.
3. Place file on Active shelf.

The 145b folder is then returned to the Security Processing Unit for filing

7.9 Issuance of Credential (NRC ID Badge)

On the first day that the consultant-Applicant reports to work, he/she enters officially into an employee-employer relationship with the NRC with 145b interim access authorization, with no access to classified information.

7.9.1 Create a record in the PCI system (if applicable)

HR directs the new consultants-employees, who were not previously enrolled, to the PSB. The Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)

- Location
- Social Security Number

4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

The consultant-employee must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

Consultants-Employees (145b) receive a temporary badge until their PIV card is ready for issuance.

7.9.2 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

7.9.3 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.
- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall ensure that the Applicant's PIV credential has "Employee" in Zone 8: Employee Affiliation.

The Issuer shall ensure that the Applicant's PIV credential has their correct office location (i.e. HQ, RI, RII, etc.) in Zone 17.

In the event the Applicant is a first responder, the Issuer shall ensure that the Applicant's PIV credential has a red line in Zone 12 indicating that the Applicant is a first responder.

The Issuer shall ensure that the Applicant (145b) receives a badge with NC in Zone 4: Clearance Designation, indicating that the individual has no clearance and he/she must have no access to classified information.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request
- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

7.9.4 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

7.10 Final Approval

Once the background investigation has been completed, OPM sends a package containing the results of the investigation to the PSB, with a *Certification of Investigation, Case Closing Transmittal (CCT)* and a Form 79A, *Report of Agency Adjudicative Action*.

The Security Processing Unit analyst will:

1. Stamp the back of the Certificate of Investigation and Case Closing Transmittal (CCT) with the date received.
2. Update the IPSS investigation record to reflect the date received from OPM, the closed investigation date, and the date forwarded for adjudication.
3. Attach the Certificate and Form 79A, and any additional investigation reports (in the order they were received) to the top, right side of the folder
4. Place the folder on the closed initial investigation shelf for adjudication.

The Adjudicator will review the consultant-employee's SF-86 and the background investigation report results in order to make a final determination for a clearance.

<u>If the consultant-employee is approved for clearance</u>:

The Adjudicator will:

1. Sign and date the Certification of Investigation, and stamp the CCT "Reviewed and Approved"; the Certificate of Investigation is retained in the folder, and a copy is sent to HR for the consultant-employee's official personnel file (OPF)
2. Complete the Form 79A with the adjudicative action, sign, and date the form; a copy of the Form 79A is retained in the folder and the original is sent to OPM
3. Update and sign the Form 225, *File Summary Sheet* with the grant date.
4. Update and sign Part IV of the NRC Form 236, including investigative agency and type of investigation; the NRC Form 236 is retained in the folder, and a copy is sent to the Facilities Security Branch Badge Office to initiate the creation of a new badge (Blue for Q clearance; Yellow for L clearance) for the consultant-employee.
5. The Adjudicator will enter favorable adjudication for Applicant in PCI
    - Login to PCI
    - Click "Adjudicate Person" and search the Applicant to be adjudicated
    - Click the Applicant's name to open the Applicant's record
    - Set the NACI status to "Approved"
    - On the Personal tab, click "Card Issuance Approved"
    - Click "Save" and then click "Yes" to confirm adjudication
    - Select the appropriate card profile and click "Accept"

Note: The consultant-employee will receive an e-mail notification when the new badge is ready for pickup at the Badging Office.

The Security Processing Unit analyst will:

1. Update the consultant-employee's clearance record in IPSS to reflect the 145b terminated with a termination date.
2. Create a clearance record with the clearance designated on the NRC Form 236, make the action "active", and add the grant date reflected on the NRC Form 236.
3. File the folder on the "pending" shelf until the consultant employee has attended the mandatory Security Orientation Briefing and signed an SF-312, *Classified Information Nondisclosure Agreement*

7.10.1 Create a record in the PCI system (Final Badge Issuance)

DFS directs the employee to the PSB. The Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data

11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

The consultant-employee must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

7.10.2 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

7.10.3 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.
- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall ensure that the Applicant's PIV credential has "Employee" in Zone 8: Employee Affiliation.

The Issuer shall ensure that the Applicant's PIV credential has their correct office location (i.e. HQ, RI, RII, etc.) in Zone 17.

In the event the Applicant is a first responder, the Issuer shall ensure that the Applicant's PIV credential has a red line in Zone 12 indicating that the Applicant is a first responder.

The Issuer shall ensure that the Applicant's PIV credential has their correct clearance designation (i.e. L, LH, Q) in Zone 4.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request
- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

7.10.4 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

<u>If the consultant-employee is not approved for clearance</u>:

The Adjudicator will:

1. Sign and date the Certification of Investigation, stamp the CCT "Denied", and retain it in the consultant-employee's security folder
2. Sign and date the Form 79A, retain a copy in the consultant-employee's security folder, and send the original to OPM
3. Update and sign the Form 225, *File Summary Sheet*
4. Write a denial memorandum stating that the consultant-employee is not eligible for an access authorization, including a brief summary of the cause
5. Write a letter to the consultant-employee, providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*
6. Deliver the consultant-employee's security folder to the PSB Chief for review and consent to the to the denial recommendation

The Branch Chief will review the consultant-employee's security folder and confirm consent by signing the denial memorandum. The letter to the consultant-employee and the folder will then be forwarded to the Division of Facilities and Security Director for review and concurrence. The file is then forwarded to the Office of Administration Director for signature (as required by 10 CFR 10.22).

The Office of Administration Director reviews the consultant-employee's security folder and signs the letter to the consultant-employee. The security folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the consultant-employee
2. Retain 1 set of copies in the consultant-employee's security folder
3. Send the original denial memorandum to HR
4. Send the original signed letter to the consultant-employee
5. Update the consultant-employee's record in IPSS
6. File the consultant-employee's security folder to the "TERM" shelf

HR will notify the consultant-employee that the clearance has been denied.

The employee will be given appeal rights according to 10 CFR Part 10.

If the situation cannot be resolved and the consultant-employee cannot be granted a clearance, the consultant-employee will be terminated per NRC HR procedures and a Form 136; *Security Termination Statement* must be completed.

7.10.5 Security Orientation Briefing

The PSB Adjudicators conduct a security orientation briefing on Monday, every other week, for newly cleared employees, consultant-employees, and contractors with clearances.

The consultant-employee must attend a security orientation briefing from the PSB and sign an SF-312, *Classified Information Nondisclosure Agreement* in order to receive a new badge indicating their clearance for "need-to-know" access to classified information.

After the consultant-employee has attended a Security Orientation Briefing and signed an SF-312, *Classified Information Nondisclosure Agreement*, a Security Processing Analyst will:

1. Retain the SF-312 in the SF-312 security binder.
2. Send a copy of the NRC Form 236 to the Facilities Security Branch badging office to initiate the creation of a new badge (Blue for Q clearance; Yellow for L clearance) for the consultant-employee

Note: The consultant-employee will receive an e-mail notification when the new badge is ready for pickup at the Badging Office.

8.0 The IT Contractor Process

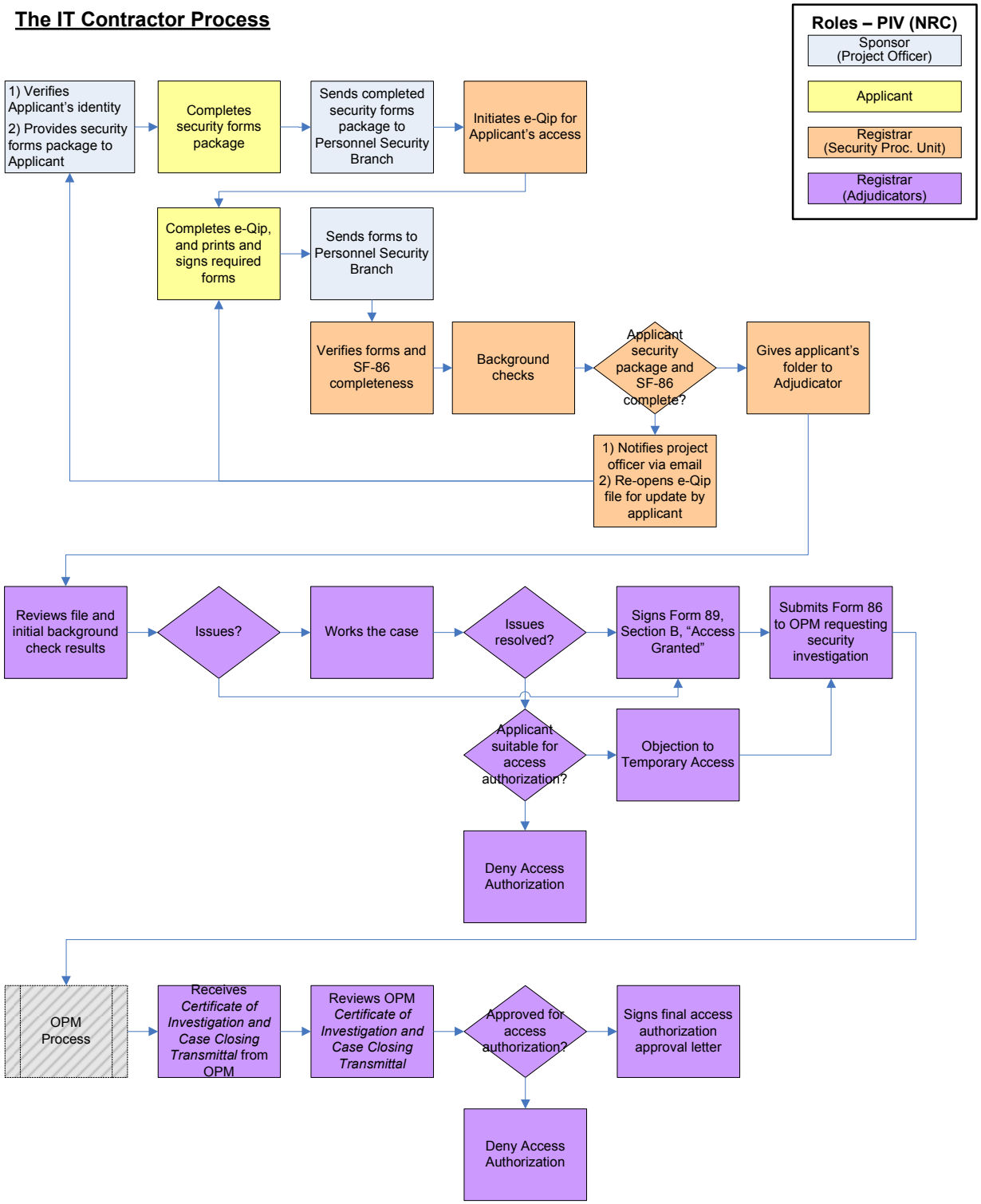
This section describes the requirements and procedures for adjudicating contractors providing information technology services for access authorization. IT Contractors are not allowed access to classified information and therefore do not receive a clearance. However, the process and procedures include a background investigation by OPM to make a determination of eligibility for permanent access authorization.

8.1 Overview

The IT Contractor Process allows for temporary access authorization to be granted, enabling contractors to begin work prior to the completion of a background investigation. Access authorizations for contractors are requested through a memo which is signed by the Applicant's Program Officer. The NRC Project Officer performs the Sponsor role for IT Contractors.

The IT Contractor Process is illustrated on the following page.

The IT Contractor Process



8.2 Request for Access Authorization

Prior to a request for access authorization, a designated security officer of the contractor's employer will assure the Applicant's identity using at least two forms of approved certificates of identity per the I-9 documents list (e.g., Drivers License, Birth Certificate, or Passport) and provide a security forms package.

The security forms package includes the following materials:

- *Request for NRC Access Authorization* form
- *Fair Credit Reporting Act of 1970* form
- NRC Form 89, *Badge Request*
- FD-258, *Fingerprint Cards* (2) for those not enrolled at HQ
- Instructions for completing security forms
- e-QIP Quick Reference Guide

The Applicant will: (a) read, complete, and sign all required forms in the security forms package; (b) obtain fingerprints from an authorized source; and, (c) return completed signed forms and fingerprint cards to the security officer, unless enrollment will occur prior to EOD at headquarters.

The security officer will then forward the contractor's security forms and fingerprint cards to the NRC Project Officer (e.g., the Sponsor).

8.2.1 Sponsor Sends Applicant's forms to the Personnel Security Branch

The NRC Project Officer will:

1. Review the Applicant's security forms package
2. Complete and sign the *Request for NRC Access Authorization* form
3. Complete and sign the NRC Form 89, *Badge Request*
4. Submit the completed security forms package to the PSB

Supplemental material may be sent with the Applicant's security package, as needed. For example: Foreign National Questionnaire, Naturalization Certificate, bankruptcy disposition papers, documentation of paid accounts, etc.

8.2.2 Registrar Initiates e-QIP for the Applicant

A Security Processing Unit analyst will:

1. Login to e-QIP
2. Enter the Applicant's SSN in the "Manage Request" section and select "Initiate Request"
3. In the "User and Request Information" screen, under "Full Name" enter the Applicant last name, first name, and middle name
4. Tab to "Date of Birth" and enter the Applicant's birth date by selecting from the drop down screen for month, day, and year

5. Tab to "Place of Birth" and enter the Applicant's city and state or city and foreign country
6. Tab to "Personal Contact Information" and enter the Applicant's email address
7. Tab to "Form Information" and select the ISP/Form from the drop down menu and tab to "Applicant Group" and select Security from the drop down
8. Scroll down and select 'Submit' to create the record
9. Complete the Agency Usage Block (AUB) using the OPM templates for the investigation type needed
10. E-mail the Applicant that the e-QIP account has been set up

The Applicant will complete, certify, and submit his/her SF-86, *Questionnaire for National Security Positions* via e-QIP, print and sign any required forms, and return completed, signed forms to their employer's security officer.

The security officer will send the forms to the NRC Project Officer.

The NRC Project Officer will review the forms and forward them to the PSB.

8.3 Initial Screening

The Applicant's security forms package undergoes initial screening by a Security Processing Unit analyst.

8.3.1 Registrar Processes the Applicant's forms

The Security Processing Unit analyst will:

1. Date stamp the back of each item in the Applicant's security forms package
2. Verify that all required forms have been received. If any required forms are missing or incomplete, the security forms package is returned to the Project Officer
3. Print a copy of the Applicant's SF-86, *Questionnaire for National Security Positions* from e-QIP
4. Create an NRC Form 225, *File Summary Sheet* from INFORMS
5. Assemble the Applicant's security folder
   a. Use a red folder
   b. Affix a label with the Applicant's SSN and name to the folder tab
   c. Affix a coversheet for Privacy Act Info to the front outer cover of the folder
   d. Arrange forms in the Applicant's security folder as follows:

Left Side, Top to Bottom	***Right Side, Top to Bottom***
NRC Form 225	SF-86 (from e-QIP)
Request for NRC Access Authorization	Fair Credit Reporting Act of 1970
Processing Unit checklist	Supplemental documents

Correspondences	2 FD-258
NRC Form 89	

Supplemental Information

To print the NRC Form 225, File Summary Sheet in INFORMS:

a. Select Master List and select Form 225
b. Enter the applicant's name and DOB
c. Select the type of access authorization to be processed
d. Date: enter the date access authorization was requested
e. Select Investigative Agency to perform the investigation
f. Type the date the Fingerprint Cards were received
g. On the remarks section, type applicant's SSN and place of birth
h. Office Symbol: "HQ"
i. Type Clearance: "None"
j. Action: "IT Level I" or IT Level II"
k. Employer Code: use assigned 5code

8.3.2 Pre-screen the Security Forms Package

The pre-screening process is a series of preliminary checks to verify completeness and accuracy.

The Security Processing Unit analyst will perform the following checks and procedures:

1. Are all required forms in the security package?
2. Are the forms complete?
3. Has the Applicant signed all of the forms?
4. Do the signatures on all the forms match?
5. Is the Applicant using his/her name as it reads on his/her official ID: Birth Certification or Social Security Card?
6. If the Applicant is not enrolled at HQ prior to EOD, ensure that data entered on FD-258, *Fingerprint Cards* matches the Applicant data in the SF-86.
7. Review the Applicant's SF-86 and flag items reflecting derogatory information.
8. Has the Applicant signed the SF-86 signature forms?
9. Has the Applicant signed the Authorization for Release of Medical Information? (It must be signed if the Applicant answered "yes" to question 21 on the SF-86).

If there are any paper forms which are missing a signature, they must be sent back to the Project Officer for the Applicant's signature.

If there is a problem with the Applicant's SF-86, it must be corrected by the Applicant in e-QIP. To release e-QIP back to the Applicant for corrections:

1. Login to e-QIP

2. In the Applicant's record, select review
3. Under the rejection comments section, in the box labeled "Reject To Applicant Comments", provide a detailed record of which sections need corrections and what information is required.
4. Scroll down and select "Reject to Applicant."
5. The Applicant is notified via e-mail to make corrections to his/her SF-86 in e-QIP. The Project Officer is carbon copied (cc:) on this notification for case tracking purposes.

Supplemental Guidance

Security Processing Unit analysts should retain all correspondence (e-mail, mail, or notes/records of telephone conversations) in the applicant's security folder.

Internal (within NRC) requests for information should be sent via e-mail.

Print all e-mail correspondence – both sent and received.

Keep record of all phone calls, including dates and times.

Date stamp any additional documents received and retain them in the applicant's security folder.

8.3.3 Create a Record in the Integrated Personnel Security System (IPSS)

The Security Processing Unit analyst will:

1. Login to IPSS
2. Under "Create a New Person", enter the Applicant's SSN and full name as appears on the SF-86. If there is no middle name, enter "nmn"
3. Select "Create" to begin entering the Applicant's personnel security record. Ensure that the fields in the following sections pertaining to an individual's personnel security record are completed. (See Appendix D for details on the fields in each IPSS section)
   - Personal Data
   - Aliases
   - Employment Data
   - INS Info
   - Documents & Forms
   - Clearances/Access
   - Security checks
   - Investigation Data

8.4 Create a record in the PCI system (prior to EOD)

For those Applicants able to come to HQ for enrollment purposes prior to EOD, the Security Processing Analyst will:

1. Login to PCI

2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

8.5 Suitability Determination

Upon confirmation that the package is complete, the Security Processing Unit analyst will perform preliminary checks that will help determine the Applicant's suitability for access authorization. These preliminary checks are:

- Credit check
- FBI Fingerprint and FBI name checks
- PIPS check, which includes:

  - the SII
  - the CVS
  - the JPAS
- CPCI

See Appendix E for detailed information about PIPS, SII, CVS, JPAS, CPCI.

IPSS is then updated and the Applicant's folder is provided to a Personnel Security Specialist (Adjudicator).

8.5.1 Perform Preliminary Checks

The Security Processing Unit analyst will:

1. Perform preliminary checks that will help determine the Applicant's suitability for access authorization
2. Retain all background check reports in the Applicant's security folder, on the right side, over the FD-258, *Fingerprint Cards*
3. Update the Applicant's Security Checks record in IPSS

When all required pre-screening and checks are complete, the Applicant's security folder should be up-to-date and ready for the Adjudicator to review. The Security Processing Unit analyst will then file the Applicant's security folder on the Adjudicators' shelf, and notify the Personnel Security Specialist (e.g., the Adjudicator) by e-mail.

8.5.1.1 Credit Check

To perform a credit check on the Applicant the Personnel Security Processing Unit analyst will:

1. Open Internet Explorer, and navigate to www.experian.com/esolutions/index.html
2. Login

   Select: **Consumer Credit**

   Access Subcode: Select **TBD3 1487040 Rockville MD**

   Product: **Employment Insight**
3. **Primary Applicant Box:** Enter the Applicant's name, SSN, date of birth, and phone number.
4. **Address Box:** Enter Applicant's current address. Click submit
5. Print the report

8.5.1.2 FBI Fingerprint and Name check

The Security Processing Unit Security Processing Unit analyst will send the Applicant's fingerprints to OPM via PIPS. Results usually come back via PIPS after a few business days.

8.5.1.3 PIPS - SII, CVS, and JPAS checks

The Personnel Security Processing Unit analyst will:

1. Login to PIPS
2. Select #2 CVS Menu
3. Select #1 SII/CVS/JPAS
4. Enter Applicant's SSN and last name and submit
5. A report screen will display Applicant's data. Scroll to the bottom of the page to view further screen options. Screens containing data will be flagged with a "Y".
6. Select the number of the desired screen to view.
7. Print the desired reports and log out of PIPS

8.5.1.4 CPCI (Central Personnel Clearance Index)

The Personnel Security Processing Unit analyst will:

1. Login to the CPCI. Open Internet Explorer and navigate to https://cpci.doe.gov/loginPage.faces
2. Enter either the SSN or name of the Applicant
3. Print the report
4. Log out of the CPCI

8.6 Temporary IT Access Authorization

Upon a favorable suitability determination by the Adjudicator, and concurrence by appropriate management officials, a temporary IT access authorization will be granted.

The PSB notifies the Project Officer and the Facilities Security Branch.

8.6.1 Favorable Eligibility Determination

The Adjudicator reviews the Applicant's security folder to determine eligibility for temporary IT access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the eligibility determination for a temporary IT access authorization is favorable, the following actions are performed:

1. The Adjudicator will:
   (a) Create an approval letter to the NRC Project Officer stating that the Applicant's temporary IT access authorization request has been adjudicated with no issues and is recommended for approval
   (b) Deliver the Applicant's security folder to the PSB Chief for review and consent to the approval recommendation

2. The Branch Chief will review the Applicant's security folder and confirm consent by signing the temporary IT access authorization letter. The folder is returned to the Adjudicator. The Adjudicator will:
   a) Update and sign the NRC Form 89, *Badge Request*
   b) Update the NRC Form 225 with the temporary access authorization approval date
   c) Release the SF-86 in e-QIP to OPM for the background investigation. (See 8.6)
3. The Adjudicator will enter favorable adjudication for Applicant in PCI
   - Login to PCI
   - Click "Adjudicate Person" and search the Applicant to be adjudicated
   - Click the Applicant's name to open the Applicant's record
   - Set the NACI status to "Approved"
   - On the Personal tab, click "Card Issuance Approved"
   - Click "Save" and then click "Yes" to confirm adjudication
   - Select the appropriate card profile and click "Accept"

   The file is then forwarded to the Security Processing Unit.
4. A Security Processing Unit analyst will:
   (a) Copy the signed Temporary Access Approval letter and retain it in the Applicant's security folder
   (b) Send the original signed Temporary Access Approval letter to the Project Officer
   (c) Update the Applicant's Clearances/Accesses record in IPSS with the date the temporary IT access is approved and the Investigation record with the date the investigation is requested and the agency conducting the investigation.
   (d) Copy the signed NRC Form 89 and place the copy in Applicant's folder. The original is held in the Badge Request tray until the Applicant appears for their badge photo process.
   (e) Place the file on the 'Active' shelf.
5. The Project Officer will notify the contractor-applicant's employer that the temporary IT access has been approved and will make arrangements for the contractor's starting date and responsibilities.

8.6.2 Unfavorable Eligibility Determination

The Adjudicator reviews the Applicant's security folder to determine eligibility for a temporary IT access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the eligibility determination for a temporary IT access authorization is unfavorable, the Adjudicator will:

1. Write a denial memorandum stating that the Applicant is not eligible for an access authorization, including a brief summary of the cause
2. write a letter to the Applicant providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*
3. deliver the Applicant's security folder to the PSB Chief for review and consent to the denial recommendation

The Branch Chief will review the Applicant's security folder and confirm consent by signing the denial memorandum. The letter to the Applicant and the folder will then be forwarded to the Division of Facilities Security Director for signature.

The Division of Facilities Security Director reviews the Applicant's security folder and signs the letter to the Applicant. The Applicant's security folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the Applicant
2. Retain 1 set of copies in the Applicant's security folder
3. Send the original denial memo to the NRC Project Officer
4. Send the original signed letter to the Applicant
5. Update the Applicant's record in IPSS
6. File the Applicant's security folder to the "Denial" shelf

8.7 Background Investigation by OPM (if applicable)

The Adjudicator will:

1. Login to e-QIP
2. Double-check the accuracy of the information in the AUB, Part I of the Applicant's SF-86
3. Print a final copy of the Applicant's SF-86 from e-QIP, stamp it with the investigation type and the date requested, and retain it in Applicant's security folder
4. Purge the old copy of the Applicant's SF-86 from the folder.

   Note: Any printed information containing sensitive personal information must be shredded or destroyed according to NRC media destruction procedure.
5. Select "release from agency" (to submit the Applicant's information to OPM for a background investigation)

   Note: The Adjudicator may have previously requested a valid prior investigation from another agency (see Reciprocity procedure.) In this case there will be a note on

the right side of the folder stating that that an OPM background investigation will not be requested.

6. Return the Applicant's security folder to the Security Processing Unit

The Security Processing Unit analyst updates the Applicant's record in IPSS with the current investigation type and date requested from OPM and files the security folder on the "Active" shelf.

8.8 Issuance of Credential (NRC ID Badge)

The IT contractor must report to NRC to be issued a red badge which indicates that he/she must have no access to classified information. The IT contractor will be informed by his/her employer's security officer of the date and time to report to NRC to have a photo taken and when the badge can be picked up. The IT contractor must bring two approved certificates of identity.

8.9 Create a record in the PCI system (if applicable)

NRC Project Officer directs the IT contractors, who were not previously enrolled, to the PSB. The Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant

8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

The IT contractor must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

IT contractors receive a temporary badge until their PIV card is ready for issuance.

8.9.1 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

8.9.2 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.

- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall ensure that the Applicant's PIV credential has "Contractor" in Zone 8: Employee Affiliation.

The Issuer shall ensure that the Applicant's PIV credential has a green line in Zone 15 indicating that the Applicant is a contractor.

The Issuer shall ensure that the Applicant's PIV credential has either "IT-I" or "IT-II" in Zone 17.

The Issuer shall ensure that the Applicant's PIV credential has their correct office location (i.e. HQ, RI, RII, etc.) in Zone 17.

In the event the Applicant is a first responder, the Issuer shall ensure that the Applicant's PIV credential has a red line in Zone 12 indicating that the Applicant is a first responder.

The Issuer shall ensure that the Applicant's PIV credential has NC in Zone 4: Clearance Designation, indicating the Applicant has no clearance.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request
- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

8.9.3 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

8.10 Final Approval

Once the background investigation has been completed, OPM sends a package containing the results of the investigation to the PSB, with a *Certification of Investigation, Case Closing Transmittal*, and a Form 79A, *Report of Agency Adjudicative Action*.

The Security Processing Unit analyst will:

1. Stamp the back of the Certification of Investigation and Case Closing Transmittal (CCT) with the date received,
2. Update the IPSS investigation record to reflect the date received from OPM, the closed investigation date, and the date forwarded for adjudication.

3. Attach the Certificate and Form 79A, and any additional investigation reports (in the order they were received) to the top, right side of the folder
4. Place the folder on the closed IT investigations shelf for adjudication

The Adjudicator will review the IT contractor's SF-86 and the background investigation report results in order to make a final determination of suitability.

<u>If the final determination of suitability is favorable</u>:

The Adjudicator will:

1. Sign and date the Certificate of Investigation, stamp the CCT "Reviewed and Approved"; and retain it in the IT contractor's security folder
2. Complete the Form 79A with the adjudicative action, sign, and date the form; a copy of the Form 79A is retained in the folder and the original is sent to OPM
3. Update and sign the Form 225, *File Summary Sheet*
4. Generate a final IT access authorization approval letter
5. Provide the letter and the IT contractor's security folder to the PSB Chief for review and signature
6. Return the folder to the Security Processing Unit
7. The Adjudicator will enter favorable adjudication for Applicant in PCI
    - Login to PCI
    - Click "Adjudicate Person" and search the Applicant to be adjudicated
    - Click the Applicant's name to open the Applicant's record
    - Set the NACI status to "Approved"
    - On the Personal tab, click "Card Issuance Approved"
    - Click "Save" and then click "Yes" to confirm adjudication
    - Select the appropriate card profile and click "Accept"

The Security Processing Unit analyst will:

1. Update the employee's Access record in IPSS to terminate the IT 'Temp' access record and create an IT 'Final' access record with the approval date.
2. Make copies of the final IT access authorization approval letter and retain one copy in the IT contractor's security folder. Forward a copy to the Facilities Security Branch.
3. Send the original final IT access authorization approval letter to the Project Officer
4. File the folder on the active shelf

8.10.1 Create a record in the PCI system (Final Badge Issuance)

NRC Project Officer directs the IT contractors to the PSB. The Security Processing Analyst will:

1. Login to PCI

2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

The IT contractor must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

IT contractors receive a temporary badge until their PIV card is ready for issuance.

8.10.2 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

8.10.3 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.
- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall ensure that the Applicant's PIV credential has "Contractor" in Zone 8: Employee Affiliation.

The Issuer shall ensure that the Applicant's PIV credential has a green line in Zone 15 indicating that the Applicant is a contractor.

The Issuer shall ensure that the Applicant's PIV credential has either "IT-I" or "IT-II" in Zone 17.

The Issuer shall ensure that the Applicant's PIV credential has their correct office location (i.e. HQ, RI, RII, etc.) in Zone 17.

In the event the Applicant is a first responder, the Issuer shall ensure that the Applicant's PIV credential has a red line in Zone 12 indicating that the Applicant is a first responder.

The Issuer shall ensure that the Applicant's PIV credential has NC in Zone 4: Clearance Designation, indicating the Applicant has no clearance.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request
- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

8.10.4 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

<u>If the final determination of suitability is unfavorable</u>:

The Adjudicator will:

1. Sign and date the Certificate of Investigation, stamp the CCT "Denied"; and retain it in the IT contractor's security folder
2. Complete the Form 79A with the adjudicative action, sign, and date the form; a copy of the Form 79A is retained in the folder and the original is sent to OPM
3. Update and sign the Form 225, *File Summary Sheet*
4. Write a denial memorandum stating that the IT contractor is not eligible for an access authorization, including a brief summary of the cause
5. Write a letter to the IT contractor providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*
6. Deliver the IT contractor's security folder to the PSB Chief for review and consent to the to the denial recommendation

The Branch Chief will review the IT contractor's security folder and confirm consent by signing the denial memorandum. The letter to the IT contractor and the folder will then be forwarded to the Division of Facilities Security Director for signature.

The Division of Facilities Security Director reviews the IT contractor's security folder and signs the letter to the IT contractor. The security folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the IT contractor
2. Retain 1 set of copies in the IT contractor's security folder
3. Send the original denial memorandum to the NRC Project Officer

4. Send the original signed letter to the IT contractor
5. Update the IT contractor's record in IPSS
6. File the IT contractor's security folder to the "Denied" shelf

9.0 The Contractor with Clearance Process

This section describes the requirements and procedures for adjudicating contractors who require "need to know" access to sensitive or classified information for access authorization and/or clearance.

9.1 Overview

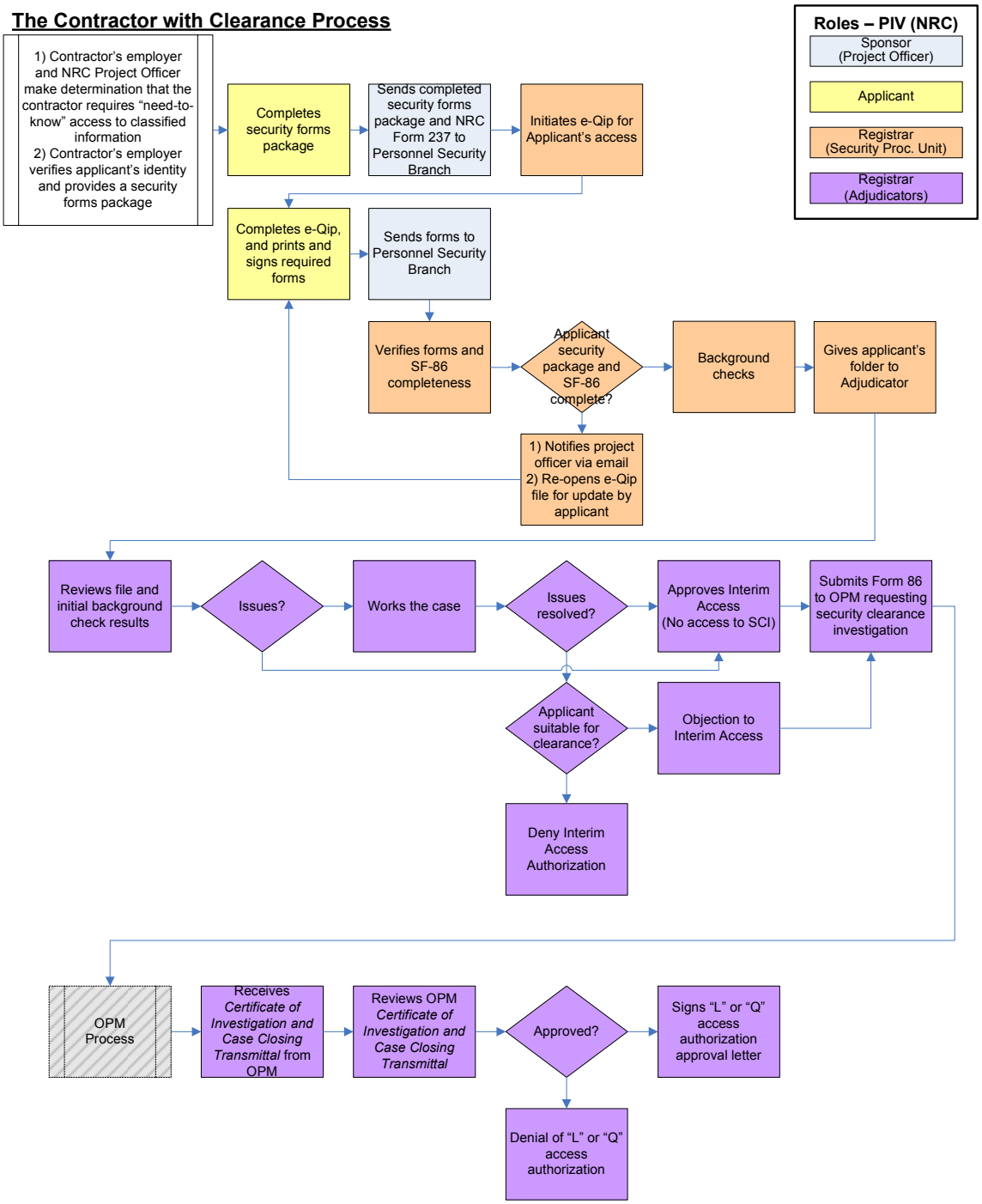
The Contractor with Clearance Process allows for temporary access authorization to be granted, enabling contractors to begin work prior to the completion of a background investigation. Access authorizations for contractors are requested through a memo which is signed by the Applicant's Program Officer. The NRC Project Officer performs the Sponsor role for contractors.

Access authorization and clearance investigations for NRC contractors requiring clearances are requested by the NRC Project Officer using the NRC Form 237, *Request for NRC Access Authorization*

The process begins with the formal request for access authorization and clearance for a contractor Applicant.

The Contractor with Clearance Process is illustrated on the following page.

The Contractor with Clearance Process



9.2 Request for Access Authorization and Clearance

Prior to a request for access authorization, the contractor's employer and the NRC Project Officer will make a determination that the contractor requires "need-to-know" access to classified information.

A designated security officer of the contractor's employer will: (a) assure the Applicant's identity using at least two forms of approved certificates of identity (e.g., Drivers License, Birth Certificate, or Passport) and provide a security forms package.

The security forms package includes the following materials:

- *E-QIP Form for Requesting an NRC Access Authorization*
- NRC Form 237, *Request for Access Authorization*
- *Fair Credit Reporting Act of 1970* form
- NRC Form 89, *Badge Request*
- FD-258, *Fingerprint Cards* (2)
- NRC Form 176, *Security Acknowledgement*
- Instructions for completing security forms
- e-QIP Quick Reference Guide

The Applicant will: (a) read, complete, and sign all required forms in the security forms package; (b) obtain fingerprints from an authorized source; and, (c) return completed signed forms and fingerprint cards to the security officer, unless enrollment will occur prior to EOD at headquarters.

The security officer will then forward the contractor's security forms and fingerprint cards to the NRC Project Officer (e.g., the Sponsor).

9.2.1 Sponsor Sends Applicant's forms to the Personnel Security Branch

The NRC Project Officer will:

1. Review the Applicant's security forms package
2. Complete and sign an NRC Form 237, *Request for Access Authorization*
3. Complete and sign the *Request for NRC Access Authorization*
4. Complete and sign the NRC Form 89, *Badge Request*
5. Submit the completed security forms package to the PSB

Supplemental material may be sent with the Applicant's security package, as needed. For example: Foreign National Questionnaire, Naturalization Certificate, bankruptcy disposition papers, documentation of paid accounts, etc.

9.2.2 Registrar Initiates e-QIP for the Applicant

A Security Processing Unit analyst will:

1. Login to e-QIP
2. Enter the Applicant's SSN in the "Manage Request" section and select "Initiate Request"

3. In the "User and Request Information" screen, under "Full Name" enter the Applicant last name, first name, and middle name
4. Tab to "Date of Birth" and enter the Applicant's birth date by selecting from the drop down screen for month, day, and year
5. Tab to "Place of Birth" and enter the Applicant's city and state or city and foreign country
6. Tab to "Personal Contact Information" and enter the Applicant's email address
7. Tab to "Form Information" and select the ISP/Form from the drop down menu and tab to "Applicant Group" and select Security from the drop down
8. Scroll down and select 'Submit' to create the record
9. Complete the AUB (Agency Usage Block) using the OPM templates for the investigation type needed
10. E-mail Applicant that the e-QIP account has been set up

The Applicant will complete, certify, and submit his/her SF-86, *Questionnaire for National Security Positions* via e-QIP, print and sign any required forms, and return completed, signed forms to their employer's security officer.

The security officer will send the forms to the NRC Project Officer.

The NRC Project Officer will review the forms and forward them to the PSB.

9.3 Initial Screening

The Applicant's security forms package undergoes initial screening by a Security Processing Unit analyst.

9.3.1 Registrar Processes the Applicant's forms

The Security Processing Unit analyst will:

1. Date stamp the back of each item in the Applicant's security forms package
2. Verify that all required forms have been received. If any required forms are missing or incomplete, the security forms package is returned to the Project Officer
3. Print a copy of the Applicant's SF-86, *Questionnaire for National Security Positions* from e-QIP
4. Create an NRC Form 225, *File Summary Sheet* from INFORMS
5. Assemble the Applicant's security folder
   a. Use a yellow folder
   b. Affix a label with the Applicant's SSN and name to the folder tab
   c. Affix a coversheet for Privacy Act Info to the front outer cover of the folder
   d. Arrange forms in the Applicant's security folder as follows:

Left Side, Top to Bottom	***Right Side, Top to Bottom***
NRC Form 225	SF-86 (from e-QIP)
NRC Form 237	Fair Credit Reporting Act
Request for NRC Access Authorization	Supplemental documents
Processing Unit checklist	NRC Form 176
Correspondences	2 FD-258
NRC Form 89	

Supplemental Information

To print the NRC Form 225, File Summary Sheet in INFORMS:

a. Select Master List and select Form 225
b. Enter the applicant's name and DOB
c. Select the type of clearance to be processed
d. Date: enter the date clearance was requested
e. Select Investigative Agency to perform the investigation
f. Type the date the Fingerprint Cards were received
g. On the remarks section, type applicant's SSN and place of birth
h. Office Symbol: "HQ"
i. Type Clearance: "Q", "LH", or "L"
j. Action: "Grant"
k. Employer Code: use assigned 5code

9.3.2 Pre-screen the Security Forms Package

The pre-screening process is a series of preliminary checks to verify completeness and accuracy.

The Security Processing Unit analyst will perform the following checks and procedures:

1. Are all required forms in the security package?
2. Are the forms complete?
3. Has the Applicant signed all of the forms?
4. Do the signatures on all the forms match?
5. Is the Applicant using his/her name as it reads on his/her official ID: Birth Certificate or Social Security Card?
6. If the Applicant is not enrolled at HQ prior to EOD, ensure that data entered on FD-258, *Fingerprint Cards* matches the Applicant data in the SF-86.
7. Review the Applicant's SF-86 and flag items reflecting derogatory information.
8. Has the Applicant signed the SF-86 signature forms?
9. Has the Applicant signed the Authorization for Release of Medical Information? (It must be signed if the Applicant answered "yes" to question 21 on the SF-86).

If there are any paper forms which are missing a signature, they must be sent back to the Project Officer for the Applicant's signature.

If there is a problem with the Applicant's SF-86, it must be corrected by the Applicant in e-QIP. To release e-QIP back to the Applicant for corrections:

1. Login to e-QIP
2. In the Applicant's record, select review
3. Under the rejection comments section, in the box labeled "Reject To Applicant Comments", provide a detailed record of which sections need corrections and what information is required.
4. Scroll down and select "Reject to Applicant"
5. The Applicant is notified via e-mail to make corrections to his/her SF-86 in e-QIP. The Project Officer is carbon copied (cc:) on this notification for case tracking purposes.

Supplemental Guidance

Security Processing Unit analysts should retain all correspondence (e-mail, mail, or notes/records of telephone conversations) in the applicant's security folder.

Internal (within NRC) requests for information should be sent via e-mail.

Print all e-mail correspondence – both sent and received.

Keep record of all phone calls, including dates and times.

Date stamp any additional documents received and retain them in the applicant's security folder.

9.3.3 Create a Record in the Integrated Personnel Security System (IPSS)

The Security Processing Unit analyst will:

1. Login to IPSS
2. Under "Create a New Person", enter the Applicant's SSN and full name as appears on the SF-86. If there is no middle name, enter "nmn".
3. Select "Create" to begin entering the Applicant's personnel security record. Ensure that the fields in the following sections pertaining to an individual's personnel security record are completed. (See Appendix D for details on the fields in each IPSS section.)
   - Personal Data
   - Aliases
   - Employment Data
   - INS Info
   - Documents & Forms
   - Clearances/Access
   - Security checks
   - Investigation Data

9.4 Create a record in the PCI system (prior to EOD)

For those Applicants able to come to HQ for enrollment purposes prior to EOD, the Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

9.5 Perform Pre-Employment Checks

Upon confirmation that the package is complete, the Security Processing Unit analyst will perform preliminary checks that will help determine the Applicant's suitability for access authorization. These preliminary checks are:

- Credit check
- FBI Fingerprint and FBI name checks
- PIPS check, which includes:
  - the SII
  - the CVS
  - the JPAS
- CPCI

See Appendix E for detailed information about PIPS, SII, CVS, JPAS, CPCI.

IPSS is then updated and the Applicant's folder is provided to a Personnel Security Specialist (Adjudicator).

9.5.1 Perform Preliminary Checks

The Security Processing Unit analyst will:

1. Perform preliminary checks that will help determine the Applicant's suitability for access authorization
2. retain all background check reports in the Applicant's security folder, on the right side, between the Fair Credit Reporting Act and the FD-258, *Fingerprint Cards*
3. Update the Applicant's Security Checks record in IPSS

When all required pre-screening and checks are complete, the Applicant's security folder should be up-to-date and ready for the Adjudicator to review. The Security Processing Unit analyst will then file the Applicant's security folder on the Adjudicators' shelf, and notify the Personnel Security Specialist (e.g., the Adjudicator) by e-mail.

9.5.1.1 Credit Check

To perform a credit check on the Applicant, the Personnel Security Processing Unit analyst will:

1. Open Internet Explorer, and navigate to www.experian.com/esolutions/index.html
2. Login

   Select: **Consumer Credit**

   Access Subcode: Select **TBD3 1487040 Rockville MD**

   Product: **Employment Insight**
3. **Primary Applicant Box:** Enter the Applicant's name, SSN, date of birth, and phone number.
4. **Address Box:** Enter Applicant's current address. Click Submit

5. Print the report

9.5.1.2 FBI Fingerprint and Name check

The Security Processing Unit analyst will scan the fingerprint card and send the file to OPM via PIPS. Results usually come back via PIPS after a few business days.

9.5.1.3 PIPS - SII, CVS, and JPAS checks

The Personnel Security Processing Unit analyst will:

1. Login to PIPS
2. Select #2 CVS Menu
3. Select #1 SII/CVS/JPAS
4. A report screen will display Applicant's data. Scroll to the bottom of the page to view further screen options. Screens with data will be flagged with a "Y".
5. Select the number of the desired screen to view.
6. Print the desired reports and log out of PIPS

9.5.1.4 CPCI (Central Personnel Clearance Index)

The Personnel Security Processing Unit analyst will:

1. Login to the CPCI. Open Internet Explorer and navigate to https://cpci.doe.gov/loginPage.faces
2. Enter either the SSN or name of the Applicant
3. Print the report
4. Log out of the CPCI

9.6 Temporary Access Authorization

Upon a favorable suitability determination by the Adjudicator, and concurrence by appropriate management officials, a temporary access authorization will be granted.

The PSB notifies the Project Officer and the Facilities Security Branch.

9.6.1 Favorable Eligibility Determination

The Adjudicator reviews the Applicant's security folder to determine eligibility for a temporary access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the eligibility determination for a temporary access authorization is favorable, the following actions are performed:

1. The Adjudicator will:
   (a) Create an approval letter to the NRC Project Officer stating that the Applicant's temporary access authorization request has been adjudicated with no issues and is recommended for approval. Contractors' clearance requests are given temporary

building access until the background investigation is completed, adjudicated, and the security clearance is granted.

(b) Deliver the Applicant's security folder to the PSB Chief for review and consent to the approval recommendation

2. The Branch Chief will review the Applicant's security folder and confirm consent by signing the temporary building access approval letter. The folder is returned to the Adjudicator. The Adjudicator will:

    a) Update and sign the NRC Form 89, Badge Request

    b) Update the NRC Form 225, File Summary, with the temporary access authorization approval date

    c) Release the SF-86 in e-QIP to OPM for the background investigation. (See 9.6)

   The file is then forwarded to the Security Processing Unit.

3. A Security Processing Unit analyst will:

   (a) Copy the signed Temporary Access Approval letter and retain it in the Applicant's security folder

   (b) Send the original signed Temporary Access Approval letter to the Project Officer

   (c) Update the Applicant's Clearances/Accesses record in IPSS with the date the temporary access is approved and the Investigations record with the date the investigation is requested and the agency conducting the investigation.

   (d) Copy the signed NRC Form 89 and place a copy in the Applicant's folder. The original is held in the Badge Request tray until the Applicant appears for their badge photo process.

   (e) Place the file on the "Active" shelf.

4. The Project Officer will notify the Applicant's employer that the temporary access has been approved and will make arrangements for the contractor's starting date and responsibilities.

9.6.2 Unfavorable Eligibility Determination

The Adjudicator reviews the Applicant's security folder to determine eligibility for temporary access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the eligibility determination for a temporary access authorization is unfavorable, the Adjudicator will:

1. Write a denial memorandum stating that the Applicant is not eligible for an access authorization, including a brief summary of the cause

2. Write a letter to the Applicant, providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*
3. Deliver the Applicant's security folder to the PSB Chief for review and consent to the to the denial recommendation

The Branch Chief will review the Applicant's security folder and confirm consent by signing the denial memorandum. The letter to the Applicant and the folder will then be forwarded to the Division of Facilities Security Director for signature.

The Division of Facilities Security Director reviews the Applicant's security folder and signs the letter to the Applicant. The Applicant's security folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the Applicant
2. Retain 1 set of copies in the Applicant's security folder
3. Send the original denial memorandum to the NRC Project Officer
4. Send the original signed letter to the Applicant
5. Update the Applicant's record in IPSS
6. File the Applicant's security folder to the "Denied" shelf

9.7 Background Investigation by OPM (if applicable)

The Adjudicator will:

1. Login to e-QIP
2. Double-check the accuracy of the information in the AUB, Part I of the Applicant's SF-86
3. Print a final copy of the Applicant's SF-86 from e-QIP, stamp it with the investigation type and the date requested, and retain it in Applicant's security folder
4. Purge the old copy of the Applicant's SF-86 from the folder.

   Note: Any printed information containing sensitive personal information must be shredded or destroyed according to NRC media destruction procedure.
5. Select "release from agency" (to submit the Applicant's information to OPM for a background investigation).

   Note: The Adjudicator may have previously requested a valid prior investigation from another agency (see Reciprocity procedure.) In this case there will be a note on the right side of the folder stating that that an OPM background investigation will not be requested.
6. Return the Applicant's security folder to the Security Processing Unit

The Security Processing Unit analyst updates the Applicant's record in IPSS with the current investigation type and date of request and files the security folder.

9.8 Issuance of Credential (NRC ID Badge)

The contractor must report to NRC to be issued a red badge which indicates that he/she must have no access to classified information. The contractor will be informed by his/her employer's security officer of the date and time to report to NRC to have a photo taken and when the badge can be picked up. The contractor must bring two approved certificates of identity.

9.8.1 Create a record in the PCI system (if applicable)

NRC Project Officer directs the new contractors, who were not previously enrolled, to the PSB. The Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data

11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

The contractors must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

Contractors receive a temporary badge until their PIV card is ready for issuance.

9.8.2 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

9.8.3 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.
- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.

- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall ensure that the Applicant's PIV credential has "Contractor" in Zone 8: Employee Affiliation.

The Issuer shall ensure that the Applicant's PIV credential has a green line in Zone 15 indicating that the Applicant is a contractor.

The Issuer shall ensure that the Applicant's PIV credential has their correct office location (i.e. HQ, RI, RII, etc.) in Zone 17.

In the event the Applicant is a first responder, the Issuer shall ensure that the Applicant's PIV credential has a red line in Zone 12 indicating that the Applicant is a first responder.

The Issuer shall ensure that the Applicant's PIV credential has their correct clearance designation (i.e. NC, L, LH, Q) in Zone 4.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request
- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

9.8.4 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

9.9 Final Approval

Once the background investigation has been completed, OPM sends a package containing the results of the investigation to the PSB, with a completed *Certification of Investigation, Case Closing Transmittal* and a Form 79A, *Report of Agency Adjudicative Action*.

The Security Processing Unit analyst will:

1. Stamp the back of the Certification of Investigation and Case Closing Transmittal (CCT) with the date received,
2. Update the IPSS investigation record to reflect the date received from OPM, the closed investigation date, and the date forwarded for adjudication.
3. Attach the Certificate and Form 79A, and any additional investigation reports (in the order they were received) to the top, right side of the folder
4. Place the folder on the closed Contractor w/ Clearance shelf for adjudication.

The Adjudicator will review the contractor's SF-86 and the background investigation report results in order to make a final determination of suitability.

If the contractor is approved for clearance:

The Adjudicator will:

1. Sign and date the Certificate of Investigation, stamp the CCT "Reviewed and Approved"; and retain it in the contractor's security folder
2. Complete the Form 79A with the adjudicative action, sign, and date the form; a copy of the Form 79A is retained in the folder and the original is sent to OPM
3. Update and sign the Form 225, *File Summary Sheet*
4. Generate a clearance approval letter.
5. Provide the letter and the contractor's security folder to the PSB Chief for review and signature
6. Return the folder to the Security Processing Unit
7. The Adjudicator will enter favorable adjudication for Applicant in PCI
    - Login to PCI
    - Click "Adjudicate Person" and search the Applicant to be adjudicated
    - Click the Applicant's name to open the Applicant's record
    - Set the NACI status to "Approved"
    - On the Personal tab, click "Card Issuance Approved"
    - Click "Save" and then click "Yes" to confirm adjudication
    - Select the appropriate card profile and click "Accept"

The Security Processing Unit analyst will:

1. Update the employee's clearance record in IPSS to reflect the temporary access authorization as terminated. Create a final access authorization record reflecting "active" with the approval date.
2. Make copies of the final access authorization approval letter and a copy in the contractor's security folder
3. Send the final access authorization approval letter to the Project Officer. Provide a copy to the Facilities Security Branch.
4. File the folder on the active shelf

9.9.1 Create a record in the PCI system (Final Badge Issuance)

NRC Project Officer directs the new contractors, who were not previously enrolled, to the PSB. The Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"

3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

The contractors must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

Contractors receive a temporary badge until their PIV card is ready for issuance.

9.9.2 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

9.9.3 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.
- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall ensure that the Applicant's PIV credential has "Contractor" in Zone 8: Employee Affiliation.

The Issuer shall ensure that the Applicant's PIV credential has a green line in Zone 15 indicating that the Applicant is a contractor.

The Issuer shall ensure that the Applicant's PIV credential has their correct office location (i.e. HQ, RI, RII, etc.) in Zone 17.

In the event the Applicant is a first responder, the Issuer shall ensure that the Applicant's PIV credential has a red line in Zone 12 indicating that the Applicant is a first responder.

The Issuer shall ensure that the Applicant's PIV credential has their correct clearance designation (i.e. NC, L, LH, Q) in Zone 4.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request

- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

9.9.4 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

<u>If the contractor is not approved for clearance</u>:

The Adjudicator will:

1. Sign and date the Certificate of Investigation, stamp the CCT "Denied"; and retain it in the contractor's security folder
2. Complete the Form 79A with the adjudicative action, sign, and date the form; a copy of the Form 79A is retained in the folder and the original is sent to OPM
3. Update and sign the Form 225, *File Summary Sheet*
4. Write a denial memorandum stating that the contractor is not eligible for an access authorization, including a brief summary of the cause
5. Write a letter to the contractor, providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*
6. Deliver the contractor's security folder to the PSB Chief for review and consent to the to the denial recommendation

The Branch Chief will review the contractor's security folder and confirm consent by signing the denial memorandum. The letter to the Applicant and the folder will then be forwarded to the Division of Facilities and Security Director for review and concurrence. The file is then forwarded to the Office of Administration Director for signature (as required by 10 CFR 10.22).

The Office of Administration Director reviews the contractor's security folder and signs the letter to the contractor. The security folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the contractor
2. Retain 1 set of copies in the contractor's security folder
3. Send the original denial memorandum to the NRC Project Officer
4. Send the original signed letter to the contractor
5. Update the contractor's record in IPSS

6. File the contractor's security folder to the "Denied" shelf

9.9.5 Security Orientation Briefing

The PSB Adjudicators conduct a security orientation briefing on Monday, every other week, for newly cleared employees, consultant-employees, and contractors with clearances.

The contractor must attend a security orientation briefing from the PSB and sign an SF-312, *Classified Information Nondisclosure Agreement* in order to receive a new badge indicating his/her clearance for "need-to-know" access to classified information.

A Security Processing Unit analyst will:

1. Retain the SF-312 in the SF-312 security binder.
2. Send a copy of the clearance approval letter to the Facilities Security Branch Badging office to initiate the creation of a new badge (Blue for Q clearance; Yellow for L clearance) for the contractor

Note: The contractor will receive an e-mail notification when the new badge is ready for pickup at the Badging Office.

10.0 The Building Access Process

This section describes the requirements and procedures for adjudicating contractors who require only building access to NRC facilities. An NRC sponsoring office decides whether performance under an NRC contract, purchase order, or similar agreement will involve unescorted building access. The designated point of contact for the NRC sponsoring office is typically a Project Officer who performs the role of Sponsor for the access authorization procedure.

10.1 Overview

The Building Access Process allows a waiver of the pre-appointment investigation enabling contractors to begin work prior to the completion of a background investigation. Access authorizations for contractors are requested through a memo, which is signed by the Applicant's Program Officer. The NRC Project Officer performs the Sponsor role for contractors requiring building access to NRC facilities.

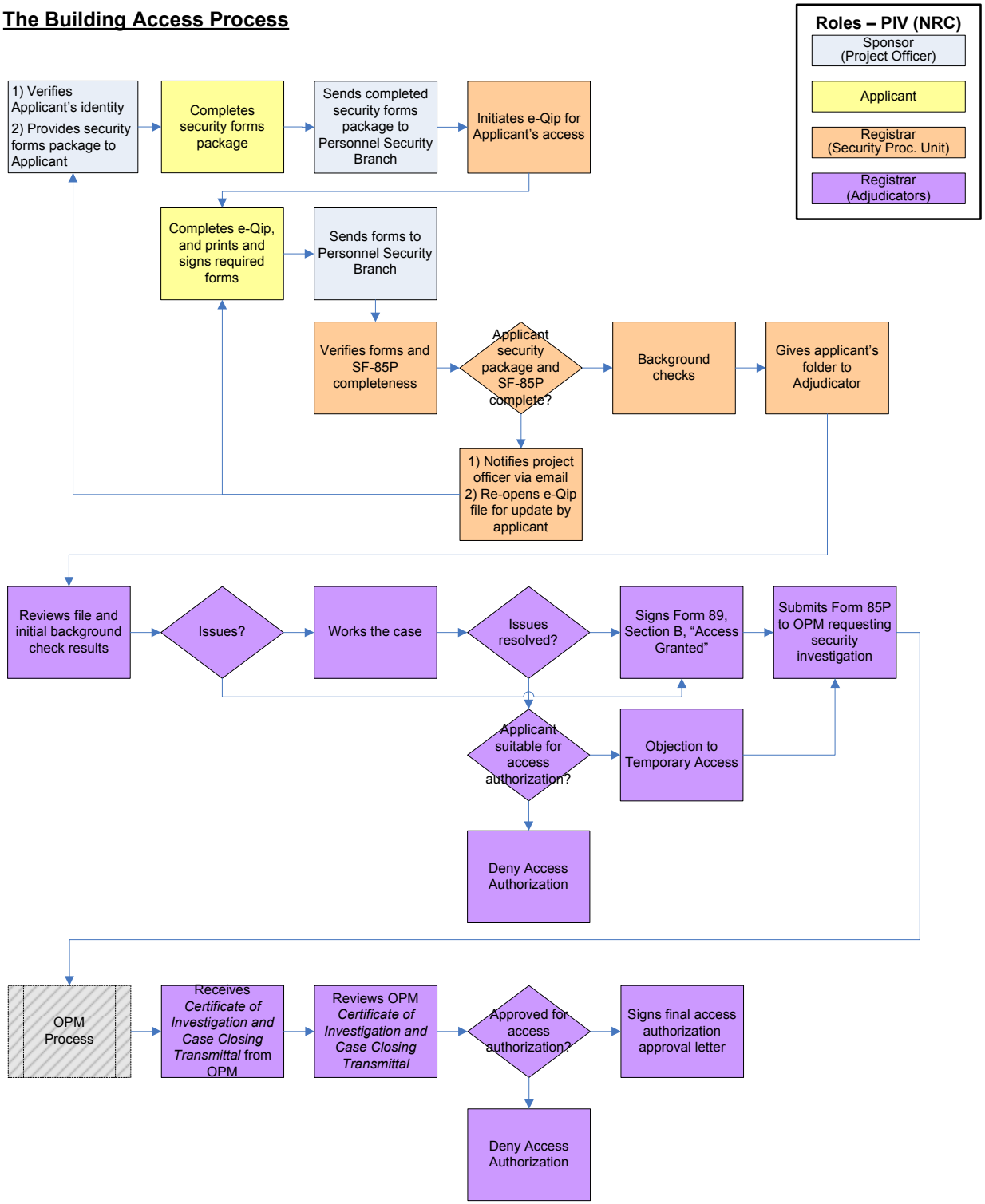
A Contractor must not be provided unescorted access to NRC facilities until he or she is approved for interim access.

All Contractors requiring building access to NRC facilities require a National Agency Check with Inquiries (NACI) by the OPM.

The process begins with the formal request for access authorization for an Applicant.

The Contractors requiring Building Access to NRC facilities process is illustrated on the following page.

The Building Access Process



10.2 Request for Access Authorization

Prior to a request for access authorization, a designated security officer of the contractor's employer will: (a) assure the Applicant's identity using at least two forms of approved certificates of identity (e.g., Drivers License, Birth Certificate, or Passport) and provide a security forms package.

The security forms package includes the following materials:

- *Request for NRC Access Authorization* form
- *Fair Credit Reporting Act of 1970* form
- NRC Form 89, *Badge Request*
- FD-258, *Fingerprint Cards* (2)
- Instructions for completing security forms
- e-QIP Quick Reference Guide

The Applicant will: (a) read, complete, and sign all required forms in the security forms package; (b) obtain fingerprints from an authorized source; and, (c) return completed, signed forms and fingerprint cards to the security officer.

The security officer will then forward the contractor's resume, security forms and fingerprint cards to the NRC Project Officer (e.g., the Sponsor).

10.2.1 Sponsor Sends Applicant's forms to the Personnel Security Branch

The NRC Project Officer will:

1. Review the Applicant's security forms package
2. Complete and sign the *Request for NRC Access Authorization* (not the NRC Form 237)
3. Complete and sign the NRC Form 89, *Badge Request*
4. Submit the completed security forms package to the PSB

Supplemental material may be sent with the Applicant's security package, as needed. For example: Foreign National Questionnaire, Naturalization Certificate, bankruptcy disposition papers, documentation of paid accounts, etc.

10.2.2 Registrar Initiates e-QIP for the Applicant

A Security Processing Unit analyst will:

1. Login to e-QIP
2. Enter the Applicant's SSN in the "Manage Request" section and select "Initiate Request"
3. In the "User and Request Information" screen, under "Full Name" enter the Applicant last name, first name, and middle name
4. Tab to "Date of Birth" and enter the Applicant's birth date by selecting from the drop down screen for month, day, year

5. Tab to "Place of Birth" and enter the Applicant's city and state or city and foreign country
6. Tab to "Personal Contact Information" and enter the Applicant's email address
7. Tab to "Form Information" and select the ISP/Form from the drop down menu and tab to "Applicant Group" and select Security from the drop down
8. Scroll down and select 'Submit' to create the record
9. Complete the AUB using the OPM templates for the investigation type needed (NACI for building access; CNACI for day care)
10. E-mail the Applicant that e-QIP account has been set up

The Applicant will complete, certify, and submit his/her SF-85P, *Questionnaire for Public Trust Positions* via e-QIP, print and sign any required forms, and return completed, signed forms to their employer's security officer.

The security officer will send the forms to the NRC Project Officer.

The NRC Project Officer will review the forms and forward them to the PSB.

10.3 Initial Screening

The Applicant's security forms package undergoes initial screening by a Security Processing Unit analyst.

10.3.1 Registrar Processes the Applicant's forms

The Security Processing Unit analyst will:

1. Date stamp the back of each item in the Applicant's security forms package.
2. Verify that all required forms have been received. If any required forms are missing or incomplete, the security forms package is returned to the Project Officer.
3. Print a copy of the Applicant's SF-85P, *Questionnaire for Public Trust Positions* from e-QIP
4. Create an NRC Form 225, *File Summary Sheet* from INFORMS.
5. Assemble the Applicant's security folder
   a. Use a blue folder
   b. Affix a label with the Applicant's SSN and name to the folder tab
   c. Affix a coversheet for Privacy Act Info to the front outer cover of the folder
   d. Arrange forms in the Applicant's security folder as follows:

Left Side, Top to Bottom	***Right Side, Top to Bottom***
NRC Form 225	SF-85P (from e-QIP)
Request for NRC Access Authorization	Fair Credit Reporting Act
Processing Unit checklist	Supplemental documents

Correspondences	2 FD-258
NRC Form 89	

Supplemental Information

To print the NRC Form 225, File Summary Sheet in INFORMS:

l. Select Master List and select Form 225
m. Enter the applicant's name and DOB
n. Select the type of clearance to be processed
o. Date: enter the date clearance was requested
p. Select Investigative Agency to perform the investigation
q. Type the date the Fingerprint Cards were received
r. On the remarks section, type applicant's SSN and place of birth
s. Office Symbol: "HQ"
t. Type Clearance: "None"
u. Action: "Building Access"
v. Employer Code: use assigned 5code

10.3.2 Pre-screen the Security Forms Package

The pre-screening process is a series of preliminary checks to verify completeness and accuracy.

The Security Processing Unit analyst will perform the following checks and procedures:

1. Are all required forms in the security package?
2. Are the forms complete?
3. Has the Applicant signed all of the forms?
4. Do the signatures on all the forms match?
5. Is the Applicant using his/her name as it reads in his/her official ID: Birth Certificate or Social Security Card?
6. Ensure that data entered on FD-258, *Fingerprint Cards* matches the Applicant data in the SF-85P.
7. Review the Applicant's SF-85P and flag items reflecting derogatory information.
8. Has the Applicant signed the SF-85P signature forms?

If there are any paper forms which are missing a signature, they must be sent back to the Project Officer for the Applicant's signature.

If there is a problem with the Applicant's SF-85P, it must be corrected by the Applicant in e-QIP. To release e-QIP back to the Applicant for corrections:

1. Login to e-QIP
2. In the Applicant's record, select review

3. Under the rejection comments section, in the box labeled "Reject To Applicant Comments", provide a detailed record of which sections need corrections and what information is required.
4. Scroll down and select "Reject to Applicant"
5. The Applicant is notified via e-mail to make corrections to his/her SF-85P in e-QIP.

Supplemental Guidance

Security Processing Unit analysts should retain all correspondence (e-mail, mail, or notes/records of telephone conversations) in the applicant's security folder.

Internal (within NRC) requests for information should be sent via e-mail.

Print all e-mail correspondence – both sent and received.

Keep record of all phone calls, including dates and times.

Date stamp any additional documents received and retain them in the applicant's security folder.

10.3.3 Create a Record in the Integrated Personnel Security System (IPSS)

The Security Processing Unit analyst will:

1. Login to IPSS
2. Under "Create a New Person", enter the Applicant's SSN and full name as appears on the SF-85P. If there is no middle name, enter "nmn"
3. Select "Create" to begin entering the Applicant's personnel security record. Ensure that the fields in the following sections pertaining to an individual's personnel security record are completed. (See Appendix D for details on the fields in each IPSS section)
   - Personal Data
   - Aliases
   - Employment Data
   - INS Info
   - Documents & Forms
   - Clearances/Access
   - Security checks
   - Investigation Data

10.4 Create a record in the PCI system (prior to EOD)

For those Applicants able to come to HQ for enrollment purposes prior to EOD, the Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields

- First Name
- Middle Name (if applicable)
- Last Name
- Date of Birth
- Agency
- E-mail
- Agency Clearance
- Contractor Clearance (if applicable)
- Location
- Social Security Number

4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

10.5 Perform Pre-Employment Checks

Upon confirmation that the package is complete, the Security Processing Unit analyst will perform preliminary checks that will help determine the Applicant's suitability for access authorization. These preliminary checks are:

- Credit check
- FBI Fingerprint and FBI Name checks
- PIPS check, which includes:
  - the SII
  - the CVS
  - the JPAS

- CPCI

See Appendix E for detailed information about PIPS, SII, CVS, JPAS, CPCI.

IPSS is then updated and the Applicant's folder is provided to a personnel security specialist (Adjudicator).

10.5.1 Perform Preliminary Checks

The Security Processing Unit analyst will:

1. Perform preliminary checks that will help determine the Applicant's suitability for access authorization
2. Retain all background check reports in the Applicant's security folder, on the right side, between the Fair Credit Reporting Act and the FD-258, *Fingerprint Cards*
3. Update the Applicant's Security Checks record in IPSS

When all required pre-screening and checks are complete, the Applicant's security folder should be up-to-date and ready for the Adjudicator to review. The Security Processing Unit analyst will then file the Applicant's security folder on the Adjudicators' shelf, and notify the Personnel Security Specialist (e.g., the Adjudicator) by e-mail.

10.5.1.1 Credit Check

To perform a credit check on the Applicant the Personnel Security Processing Unit analyst will:

1. Open Internet Explorer, and navigate to www.experian.com/esolutions.index.html
2. Login

   Select: **Consumer Credit**

   Access Subcode: **TBD3 1487040 Rockville MD**

   Product: **Employer Insight**
3. **Primary Applicant Box:** Enter the Applicant's name, SSN, date of birth, and phone number.
4. **Address Box:** Enter Applicant's current address. Click Submit
5. Print the report

10.5.1.2 FBI Fingerprint and Name check

The Security Processing Unit analyst will scan the fingerprint card and send the file to OPM via PIPS. Results usually come back via PIPS after a few business days.

10.5.1.3 PIPS - SII, CVS, and JPAS checks

The Personnel Security Processing Unit analyst will:

1. Login to PIPS
2. Select #2 CVS Menu

3. Select #1 SII/CVS/JPAS
4. Enter Applicant's SSN and last name and submit
5. A report screen will display Applicant's data. Scroll to the bottom of the page to view further screen options. Screens containing data will be flagged with a "Y".
6. Select the number of the desired screen to view.
7. Print the report and log out of PIPS

10.5.1.4 CPCI (Central Personnel Clearance Index)

The Personnel Security Processing Unit analyst will:

1. Login to the CPCI. Open Internet Explorer and navigate to: https://cpci.doe.gov/loginPage.faces
2. Enter either the SSN or name of the Applicant
3. Print the report
4. Log out of the CPCI

10.6 Interim Access Authorization

Upon a favorable suitability determination by the Adjudicator, and concurrence by appropriate management officials, a temporary access authorization will be granted.

The PSB notifies the Project Officer and the Facilities Security Branch.

10.6.1 Favorable Eligibility Determination

The Adjudicator reviews the Applicant's security folder to determine eligibility for a temporary access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the eligibility determination for an interim access authorization is favorable, the following actions are performed:

1. The Adjudicator will:
   (a) Create an access authorization approval letter to the NRC Project Officer stating that the Applicant's temporary access authorization request has been adjudicated with no issues and is recommended for approval
   (b) Deliver the Applicant's security folder to the PSB Chief for review and consent to the approval recommendation
2. The Branch Chief will review the Applicant's security folder and confirm consent by signing the access authorization approval letter. The folder is returned to the Adjudicator. The Adjudicator will:
   a) Update and sign the NRC Form 89, *Badge Request*
   b) Update the NRC Form 225, *File Summary,* with the interim access authorization approval date

c) Release the SF-85P in e-QIP to OPM for the background investigation (See 10.6)

The file is then forwarded to the Security Processing Unit.

3. The Adjudicator will enter favorable adjudication for Applicant in PCI
   - Login to PCI
   - Click "Adjudicate Person" and search the Applicant to be adjudicated
   - Click the Applicant's name to open the Applicant's record
   - Set the NACI status to "Approved"
   - On the Personal tab, click "Card Issuance Approved"
   - Click "Save" and then click "Yes" to confirm adjudication
   - Select the appropriate card profile and click "Accept"
4. A Security Processing Unit analyst will:
   (a) Copy the signed Interim Access Approval letter and retain it in the Applicant's security folder
   (b) Send the original signed interim access approval letter to the Project Officer
   (c) Update the Applicant's Clearances/Accesses record in IPSS with the date the interim access was approved and the Investigation record with the date the investigation was requested and the agency conducting the investigation.
   (d) Copy the signed NRC Form 89 and place a copy in the Applicant's folder. The original is held in the Badge Request tray until the Applicant appears for their photo badge process.
   (e) Place the file on the 'Active' shelf.
5. The Project Officer will notify the Applicant's employer that the interim access has been approved and will make arrangements for the contractor's starting date and responsibilities.

10.6.2 Unfavorable Eligibility Determination

The Adjudicator reviews the Applicant's security folder to determine eligibility for temporary access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the eligibility determination for a temporary access authorization is unfavorable, the Adjudicator will:

1. Write a denial memorandum stating that the Applicant is not eligible for an access authorization, including a brief summary of the cause.
2. Write a letter to the Applicant, providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*.

3. Deliver the Applicant's security folder to the PSB Chief for review and consent to the to the denial recommendation

The Branch Chief will review the Applicant's security folder and confirm consent by signing the denial memorandum. The letter to the Applicant and the folder will then be forwarded to the Division of Facilities Security Director for signature.

The Division of Facilities Security Director reviews the Applicant's security folder and signs the letter to the Applicant. The Applicant's security folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the Applicant
2. Retain 1 set of copies in the Applicant's security folder
3. Send the original denial memorandum to the NRC Project Officer
4. Send the original signed letter to the Applicant
5. Update the Applicant's record in IPSS
6. File the Applicant's security folder to the "Denied" shelf

10.7 Background Investigation by OPM (if applicable)

The Adjudicator will:

1. Login to e-QIP
2. Double-check the accuracy of the information in the AUB, Part I of the Applicant's SF-85P
3. Print a final copy of the Applicant's SF-85P from e-QIP, stamp it with the investigation type and the date requested, and retain it in Applicant's security folder
4. Purge the old copy of the Applicant's SF-85P from the folder.

   Note: Any printed information containing sensitive personal information must be shredded or destroyed according to NRC media destruction procedure.
5. Select "release from agency" (to submit the Applicant's information to OPM for a background investigation)

   Note: The Adjudicator may have previously requested a valid prior investigation from another agency (see Reciprocity procedure.) In this case there will be a note on the right side of the folder stating that that an OPM background investigation will not be requested.
6. Return the Applicant's security folder to the Security Processing Unit

The Security Processing Unit analyst updates the Applicant's record in IPSS with the current investigation type and date, and files the security folder.

10.8 Issuance of Credential (NRC ID Badge)

The contractor must report to NRC to be issued a red badge which indicates that he/she must have no access to classified information. The contractor will be informed by his/her employer's security officer of the date and time to report to NRC for a photo and when the badge can be picked up. The contractor must bring two approved certificates of identity.

10.8.1 Create a record in the PCI system (if applicable)

NRC Project Officer directs the new contractors, who were not previously enrolled, to the PSB. The Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents

13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

The contractors must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

Contractors receive a temporary badge until their PIV card is ready for issuance.

10.8.2 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

10.8.3 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.
- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall ensure that the Applicant's PIV credential has "Contractor" in Zone 8: Employee Affiliation.

The Issuer shall ensure that the Applicant's PIV credential has a green line in Zone 15 indicating that the Applicant is a contractor.

The Issuer shall ensure that the Applicant's PIV credential has their correct office location (i.e. HQ, RI, RII, etc.) in Zone 17.

The Issuer shall ensure that the Applicant receives a badge with NC in Zone 4: Clearance Designation, indicating that the individual has no clearance and he/she must have no access to classified information.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request
- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

10.8.4 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

10.9 Final Approval

Once the background investigation has been completed, OPM sends a package containing the results of the investigation to the PSB with a completed *Certification of Investigation and Case Closing Transmittal* and a Form 79A, *Report of Agency Adjudicative Action*.

The Security Processing Unit analyst will:

1. Stamp the back of the Certification of Investigation an Case Closing Transmittal (CCT) with the date received,
2. Update the IPSS investigation record to reflect the date received from OPM, the closed investigation date, and the date forwarded for adjudication.
3. Attach the Certification of Investigation and Form79A, and any additional investigation reports (in the order they were received) to the top, right side of the folder
4. Place the folder on the closed Building Access investigations shelf for adjudication.

The Adjudicator will review the contractor's SF-85P and the background investigation report results in order to make a final determination of suitability.

<u>If the contractor is approved for access</u>:

The Adjudicator will:

1. Sign and date the Certificate of Investigation, stamp the CCT "Reviewed and Approved"; and retain it in the contractor's security folder
2. Complete the Form 79A with the adjudicative action, sign, and date the form; a copy of the Form 79A is retained in the folder and the original is sent to OPM
3. Update and sign the Form 225, *File Summary Sheet*
4. Generate a final access authorization approval letter
5. Provide the letter and the contractor's security folder to the PSB Chief for review and signature
6. Return the folder to the Security Processing Unit

The Security Processing Unit analyst will:

1. Update the employee's clearance record in IPSS to reflect the temporary access authorization as terminated. Create a final access authorization record reflecting "active" with the approval date.
2. Make copies of the final access authorization approval letter and retain a copy in the contractor's security folder
3. Send the final access authorization approval letter to the Project Officer. Provide the Facilities Security Branch a copy of the approval letter.
4. File the folder on the active shelf

<u>If the contractor is not approved for access</u>:

The Adjudicator will:

1. Sign and date the Certificate of Investigation, stamp the CCT "Denied"; and retain it in the contractor's security folder
2. Complete the Form 79A with the adjudicative action, sign, and date the form; a copy of the Form 79A is retained in the folder and the original is sent to OPM
3. Update and sign the Form 225, *File Summary Sheet*
4. Write a denial memorandum stating that the contractor is not eligible for an access authorization including a brief summary of the cause
5. Write a letter to the contractor, providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*
6. Deliver the contractor's security folder to the PSB Chief for review and consent to the to the denial recommendation

The Branch Chief will review the contractor's security folder and confirm consent by signing the denial memorandum. The letter to the contractor and the folder will then be forwarded to the Division of Facilities and Security Director for signature (as required by 10 CFR 10.22).

The Division of Facilities and Security Director reviews the contractor's security folder and signs the letter to the contractor. The security folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the contractor
2. Retain 1 set of copies in the contractor's security folder
3. Send the original denial memorandum to the NRC Project Officer
4. Send the original signed letter to the contractor
5. Update the contractor's record in IPSS
6. File the contractor's security folder to the "Term" shelf

11.0 The Daycare Worker Process

This section describes the requirements and procedures for adjudicating daycare workers providing childcare services in the NRC daycare facility. Daycare workers are not allowed access to classified information and therefore do not receive a clearance. Daycare workers, unless they receive prior access authorization, do not receive IT access authorization. However, the process and procedures include a background investigation by OPM to make a determination of eligibility for permanent access authorization.

11.1 Overview

The Daycare Worker Process allows for temporary access authorization to be granted, enabling daycare workers to begin work prior to the completion of a background investigation. Access authorizations for daycare workers are requested through a memo which is signed by the Applicant's Program Officer. The NRC Project Officer performs the Sponsor role for daycare workers. Daycare workers receive either IT-II access authorization or building access authorization.

Daycare providers requiring building access to NRC facilities require a Child Care National Agency Check with Inquiries (CNACI) by the OPM.

11.2 Daycare Worker with IT-II Access Authorization

11.2.1 Request for IT-II Access Authorization

Prior to a request for access authorization, a designated security officer of the daycare worker's employer will assure the Applicant's identity using at least two forms of approved certificates of identity per the I-9 documents list (e.g., Drivers License, Birth Certificate, or Passport) and provide a security forms package.

The security forms package includes the following materials:

- *Request for NRC Access Authorization* form
- *Fair Credit Reporting Act of 1970* form
- NRC Form 89, *Badge Request*
- FD-258, *Fingerprint Cards* (2) for those not enrolled at HQ
- Instructions for completing security forms
- e-QIP Quick Reference Guide

The Applicant will: (a) read, complete, and sign all required forms in the security forms package; (b) obtain fingerprints from an authorized source; and, (c) return completed signed forms and fingerprint cards to the security officer, unless enrollment will occur prior to EOD at headquarters.

The security officer will then forward the daycare worker's security forms and fingerprint cards to the NRC Project Officer (e.g., the Sponsor).

11.2.1.1 Sponsor Sends Applicant's forms to the Personnel Security Branch

The NRC Project Officer will:

1. Review the Applicant's security forms package
2. Complete and sign the *Request for NRC Access Authorization* form
3. Complete and sign the NRC Form 89, *Badge Request*
4. Submit the completed security forms package to the PSB

Supplemental material may be sent with the Applicant's security package, as needed. For example: Foreign National Questionnaire, Naturalization Certificate, bankruptcy disposition papers, documentation of paid accounts, etc.

11.2.1.2 Registrar Initiates e-QIP for the Applicant

A Security Processing Unit analyst will:

1. Login to e-QIP
2. Enter the Applicant's SSN in the "Manage Request" section and select "Initiate Request"
3. In the "User and Request Information" screen, under "Full Name" enter the Applicant last name, first name, and middle name
4. Tab to "Date of Birth" and enter the Applicant's birth date by selecting from the drop down screen for month, day, and year
5. Tab to "Place of Birth" and enter the Applicant's city and state or city and foreign country
6. Tab to "Personal Contact Information" and enter the Applicant's email address
7. Tab to "Form Information" and select the ISP/Form from the drop down menu and tab to "Applicant Group" and select Security from the drop down
8. Scroll down and select 'Submit' to create the record
9. Complete the Agency Usage Block (AUB) using the OPM templates for the investigation type needed
10. E-mail the Applicant that the e-QIP account has been set up

The Applicant will complete, certify, and submit his/her SF-86, *Questionnaire for National Security Positions* via e-QIP, print and sign any required forms, and return completed, signed forms to their employer's security officer.

The security officer will send the forms to the NRC Project Officer.

The NRC Project Officer will review the forms and forward them to the PSB.

11.2.2 Initial Screening

The Applicant's security forms package undergoes initial screening by a Security Processing Unit analyst.

11.2.2.1 Registrar Processes the Applicant's forms

The Security Processing Unit analyst will:

1. Date stamp the back of each item in the Applicant's security forms package
2. Verify that all required forms have been received. If any required forms are missing or incomplete, the security forms package is returned to the Project Officer
3. Print a copy of the Applicant's SF-86, *Questionnaire for National Security Positions* from e-QIP
4. Create an NRC Form 225, *File Summary Sheet* from INFORMS
5. Assemble the Applicant's security folder
   a. Use a red folder
   b. Affix a label with the Applicant's SSN and name to the folder tab
   c. Affix a coversheet for Privacy Act Info to the front outer cover of the folder
   d. Arrange forms in the Applicant's security folder as follows:

Left Side, Top to Bottom	***Right Side, Top to Bottom***
NRC Form 225	SF-86 (from e-QIP)
Request for NRC Access Authorization	Fair Credit Reporting Act of 1970
Processing Unit checklist	Supplemental documents
Correspondences	2 FD-258
NRC Form 89	

Supplemental Information

To print the NRC Form 225, File Summary Sheet in INFORMS:
l. Select Master List and select Form 225
m. Enter the applicant's name and DOB
n. Select the type of access authorization to be processed
o. Date: enter the date access authorization was requested
p. Select Investigative Agency to perform the investigation
q. Type the date the Fingerprint Cards were received
r. On the remarks section, type applicant's SSN and place of birth
s. Office Symbol: "HQ"
t. Type Clearance: "None"
u. Action: "IT Level I" or IT Level II"
v. Employer Code: use assigned 5code

11.2.2.2 Pre-screen the Security Forms Package

The pre-screening process is a series of preliminary checks to verify completeness and accuracy.

The Security Processing Unit analyst will perform the following checks and procedures:

1. Are all required forms in the security package?

2. Are the forms complete?
3. Has the Applicant signed all of the forms?
4. Do the signatures on all the forms match?
5. Is the Applicant using his/her name as it reads on his/her official ID: Birth Certification or Social Security Card?
6. If the Applicant is not enrolled at HQ prior to EOD, ensure that data entered on FD-258, *Fingerprint Cards* matches the Applicant data in the SF-86.
7. Review the Applicant's SF-86 and flag items reflecting derogatory information.
8. Has the Applicant signed the SF-86 signature forms?
9. Has the Applicant signed the Authorization for Release of Medical Information? (It must be signed if the Applicant answered "yes" to question 21 on the SF-86).

If there are any paper forms which are missing a signature, they must be sent back to the Project Officer for the Applicant's signature.

If there is a problem with the Applicant's SF-86, it must be corrected by the Applicant in e-QIP. To release e-QIP back to the Applicant for corrections:

1. Login to e-QIP
2. In the Applicant's record, select review
3. Under the rejection comments section, in the box labeled "Reject To Applicant Comments", provide a detailed record of which sections need corrections and what information is required.
4. Scroll down and select "Reject to Applicant."
5. The Applicant is notified via e-mail to make corrections to his/her SF-86 in e-QIP. The Project Officer is carbon copied (cc:) on this notification for case tracking purposes.

Supplemental Guidance

Security Processing Unit analysts should retain all correspondence (e-mail, mail, or notes/records of telephone conversations) in the applicant's security folder.

Internal (within NRC) requests for information should be sent via e-mail.

Print all e-mail correspondence – both sent and received.

Keep record of all phone calls, including dates and times.

Date stamp any additional documents received and retain them in the applicant's security folder.

11.2.2.3 Create a Record in the Integrated Personnel Security System (IPSS)

The Security Processing Unit analyst will:

1. Login to IPSS

2. Under “Create a New Person”, enter the Applicant’s SSN and full name as appears on the SF-86. If there is no middle name, enter “nmn”
3. Select “Create” to begin entering the Applicant’s personnel security record. Ensure that the fields in the following sections pertaining to an individual’s personnel security record are completed. (See Appendix D for details on the fields in each IPSS section)
   - Personal Data
   - Aliases
   - Employment Data
   - INS Info
   - Documents & Forms
   - Clearances/Access
   - Security checks
   - Investigation Data

11.2.3 Create a record in the PCI system (prior to EOD)

For those Applicants able to come to HQ for enrollment purposes prior to EOD, the Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant’s information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position” tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the “Sponsor” tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click “Save” and then click “Yes” to confirm sponsorship
7. Click “Enroll Person” and search the Applicant

8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

11.2.4 Suitability Determination

Upon confirmation that the package is complete, the Security Processing Unit analyst will perform preliminary checks that will help determine the Applicant's suitability for access authorization. These preliminary checks are:

- Credit check
- FBI Fingerprint and FBI name checks
- PIPS check, which includes:
  - the SII
  - the CVS
  - the JPAS
- CPCI

See Appendix E for detailed information about PIPS, SII, CVS, JPAS, CPCI.

IPSS is then updated and the Applicant's folder is provided to a Personnel Security Specialist (Adjudicator).

11.2.4.1 Perform Preliminary Checks

The Security Processing Unit analyst will:

1. Perform preliminary checks that will help determine the Applicant's suitability for access authorization
2. Retain all background check reports in the Applicant's security folder, on the right side, over the FD-258, *Fingerprint Cards*
3. Update the Applicant's Security Checks record in IPSS

When all required pre-screening and checks are complete, the Applicant's security folder should be up-to-date and ready for the Adjudicator to review. The Security Processing Unit analyst will then file the Applicant's security folder on the Adjudicators' shelf, and notify the Personnel Security Specialist (e.g., the Adjudicator) by e-mail.

11.2.4.1.1 Credit Check

To perform a credit check on the Applicant the Personnel Security Processing Unit analyst will:

1. Open Internet Explorer, and navigate to www.experian.com/esolutions/index.html
2. Login

   Select: **Consumer Credit**

   Access Subcode: Select **TBD3 1487040 Rockville MD**

   Product: **Employment Insight**
3. **Primary Applicant Box:** Enter the Applicant's name, SSN, date of birth, and phone number.
4. **Address Box:** Enter Applicant's current address. Click submit
5. Print the report

11.2.4.1.2 FBI Fingerprint and Name check

The Security Processing Unit Security Processing Unit analyst will send the Applicant's fingerprints to OPM via PIPS. Results usually come back via PIPS after a few business days.

11.2.4.1.3 PIPS - SII, CVS, and JPAS checks

The Personnel Security Processing Unit analyst will:

1. Login to PIPS
2. Select #2 CVS Menu
3. Select #1 SII/CVS/JPAS
4. Enter Applicant's SSN and last name and submit
5. A report screen will display Applicant's data. Scroll to the bottom of the page to view further screen options. Screens containing data will be flagged with a "Y".
6. Select the number of the desired screen to view.
7. Print the desired reports and log out of PIPS

11.2.4.1.4 CPCI (Central Personnel Clearance Index)

The Personnel Security Processing Unit analyst will:

1. Login to the CPCI. Open Internet Explorer and navigate to https://cpci.doe.gov/loginPage.faces
2. Enter either the SSN or name of the Applicant
3. Print the report
4. Log out of the CPCI

11.2.5 Temporary IT Access Authorization

Upon a favorable suitability determination by the Adjudicator, and concurrence by appropriate management officials, a temporary IT access authorization will be granted.

The PSB notifies the Project Officer and the Facilities Security Branch.

11.2.5.1 Favorable Eligibility Determination

The Adjudicator reviews the Applicant's security folder to determine eligibility for temporary IT access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the eligibility determination for a temporary IT access authorization is favorable, the following actions are performed:

1. The Adjudicator will:
   (a) Create an approval letter to the NRC Project Officer stating that the Applicant's temporary IT access authorization request has been adjudicated with no issues and is recommended for approval
   (b) Deliver the Applicant's security folder to the PSB Chief for review and consent to the approval recommendation
2. The Branch Chief will review the Applicant's security folder and confirm consent by signing the temporary IT access authorization letter. The folder is returned to the Adjudicator. The Adjudicator will:
   a) Update and sign the NRC Form 89, *Badge Request*
   b) Update the NRC Form 225 with the temporary access authorization approval date
   c) Release the SF-86 in e-QIP to OPM for the background investigation. (See 8.6)
3. The Adjudicator will enter favorable adjudication for Applicant in PCI
   - Login to PCI
   - Click "Adjudicate Person" and search the Applicant to be adjudicated
   - Click the Applicant's name to open the Applicant's record
   - Set the NACI status to "Approved"
   - On the Personal tab, click "Card Issuance Approved"
   - Click "Save" and then click "Yes" to confirm adjudication
   - Select the appropriate card profile and click "Accept"

   The file is then forwarded to the Security Processing Unit.
4. A Security Processing Unit analyst will:

(a) Copy the signed Temporary Access Approval letter and retain it in the Applicant's security folder

(b) Send the original signed Temporary Access Approval letter to the Project Officer

(c) Update the Applicant's Clearances/Accesses record in IPSS with the date the temporary IT access is approved and the Investigation record with the date the investigation is requested and the agency conducting the investigation.

5. Copy the signed NRC Form 89 and place the copy in Applicant's folder. The original is held in the Badge Request tray until the Applicant appears for their badge photo process.
6. Place the file on the 'Active' shelf.
7. The Project Officer will notify the applicant's employer that the temporary IT access has been approved and will make arrangements for the daycare worker's starting date and responsibilities.

11.2.5.2 Unfavorable Eligibility Determination

The Adjudicator reviews the Applicant's security folder to determine eligibility for a temporary IT access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the eligibility determination for a temporary IT access authorization is unfavorable, the Adjudicator will:

1. Write a denial memorandum stating that the Applicant is not eligible for an access authorization, including a brief summary of the cause
2. Write a letter to the Applicant providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*
3. Deliver the Applicant's security folder to the PSB Chief for review and consent to the denial recommendation

The Branch Chief will review the Applicant's security folder and confirm consent by signing the denial memorandum. The letter to the Applicant and the folder will then be forwarded to the Division of Facilities Security Director for signature.

The Division of Facilities Security Director reviews the Applicant's security folder and signs the letter to the Applicant. The Applicant's security folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the Applicant
2. Retain 1 set of copies in the Applicant's security folder
3. Send the original denial memo to the NRC Project Officer

4. Send the original signed letter to the Applicant
5. Update the Applicant's record in IPSS
6. File the Applicant's security folder to the "Denial" shelf

11.2.6 Background Investigation by OPM (if applicable)

The Adjudicator will:

1. Login to e-QIP
2. Double-check the accuracy of the information in the AUB, Part I of the Applicant's SF-86
3. Print a final copy of the Applicant's SF-86 from e-QIP, stamp it with the investigation type and the date requested, and retain it in Applicant's security folder
4. Purge the old copy of the Applicant's SF-86 from the folder.

   Note: Any printed information containing sensitive personal information must be shredded or destroyed according to NRC media destruction procedure.
5. Select "release from agency" (to submit the Applicant's information to OPM for a background investigation)

   Note: The Adjudicator may have previously requested a valid prior investigation from another agency (see Reciprocity procedure.) In this case there will be a note on the right side of the folder stating that that an OPM background investigation will not be requested.
6. Return the Applicant's security folder to the Security Processing Unit

The Security Processing Unit analyst updates the Applicant's record in IPSS with the current investigation type and date requested from OPM and files the security folder on the "Active" shelf.

11.2.7 Issuance of Credential (NRC ID Badge)

The daycare worker must report to NRC to be issued a red badge which indicates that he/she must have no access to classified information. The daycare worker will be informed by his/her employer's security officer of the date and time to report to NRC to have a photo taken and when the badge can be picked up. The daycare worker must bring two approved certificates of identity.

11.2.7.1 Create a record in the PCI system (if applicable)

NRC Project Officer directs the daycare workers, who were not previously enrolled, to the PSB. The Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields

- First Name
- Middle Name (if applicable)
- Last Name
- Date of Birth
- Agency
- E-mail
- Agency Clearance
- Contractor Clearance (if applicable)
- Location
- Social Security Number

4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

The daycare worker must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

Daycare workers receive a temporary badge until their PIV card is ready for issuance.

11.2.7.2 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

11.2.7.3 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.
- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall ensure that the Applicant's PIV credential has either "Daycare" in Zone 17.

The Issuer shall ensure that the Applicant's PIV credential has their correct office location (i.e. HQ, RI, RII, etc.) in Zone 17.

In the event the Applicant is a first responder, the Issuer shall ensure that the Applicant's PIV credential has a red line in Zone 12 indicating that the Applicant is a first responder.

The Issuer shall ensure that the Applicant's PIV credential has NC in Zone 4: Clearance Designation, indicating the Applicant has no clearance.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request
- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

11.2.7.4 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

11.2.8 Final Approval

Once the background investigation has been completed, OPM sends a package containing the results of the investigation to the PSB, with a *Certification of Investigation, Case Closing Transmittal*, and a Form 79A, *Report of Agency Adjudicative Action*.

The Security Processing Unit analyst will:

1. Stamp the back of the Certification of Investigation and Case Closing Transmittal (CCT) with the date received,
2. Update the IPSS investigation record to reflect the date received from OPM, the closed investigation date, and the date forwarded for adjudication.
3. Attach the Certificate and Form 79A, and any additional investigation reports (in the order they were received) to the top, right side of the folder
4. Place the folder on the closed IT investigations shelf for adjudication

The Adjudicator will review the daycare worker's SF-86 and the background investigation report results in order to make a final determination of suitability.

<u>If the final determination of suitability is favorable</u>:

The Adjudicator will:

1. Sign and date the Certificate of Investigation, stamp the CCT "Reviewed and Approved"; and retain it in the daycare worker's security folder
2. Complete the Form 79A with the adjudicative action, sign, and date the form; a copy of the Form 79A is retained in the folder and the original is sent to OPM
3. Update and sign the Form 225, *File Summary Sheet*
4. Generate a final IT access authorization approval letter
5. Provide the letter and the daycare worker's security folder to the PSB Chief for review and signature
6. Return the folder to the Security Processing Unit
7. The Adjudicator will enter favorable adjudication for Applicant in PCI
    - Login to PCI
    - Click "Adjudicate Person" and search the Applicant to be adjudicated
    - Click the Applicant's name to open the Applicant's record
    - Set the NACI status to "Approved"
    - On the Personal tab, click "Card Issuance Approved"
    - Click "Save" and then click "Yes" to confirm adjudication

- Select the appropriate card profile and click "Accept"

The Security Processing Unit analyst will:

1. Update the employee's Access record in IPSS to terminate the IT 'Temp' access record and create an IT 'Final' access record with the approval date.
2. Make copies of the final IT access authorization approval letter and retain one copy in the daycare worker's security folder. Forward a copy to the Facilities Security Branch.
3. Send the original final IT access authorization approval letter to the Project Officer
4. File the folder on the active shelf

11.2.8.1 Create a record in the PCI system (Final Badge Issuance)

NRC Project Officer directs the daycare workers to the PSB. The Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab

10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

The daycare workers must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

Daycare workers receive a temporary badge until their PIV card is ready for issuance.

11.2.8.2 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

11.2.8.3 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.

- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall ensure that the Applicant's PIV credential has either "Daycare" in Zone 17.

The Issuer shall ensure that the Applicant's PIV credential has their correct office location (i.e. HQ, RI, RII, etc.) in Zone 17.

In the event the Applicant is a first responder, the Issuer shall ensure that the Applicant's PIV credential has a red line in Zone 12 indicating that the Applicant is a first responder.

The Issuer shall ensure that the Applicant's PIV credential has NC in Zone 4: Clearance Designation, indicating the Applicant has no clearance.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request
- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

11.2.8.4 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

<u>If the final determination of suitability is unfavorable</u>:

The Adjudicator will:

1. Sign and date the Certificate of Investigation, stamp the CCT "Denied"; and retain it in the daycare worker's security folder
2. Complete the Form 79A with the adjudicative action, sign, and date the form; a copy of the Form 79A is retained in the folder and the original is sent to OPM
3. Update and sign the Form 225, *File Summary Sheet*
4. Write a denial memorandum stating that the daycare worker is not eligible for an access authorization, including a brief summary of the cause
5. Write a letter to the daycare worker providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*

6. Deliver the daycare worker's security folder to the PSB Chief for review and consent to the to the denial recommendation

The Branch Chief will review the daycare worker's security folder and confirm consent by signing the denial memorandum. The letter to the daycare worker and the folder will then be forwarded to the Division of Facilities Security Director for signature.

The Division of Facilities Security Director reviews the daycare worker's security folder and signs the letter to the daycare worker. The security folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the daycare worker
2. Retain 1 set of copies in the daycare worker's security folder
3. Send the original denial memorandum to the NRC Project Officer
4. Send the original signed letter to the daycare worker
5. Update the daycare worker's record in IPSS
6. File the daycare worker's security folder to the "Denied" shelf

11.3 Daycare Worker with Building Access Authorization

11.3.1 Request for Access Authorization

Prior to a request for access authorization, a designated security officer of the daycare worker's employer will: (a) assure the Applicant's identity using at least two forms of approved certificates of identity (e.g., Drivers License, Birth Certificate, or Passport) and provide a security forms package.

The security forms package includes the following materials:

- *Request for NRC Access Authorization* form
- *Fair Credit Reporting Act of 1970* form
- NRC Form 89, *Badge Request*
- FD-258, *Fingerprint Cards* (2)
- Instructions for completing security forms
- e-QIP Quick Reference Guide

The Applicant will: (a) read, complete, and sign all required forms in the security forms package; (b) obtain fingerprints from an authorized source; and, (c) return completed, signed forms and fingerprint cards to the security officer.

The security officer will then forward the daycare worker's resume, security forms and fingerprint cards to the NRC Project Officer (e.g., the Sponsor).

11.3.1.1 Sponsor Sends Applicant's forms to the Personnel Security Branch

The NRC Project Officer will:

1. Review the Applicant's security forms package

2. Complete and sign the *Request for NRC Access Authorization* (not the NRC Form 237)
3. Complete and sign the NRC Form 89, *Badge Request*
4. Submit the completed security forms package to the PSB

Supplemental material may be sent with the Applicant's security package, as needed. For example: Foreign National Questionnaire, Naturalization Certificate, bankruptcy disposition papers, documentation of paid accounts, etc.

11.3.1.2 Registrar Initiates e-QIP for the Applicant

A Security Processing Unit analyst will:

1. Login to e-QIP
2. Enter the Applicant's SSN in the "Manage Request" section and select "Initiate Request"
3. In the "User and Request Information" screen, under "Full Name" enter the Applicant last name, first name, and middle name
4. Tab to "Date of Birth" and enter the Applicant's birth date by selecting from the drop down screen for month, day, year
5. Tab to "Place of Birth" and enter the Applicant's city and state or city and foreign country
6. Tab to "Personal Contact Information" and enter the Applicant's email address
7. Tab to "Form Information" and select the ISP/Form from the drop down menu and tab to "Applicant Group" and select Security from the drop down
8. Scroll down and select 'Submit' to create the record
9. Complete the AUB using the OPM templates for the investigation type needed (NACI for building access; CNACI for day care)
10. E-mail the Applicant that e-QIP account has been set up

The Applicant will complete, certify, and submit his/her SF-85P, *Questionnaire for Public Trust Positions* via e-QIP, print and sign any required forms, and return completed, signed forms to their employer's security officer.

The security officer will send the forms to the NRC Project Officer.

The NRC Project Officer will review the forms and forward them to the PSB.

11.3.2 Initial Screening

The Applicant's security forms package undergoes initial screening by a Security Processing Unit analyst.

11.3.2.1 Registrar Processes the Applicant's forms

The Security Processing Unit analyst will:

1. Date stamp the back of each item in the Applicant's security forms package.
2. Verify that all required forms have been received. If any required forms are missing or incomplete, the security forms package is returned to the Project Officer.
3. Print a copy of the Applicant's SF-85P, *Questionnaire for Public Trust Positions* from e-QIP
4. Create an NRC Form 225, *File Summary Sheet* from INFORMS.
5. Assemble the Applicant's security folder
   a. Use a blue folder
   b. Affix a label with the Applicant's SSN and name to the folder tab
   c. Affix a coversheet for Privacy Act Info to the front outer cover of the folder
   d. Arrange forms in the Applicant's security folder as follows:

Left Side, Top to Bottom	***Right Side, Top to Bottom***
NRC Form 225	SF-85P (from e-QIP)
Request for NRC Access Authorization	Fair Credit Reporting Act
Processing Unit checklist	Supplemental documents
Correspondences	2 FD-258
NRC Form 89	

Supplemental Information

To print the NRC Form 225, File Summary Sheet in INFORMS:
a. Select Master List and select Form 225
b. Enter the applicant's name and DOB
c. Select the type of clearance to be processed
d. Date: enter the date clearance was requested
e. Select Investigative Agency to perform the investigation
f. Type the date the Fingerprint Cards were received
g. On the remarks section, type applicant's SSN and place of birth
h. Office Symbol: "HQ"
i. Type Clearance: "None"
j. Action: "Building Access"
k. Employer Code: use assigned 5code

11.3.2.2 Pre-screen the Security Forms Package

The pre-screening process is a series of preliminary checks to verify completeness and accuracy.

The Security Processing Unit analyst will perform the following checks and procedures:

1. Are all required forms in the security package?

2. Are the forms complete?
3. Has the Applicant signed all of the forms?
4. Do the signatures on all the forms match?
5. Is the Applicant using his/her name as it reads in his/her official ID: Birth Certificate or Social Security Card?
6. Ensure that data entered on FD-258, *Fingerprint Cards* matches the Applicant data in the SF-85P.
7. Review the Applicant's SF-85P and flag items reflecting derogatory information.
8. Has the Applicant signed the SF-85P signature forms?

If there are any paper forms which are missing a signature, they must be sent back to the Project Officer for the Applicant's signature.

If there is a problem with the Applicant's SF-85P, it must be corrected by the Applicant in e-QIP. To release e-QIP back to the Applicant for corrections:

1. Login to e-QIP
2. In the Applicant's record, select review
3. Under the rejection comments section, in the box labeled "Reject To Applicant Comments", provide a detailed record of which sections need corrections and what information is required.
4. Scroll down and select "Reject to Applicant"
5. The Applicant is notified via e-mail to make corrections to his/her SF-85P in e-QIP.

Supplemental Guidance

Security Processing Unit analysts should retain all correspondence (e-mail, mail, or notes/records of telephone conversations) in the applicant's security folder.

Internal (within NRC) requests for information should be sent via e-mail.

Print all e-mail correspondence – both sent and received.

Keep record of all phone calls, including dates and times.

Date stamp any additional documents received and retain them in the applicant's security folder.

11.3.2.3 Create a Record in the Integrated Personnel Security System (IPSS)

The Security Processing Unit analyst will:

1. Login to IPSS
2. Under "Create a New Person", enter the Applicant's SSN and full name as appears on the SF-85P. If there is no middle name, enter "nmn"
3. Select "Create" to begin entering the Applicant's personnel security record. Ensure that the fields in the following sections pertaining to an individual's personnel

security record are completed. (See Appendix D for details on the fields in each IPSS section)

- Personal Data
- Aliases
- Employment Data
- INS Info
- Documents & Forms
- Clearances/Access
- Security checks
- Investigation Data

11.3.3 Create a record in the PCI system (prior to EOD)

For those Applicants able to come to HQ for enrollment purposes prior to EOD, the Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab

10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

11.3.4 Perform Pre-Employment Checks

Upon confirmation that the package is complete, the Security Processing Unit analyst will perform preliminary checks that will help determine the Applicant's suitability for access authorization. These preliminary checks are:

- Credit check
- FBI Fingerprint and FBI Name checks
- PIPS check, which includes:
  - the SII
  - the CVS
  - the JPAS
- CPCI

See Appendix E for detailed information about PIPS, SII, CVS, JPAS, CPCI.

IPSS is then updated and the Applicant's folder is provided to a personnel security specialist (Adjudicator).

11.3.4.1 Perform Preliminary Checks

The Security Processing Unit analyst will:

1. Perform preliminary checks that will help determine the Applicant's suitability for access authorization
2. Retain all background check reports in the Applicant's security folder, on the right side, between the Fair Credit Reporting Act and the FD-258, *Fingerprint Cards*
3. Update the Applicant's Security Checks record in IPSS

When all required pre-screening and checks are complete, the Applicant's security folder should be up-to-date and ready for the Adjudicator to review. The Security Processing Unit analyst will then file the Applicant's security folder on the Adjudicators' shelf, and notify the Personnel Security Specialist (e.g., the Adjudicator) by e-mail.

11.3.4.1.1 Credit Check

To perform a credit check on the Applicant the Personnel Security Processing Unit analyst will:

1. Open Internet Explorer, and navigate to www.experian.com/esolutions.index.html

2. Login

   Select: **Consumer Credit**

   Access Subcode: **TBD3 1487040 Rockville MD**

   Product: **Employer Insight**

3. **Primary Applicant Box:** Enter the Applicant's name, SSN, date of birth, and phone number.
4. **Address Box:** Enter Applicant's current address. Click Submit
5. Print the report

11.3.4.1.2 FBI Fingerprint and Name check

The Security Processing Unit analyst will scan the fingerprint card and send the file to OPM via PIPS. Results usually come back via PIPS after a few business days.

11.3.4.1.3 PIPS - SII, CVS, and JPAS checks

The Personnel Security Processing Unit analyst will:

1. Login to PIPS
2. Select #2 CVS Menu
3. Select #1 SII/CVS/JPAS
4. Enter Applicant's SSN and last name and submit
5. A report screen will display Applicant's data. Scroll to the bottom of the page to view further screen options. Screens containing data will be flagged with a "Y".
6. Select the number of the desired screen to view.
7. Print the report and log out of PIPS

11.3.4.1.4 CPCI (Central Personnel Clearance Index)

The Personnel Security Processing Unit analyst will:

1. Login to the CPCI. Open Internet Explorer and navigate to: https://cpci.doe.gov/loginPage.faces
2. Enter either the SSN or name of the Applicant
3. Print the report
4. Log out of the CPCI

11.3.5 Interim Access Authorization

Upon a favorable suitability determination by the Adjudicator, and concurrence by appropriate management officials, a temporary access authorization will be granted.

The PSB notifies the Project Officer and the Facilities Security Branch.

11.3.5.1 Favorable Eligibility Determination

The Adjudicator reviews the Applicant's security folder to determine eligibility for a temporary access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the eligibility determination for an interim access authorization is favorable, the following actions are performed:

1. The Adjudicator will:
   (a) Create an access authorization approval letter to the NRC Project Officer stating that the Applicant's temporary access authorization request has been adjudicated with no issues and is recommended for approval
   (b) Deliver the Applicant's security folder to the PSB Chief for review and consent to the approval recommendation
2. The Branch Chief will review the Applicant's security folder and confirm consent by signing the access authorization approval letter. The folder is returned to the Adjudicator. The Adjudicator will:
   a) Update and sign the NRC Form 89, *Badge Request*
   b) Update the NRC Form 225, *File Summary,* with the interim access authorization approval date
   c) Release the SF-85P in e-QIP to OPM for the background investigation (See 10.6)

   The file is then forwarded to the Security Processing Unit.
3. The Adjudicator will enter favorable adjudication for Applicant in PCI
   - Login to PCI
   - Click "Adjudicate Person" and search the Applicant to be adjudicated
   - Click the Applicant's name to open the Applicant's record
   - Set the NACI status to "Approved"
   - On the Personal tab, click "Card Issuance Approved"
   - Click "Save" and then click "Yes" to confirm adjudication
   - Select the appropriate card profile and click "Accept"
4. A Security Processing Unit analyst will:
   (a) Copy the signed Interim Access Approval letter and retain it in the Applicant's security folder
   (b) Send the original signed interim access approval letter to the Project Officer
   (c) Update the Applicant's Clearances/Accesses record in IPSS with the date the interim access was approved and the Investigation record with the date the investigation was requested and the agency conducting the investigation.

(d) Copy the signed NRC Form 89 and place a copy in the Applicant's folder. The original is held in the Badge Request tray until the Applicant appears for their photo badge process.

(e) Place the file on the 'Active' shelf.

5. The Project Officer will notify the Applicant's employer that the interim access has been approved and will make arrangements for the daycare worker's starting date and responsibilities.

11.3.5.2 Unfavorable Eligibility Determination

The Adjudicator reviews the Applicant's security folder to determine eligibility for temporary access authorization. If the review results are not conclusive, the Adjudicator works the case to resolve issues or get additional information from the Applicant.

If the eligibility determination for a temporary access authorization is unfavorable, the Adjudicator will:

1. Write a denial memorandum stating that the Applicant is not eligible for an access authorization, including a brief summary of the cause.
2. Write a letter to the Applicant, providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*.
3. Deliver the Applicant's security folder to the PSB Chief for review and consent to the to the denial recommendation

The Branch Chief will review the Applicant's security folder and confirm consent by signing the denial memorandum. The letter to the Applicant and the folder will then be forwarded to the Division of Facilities Security Director for signature.

The Division of Facilities Security Director reviews the Applicant's security folder and signs the letter to the Applicant. The Applicant's security folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the Applicant
2. Retain 1 set of copies in the Applicant's security folder
3. Send the original denial memorandum to the NRC Project Officer
4. Send the original signed letter to the Applicant
5. Update the Applicant's record in IPSS
6. File the Applicant's security folder to the "Denied" shelf

11.3.6 Background Investigation by OPM (if applicable)

The Adjudicator will:

1. Login to e-QIP

2. Double-check the accuracy of the information in the AUB, Part I of the Applicant's SF-85P
3. Print a final copy of the Applicant's SF-85P from e-QIP, stamp it with the investigation type and the date requested, and retain it in Applicant's security folder
4. Purge the old copy of the Applicant's SF-85P from the folder.

   Note: Any printed information containing sensitive personal information must be shredded or destroyed according to NRC media destruction procedure.
5. Select "release from agency" (to submit the Applicant's information to OPM for a background investigation)

   Note: The Adjudicator may have previously requested a valid prior investigation from another agency (see Reciprocity procedure.) In this case there will be a note on the right side of the folder stating that that an OPM background investigation will not be requested.
6. Return the Applicant's security folder to the Security Processing Unit

The Security Processing Unit analyst updates the Applicant's record in IPSS with the current investigation type and date, and files the security folder.

11.3.7 Issuance of Credential (NRC ID Badge)

The daycare worker must report to NRC to be issued a red badge which indicates that he/she must have no access to classified information. The daycare worker will be informed by his/her employer's security officer of the date and time to report to NRC for a photo and when the badge can be picked up. The daycare worker must bring two approved certificates of identity.

11.3.7.1 Create a record in the PCI system (if applicable)

NRC Project Officer directs the new daycare workers, who were not previously enrolled, to the PSB. The Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance

- Contractor Clearance (if applicable)
- Location
- Social Security Number

4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant
8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

The daycare workers must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

Daycare workers receive a temporary badge until their PIV card is ready for issuance.

11.3.7.2 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

11.3.7.3 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.
- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall ensure that the Applicant's PIV credential has their correct office location (i.e. HQ, RI, RII, etc.) in Zone 17.

The Issuer shall ensure that the Applicant receives a badge with NC in Zone 4: Clearance Designation, indicating that the individual has no clearance and he/she must have no access to classified information.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request
- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

11.3.7.4 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

11.3.8 Final Approval

Once the background investigation has been completed, OPM sends a package containing the results of the investigation to the PSB with a completed *Certification of Investigation and Case Closing Transmittal* and a Form 79A, *Report of Agency Adjudicative Action*.

The Security Processing Unit analyst will:

5. Stamp the back of the Certification of Investigation an Case Closing Transmittal (CCT) with the date received,
6. Update the IPSS investigation record to reflect the date received from OPM, the closed investigation date, and the date forwarded for adjudication.
7. Attach the Certification of Investigation and Form79A, and any additional investigation reports (in the order they were received) to the top, right side of the folder
8. Place the folder on the closed Building Access investigations shelf for adjudication.

The Adjudicator will review the daycare worker's SF-85P and the background investigation report results in order to make a final determination of suitability.

<u>If the daycare worker is approved for access</u>:

The Adjudicator will:

1. Sign and date the Certificate of Investigation, stamp the CCT "Reviewed and Approved"; and retain it in the daycare worker's security folder
2. Complete the Form 79A with the adjudicative action, sign, and date the form; a copy of the Form 79A is retained in the folder and the original is sent to OPM
3. Update and sign the Form 225, *File Summary Sheet*
4. Generate a final access authorization approval letter
5. Provide the letter and the daycare worker's security folder to the PSB Chief for review and signature
6. Return the folder to the Security Processing Unit

The Security Processing Unit analyst will:

1. Update the employee's clearance record in IPSS to reflect the temporary access authorization as terminated. Create a final access authorization record reflecting "active" with the approval date.
2. Make copies of the final access authorization approval letter and retain a copy in the daycare worker's security folder
3. Send the final access authorization approval letter to the Project Officer. Provide the Facilities Security Branch a copy of the approval letter.
4. File the folder on the active shelf

<u>If the daycare worker is not approved for access</u>:

The Adjudicator will:

1. Sign and date the Certificate of Investigation, stamp the CCT "Denied"; and retain it in the daycare worker's security folder
2. Complete the Form 79A with the adjudicative action, sign, and date the form; a copy of the Form 79A is retained in the folder and the original is sent to OPM

3. Update and sign the Form 225, *File Summary Sheet*
4. Write a denial memorandum stating that the daycare worker is not eligible for an access authorization including a brief summary of the cause
5. Write a letter to the daycare worker, providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied access authorization in accordance with the criteria established in 10 CFR 10.11, *Criteria*
6. Deliver the daycare worker's security folder to the PSB Chief for review and consent to the to the denial recommendation

The Branch Chief will review the daycare worker's security folder and confirm consent by signing the denial memorandum. The letter to the daycare worker and the folder will then be forwarded to the Division of Facilities and Security Director for signature (as required by 10 CFR 10.22).

The Division of Facilities and Security Director reviews the daycare worker's security folder and signs the letter to the daycare worker. The security folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the denial memorandum and the letter to the daycare worker
2. Retain 1 set of copies in the daycare worker's security folder
3. Send the original denial memorandum to the NRC Project Officer
4. Send the original signed letter to the daycare worker
5. Update the daycare worker's record in IPSS
6. File the daycare worker's security folder to the "Term" shelf

12.0 The Licensee Process

This section describes the requirements and procedures for adjudicating licensees who require unescorted access to nuclear facility sensitive areas and/or access to sensitive or classified information.

Licensees are companies which are licensed to operate by the NRC. Individuals working for these companies who will have "need-to-know" access to classified information or to protected and vital areas of nuclear power facilities, are required to have a clearance. These individuals are the "Applicant" (or sometimes, "subject") during the clearance process.

12.1 Overview

The Licensee Process applies only to background investigations for clearances. The process does not grant access authorization to NRC facilities. Therefore, the pre-investigation waiver permitting temporary access authorization does not apply to Licensees.

The Licensees perform their own standard background checks and investigations on their employees (and contractors) that do not have a need for access to classified information. The purpose of the Licensee Process is only to provide clearances for access to classified information or special nuclear material.

12.1.1 Materials Access Authorization Program (MAAP)

Under the Materials Access Authorization Program, individuals whose work affords access to or control over special nuclear material are required to have special nuclear material access authorization.

Special nuclear material access authorization means an administrative determination that an individual may work at a job which affords access to or control over special nuclear material and that permitting the individual to work at that job would not be harmful to the common defense and security.

There are two types of NRC access authorization under MAAP: "U" for Top Secret and "R" for Secret.

12.1.1.1 "U" Access Authorization

The NRC "U" special nuclear material access authorization applies only to MAAP. It is required for eligibility to work at a job in which an individual could steal or divert special nuclear material, or commit sabotage which would endanger the public by exposure to radiation. Such jobs include but are not limited to:

(i) All positions in the licensee's security force

(ii) Management positions with the authority to (a) direct the actions of members of the security force or alter security procedures, or (b) direct routine movements of special nuclear material, or (c) direct the routine status of vital equipment

(iii) All jobs which require unescorted access within onsite alarm stations

(iv) All jobs which require unescorted access to special nuclear material or within vital areas

(v) All jobs which require the individual to transport, arrange for transport, drive motor vehicles in road shipments of special nuclear material, pilot aircraft in air shipments of special nuclear material, act as monitors at transfer points, or escort road, rail, sea, or air shipments of special nuclear material subject to certain physical protection requirements, or alter the scheduling and routing of such transport

12.1.1.2 "R" Access Authorization

The NRC "R" special nuclear material access authorization is required for eligibility to work at a job which requires unescorted access within protected areas, and which does not fall within the criterion listed above for a "U" access authorization.

The NRC "R" access authorization applies only to MAAP, and is sometimes called a "DOE CERT."

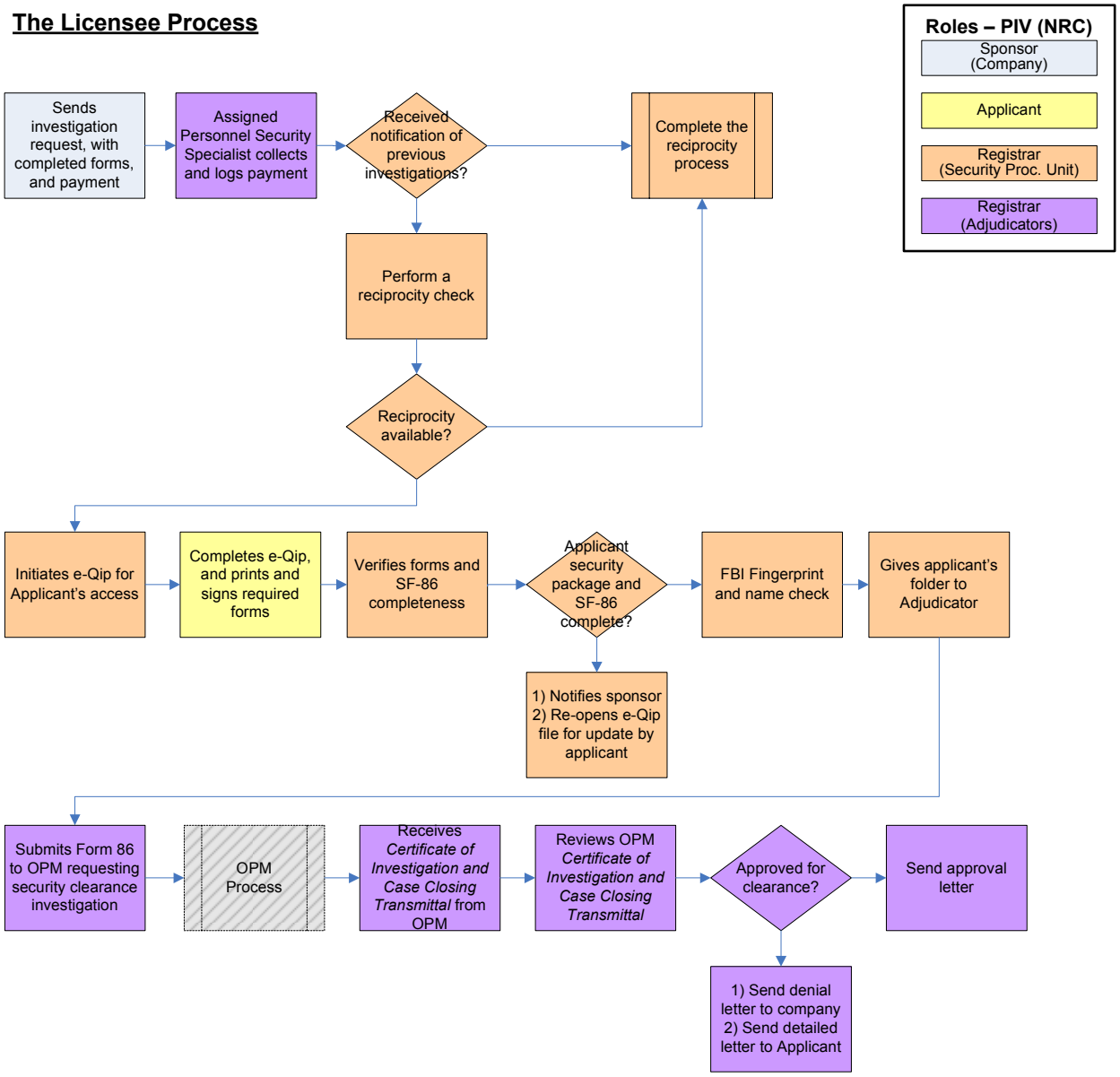
12.1.2 Information Access Authorization Program (IAAP)

Under the Information Access Authorization Program, individuals whose work involves "need-to-know" access to restricted data or national security information are required to have a clearance.

The Licensee Process begins with the formal request from a Licensee for a clearance investigation for the Applicant. The Sponsor role is filled by the Licensee.

The Licensee Process is illustrated on the following page.

The Licensee Process



12.2 Request for Access Authorization

Prior to a request for access authorization, a designated security officer of the Licensee will: (a) assure the Applicant's identity using at least two forms of approved certificates of identity (e.g., Drivers License, Birth Certificate, or Passport) and provide a security forms package.

The security forms package includes the following materials:

- *E-QIP Form for Requesting an NRC Clearance for Licensees*
- NRC Form 237, *Request for Access Authorization*
- *Fair Credit Reporting Act of 1970* form
- FD-258, *Fingerprint Cards* (2)
- NRC Form 176, *Security Acknowledgement*
- Instructions for completing security forms
- e-QIP Quick Reference Guide

The Applicant will: (a) read, complete, and sign all required forms in the security forms package, except the NRC Form 176, which will be completed and signed later; (b) obtain fingerprints from an authorized source; and, (c) return completed, signed forms and fingerprint cards to the security officer.

The security officer will then forward the Applicant's security forms and fingerprint cards along with a payment to the NRC PSB (PSB). The payment is charged by the NRC for completing the required OPM investigation and adjudication.

12.2.1 Payment Collection and Records

A PSB representative is assigned to receive all Licensee requests for NRC clearance. This person will collect and log the Licensee payment. If a payment is omitted from the Licensee clearance request package, the PSB representative will call the Licensee.

The Applicant's package is then provided to the Security Processing Unit.

12.2.2 Registrar Initiates e-QIP for the Applicant

A Security Processing Unit analyst will:

1. Login to e-QIP
2. Enter the Applicant's SSN in the "Manage Request" section and select "Initiate Request"
3. In the "User and Request Information" screen, under "Full Name" enter the Applicant last name, first name, and middle name
4. Tab to "Date of Birth" and enter the Applicant's birth date by selecting from the drop down screen for month and day, and entering the year
5. Tab to "Place of Birth" and enter the Applicant's city and state or city and foreign country
6. Tab to "Personal Contact Information" and enter the Applicant's email address

7. Tab to "Form Information" and select the ISP/Form from the drop down menu and tab to "Applicant Group" and select Security from the drop down list
8. Scroll down and select 'Submit' to create the record
9. Complete the AUB using the OPM templates for the investigation type needed
10. E-mail the Applicant that the e-QIP account has been set up

The Applicant will complete, certify, and submit his/her SF-86, *Questionnaire for National Security Positions* via e-QIP, and print and sign any required forms. The Applicant will also complete and sign the NRC Form 176, *Security Acknowledgement* and return all signed forms to the Licensee security officer.

The security officer will send the forms to the NRC Personnel Security Branch.

12.3 Initial Screening

The Applicant's security forms package undergoes initial screening by a Security Processing Unit analyst.

12.3.1 Registrar Processes the Applicant's forms

The Security Processing Unit analyst will:

1. Date stamp the back of each item in the Applicant's security forms package.
2. Verify that all required forms have been received.
3. Print a copy of the Applicant's SF-86, *Questionnaire for National Security Positions* from e-QIP
4. Create an NRC Form 225, *File Summary Sheet* from INFORMS.
5. Assemble the Applicant's security folder
   a. Use a brown folder for MAAP Applicants; use an orange folder for IAAP Applicants
   b. Affix a label with the Applicant's SSN and name to the folder tab
   c. Affix a coversheet for Privacy Act Info to the front outer cover of the folder
   d. Arrange forms in the Applicant's security folder as follows:

Left Side, Top to Bottom	***Right Side, Top to Bottom***
NRC Form 225	SF-86 (from e-QIP)
NRC Form 237	Fair Credit Reporting Act
Request for NRC Access Authorization	Supplemental documents
Correspondences	NRC From 176
Processing Unit checklist	2 FD-258

Supplemental Information

To print the NRC Form 225, File Summary Sheet in INFORMS:

a. Select Master List and select Form 225
b. Enter the applicant's name and DOB
c. Select the type of clearance to be processed
d. Date: enter the date clearance was requested
e. Select Investigative Agency to perform the investigation
f. Type the date the Fingerprint Cards were received
g. On the remarks section, type applicant's SSN and place of birth
h. Office Symbol: "IAAP" or "MAAP" for L or Q clearance; "MAAP" for R or U clearance
i. Type Clearance: "Q", "L", "R", or "U"
j. Action: "Grant"
k. Employer Code: use assigned 4code for licensee

12.3.2 Pre-screen the Security Forms Package

The pre-screening process is a series of preliminary checks to verify completeness and accuracy.

The Security Processing Unit analyst will perform the following checks and procedures:

1. Are all required forms in the security package?
2. Are the forms complete?
3. Has the Applicant signed all of the forms?
4. Do the signatures on all the forms match?
5. Ensure that data entered on FD-258, *Fingerprint Cards* matches the Applicant in the SF-86.
6. Review the Applicant's SF-86 and flag items reflecting derogatory information.
7. Has the Applicant signed the SF-86 signature forms?
8. Has the Applicant signed the Authorization for Release of Medical Information? (It must be signed if the Applicant answered "yes" to question 21 on the SF-86).

If there are any paper forms which are missing a signature, they must be sent back to the Licensee for the Applicant's signature.

If there is a problem with the Applicant's SF-86, it must be corrected by the Applicant in e-QIP. To release e-QIP back to the Applicant for corrections:

1. Login to e-QIP
2. In the Applicant's record, select Review
3. Under the rejection comments section, in the box labeled "Reject To Applicant Comments", provide a detailed record of which sections need corrections and what information is required.
4. Scroll down and select "Reject to Applicant"

5. The Applicant is notified via e-mail to make corrections to his/her SF-86 in e-QIP.

Supplemental Guidance

Security Processing Unit analysts should retain all correspondence (e-mail, mail, or notes/records of telephone conversations) in the applicant's security folder.

Internal (within NRC) requests for information should be sent via e-mail.

Print all e-mail correspondence – both sent and received.

Keep record of all phone calls, including dates and times.

Date stamp any additional documents received and retain them in the applicant's security folder.

12.3.3 Create a Record in the Integrated Personnel Security System (IPSS)

The Security Processing Unit analyst will:

1. Login to IPSS
2. Under "Create a New Person", enter the Applicant's SSN and full name as appears on the SF-85P. If there is no middle name, enter "nmn"
3. Select "Create" to begin entering the Applicant's personnel security record. Ensure that the fields in the following sections pertaining to an individual's personnel security record are completed. (See Appendix D for details on the fields in each IPSS section)
   - Personal Data
   - Aliases
   - Employment Data
   - INS Info
   - Documents & Forms
   - Clearances/Access
   - Security checks
   - Investigation Data

12.4 Perform Preliminary Checks

Upon confirmation that the package is complete, the Security Processing Unit analyst will perform an FBI Fingerprint and name check.

12.4.1 FBI Fingerprint and Name Check

The Security Processing Unit analyst will scan the fingerprint card and send the file to OPM via PIPS. Results usually come back via PIPS after a few business days.

If there is a notice of previous clearance processing for the individual, a reciprocity check may be performed.

IPSS is then updated and the Applicant's folder is provided to a personnel security specialist (Adjudicator).

12.5 Background Investigation by OPM

The Adjudicator will:

1. Login to e-QIP
2. Double-check the accuracy of the information in the Agency Usage Block, Part I of the Applicant's SF-86
3. Print a final copy of the Applicant's SF-86 from e-QIP, stamp it with the investigation type and the date requested, and retain it in Applicant's security folder
4. Purge the old copy of the Applicant's SF-86 from the folder

   Note: Any printed information containing sensitive personal information must be shredded or destroyed according to NRC media destruction procedure
5. Select "release from agency" (to submit the Applicant's information to OPM for a background investigation).

   Note: The Adjudicator might have already requested a valid prior investigation from another agency (see Reciprocity procedure.) In this case there will be a note on the right side of the folder stating that that an OPM background investigation will not be requested
6. Return the Applicant's security folder to the Security Processing Unit

The Security Processing Unit analyst updates the Applicant's record in IPSS with the current investigation type and date, and files the security folder.

12.6 Adjudication for Clearance

Once the background investigation has been completed, OPM sends a package containing the results of the investigation to the Personnel Security Branch, with a completed *Certification of Investigation and Case Closing Transmittal* and a Form 79A, *Report of Agency Adjudicative Action*.

The Security Processing Unit analyst will:

1. Stamp the back of the Certificate of Investigation and Case Closing Transmittal (CCT) with the date received
2. Update the IPSS investigation record to reflect the date received from OPM, the closed investigation date, and the date forwarded for adjudication.
3. Attach the Certificate and Form79A, and any additional investigation reports (in the order they were received) to the top, right side of the folder
4. Place file on the closed Licensee investigations shelf for adjudication.

The Adjudicator will review the Applicant's SF-86 and the background investigation report results.

<u>If the Applicant is approved for clearance</u>:

The Adjudicator will:

1. Sign and date the Certificate of Investigation, stamp the CCT "Reviewed and Approved"; and retain it in the Applicant's security folder
2. Complete the Form 79A with the adjudicative action, sign, and date the form; a copy of the Form 79A is retained in the folder and the original is sent to OPM
3. Update and sign the Form 225, *File Summary Sheet*
4. Generate an approval letter
5. Provide the letter and the Applicant's security folder to the PSB Chief for review and signature
6. Return the folder to the Security Processing Unit

The Security Processing Unit analyst will:

1. Update the Applicant's clearance record in IPSS to "active"
2. Make of copy of the approval letter and retain it in the Applicant's security folder
3. Send the original, signed approval letter to the Licensee
4. File the folder on the active shelf

<u>If the contractor is not approved for clearance</u>:

The Adjudicator will:

1. Sign and date the Certificate of Investigation, stamp it "Denied", and retain it in the IT contractor's security folder
2. Sign and date the Form 79A, retain a copy in the Applicant's security folder, and send the original to OPM
3. Update and sign the Form 225, *File Summary Sheet*
4. Write a denial letter to the Licensee stating that the Applicant is not eligible for the requested clearance, including a brief summary of the cause
5. Write a letter to the Applicant, providing notice in accordance with 10 CFR 10.22, *Notice to Individual*, that states he/she is denied clearance in accordance with the criteria established in 10 CFR 10.11, *Criteria*
6. Deliver the Applicant's security folder to the PSB Chief for review and consent to the to the denial recommendation

The Branch Chief will review the contractor's security folder and confirm consent by signing the denial memorandum. The letter to the Applicant and the folder will then be forwarded to the Division of Facilities and Security Director for review and concurrence. The file is then forwarded to the Office of Administration Director for signature (as required by 10 CFR 10.22).

The Office of Administration Director reviews the contractor's security folder and signs the letter to the contractor. The security folder is then returned to the Security Processing Unit.

The Security Processing Unit analyst will:

1. Make copies of the letters
2. Retain 1 set of copies in the Applicant's security folder
3. Send the original signed denial letter to the Licensee
4. Send the original signed letter to the Applicant
5. Update the Applicant's record in IPSS
6. File the Applicant's security folder to the "Denied " shelf

12.6.1 Security Orientation Briefing

Applicants are required to be briefed by their employer, the Licensee, and are required to complete and sign an SF-312, *Classified Information Non-Disclosure Agreement.*

13.0 The Foreign Assignee Process

This section describes the requirements and procedures for issuing access authorization to Foreign Assignees who require unescorted access to NRC facilities.

Foreign Assignees are staff assigned from other countries to the NRC.

13.1 Overview

The Foreign Assignee process applies to individuals who will require building access authorization to NRC facilities. Foreign Assignees will not have logical access at any point during the duration of their stay with the agency.

The Foreign Assignee process does not include preliminary checks or a background investigation conducted by the PSB. The required checks are conducted by the FSB.

13.2 Request for Access Authorization

The International Programs Manager in the Office of International Programs will complete NRC Form 70A, *Request for Name Check*, and a security plan and submit the completed documents to the FSB.

13.2.1 Create a Record in the Integrated Personnel Security System (IPSS)

The Security Processing Unit analyst will:

1. Login to IPSS
2. Under "Create a New Person", generate a SSN for the Applicant and enter the Applicant's full name. If there is no middle name, enter "nmn"
3. Select "Create" to begin entering the Applicant's personnel security record. Ensure that the fields in the following sections pertaining to an individual's personnel security record are completed. (See Appendix D for details on the fields in each IPSS section)
   - Personal Data
   - Aliases
   - Employment Data
   - INS Info
   - Documents & Forms
   - Clearances/Access
   - Security checks
   - Investigation Data

13.3 Perform Pre-Employment Checks

FSB will conduct name checks with various divisions within the CIA and FBI for the individual specified on NRC Form 70A.

13.4 Physical Security Plan

FSB will receive a security plan from the International Programs Manager. The DFS Director will be required to concur with the documented security plan.

The FSB will conduct a physical security check of the office space assigned to the Foreign Assignee ensuring the space there is no remaining classified information in the designated office area and that the office space and equipment do not have access to the local area network (LAN).

13.5 Issuance of Credential (NRC ID Badge)

The Foreign Assignee must report to NRC to be issued a badge which indicates that he/she must have no access to classified information. The Foreign Assignee will be informed by his/her project officer of the date and time to report to NRC for a photo and when the badge can be picked up. The Foreign Assignee must bring two approved certificates of identity.

13.5.1 Create a record in the PCI system

NRC Project Officer directs the new Foreign Assignee to the PSB. The Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct
6. Click "Save" and then click "Yes" to confirm sponsorship
7. Click "Enroll Person" and search the Applicant

8. Click on the Applicant's name to open the Applicant's record
9. Click the "Biometrics" tab
10. Capture the Applicant's biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant's two I-9 documents
13. Upon verifying all the required information is both captured and valid, click "Save" and then click "Yes" to confirm enrollment

The Foreign Assignee must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

Foreign Assignees receive a temporary badge until their PIV card is ready for issuance.

13.5.2 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

13.5.3 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the

appearance of the individual matches the picture being printed on the PIV credential.

- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall ensure that the Applicant's PIV credential has a blue line in Zone 15 indicating that the Applicant is a Foreign Assignee.

The Issuer shall ensure that the Applicant's PIV credential has their correct office location (i.e. HQ, RI, RII, etc.) in Zone 17.

The Issuer shall ensure that the Applicant receives a badge with NC in Zone 4: Clearance Designation, indicating that the individual has no clearance and he/she must have no access to classified information.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request
- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

13.5.4 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

14.0 Special Situations Concerning Citizenship of Applicants

14.1 Applicants or Family Members Not US Citizens By Birth

Any Applicant who has a family member, spouse, prospective spouse, or a co-habitant that is not a US citizen by birth is required to complete the *Foreign Nationals Questionnaire* in addition to the SF-86 *Questionnaire for National Security Positions*.

The Applicant must submit a copy of his/her Naturalization Certificate or Citizenship Certificate with the completed security package.

The Adjudicator will call the Applicant to clarify foreign activities, interests, and contacts as part of the suitability determination process.

14.2 Access Authorization for Dual Citizens

A Dual Citizen is a U.S. citizen who is also a citizen of another country.

Pursuant to NRC MD 12.3, *NRC Personnel Security Program Handbook*, a dual citizen may be processed for access authorization when the need is adequately supported and investigative coverage in the United States can be obtained for the immediate 10-year retrospective period.

The Adjudicator will call the Applicant to clarify foreign activities, interests, and contacts as part of the suitability determination process.

14.3 Access Authorization for Non-US Citizens

Pursuant to NRC MD 12.3, *NRC Personnel Security Program Handbook*, and as provided for in Executive Order 12968, *Access to Classified Information*, where there are compelling reasons in furtherance of the NRC's mission, individuals who possess a special expertise may, at the discretion of the Executive Director for Operations (EDO) or the Deputy Executive Director for Management Services (DEDM), be granted access authorization with access to classified information limited to the specific programs, project, contracts, licenses, certificates, or grants for which there is a need for access. Cases where clearance is granted to a foreign national are extremely rare.

Such individuals shall not be eligible for access to any greater level of classified information than the U.S. Government has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only if the previous 10 years of the subject's life have 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.

An interview with the Applicant must be conducted, to include the Applicant's—

- Statement and disclosure of national allegiance
- Intent as to permanent residence in the United States
- General attitude toward the United States vis-à-vis the country of the Applicant's current citizenship
- For dual citizens, eligibility and intention to maintain dual citizenship
- Previous civilian or military service with a foreign government.
- Family or other relatives abroad or employed by a foreign government

- The names and addresses of U.S. citizens who can furnish information as to the Applicant's background and activities outside the United States

A verbatim transcript or detailed summary of the interview will be maintained and provided to the Applicant upon request.

If the PSB concludes that adequate support exists to initiate the investigation, the pertinent records will be forwarded to the investigation agency. A Single Scope Background Investigation (SSBI) will be required for an “L” or “Q” access authorization.

14.4 Applicants Who are US Citizens Residing Overseas for More Than 7 Years

Applicants for employment with the NRC who are US citizens who have been residing overseas for more than 7 years can not be granted 145b (temporary) access. These Applicants must have a favorable suitability determination based on a completed OPM background investigation before being granted access authorization and NRC employment.

15.0 The Renewal Process

Renewal is the process by which a PIV Card is replaced without the need to repeat the full registration procedure unless FSB determines that the Applicant requires an updated photograph. The card issuer shall verify that the employee remains in good standing and personnel records are current before renewing the card and associated credentials. When renewing identity credentials to current employees, the NACI checks shall be followed in accordance with the OPM guidance.

The PIV Card shall be valid for no more than five years. A cardholder shall be allowed to apply for a renewal starting six weeks prior to the expiration of a valid PIV Card and until the actual expiration of the card. A new photograph of the Applicant will be taken if required by FSB. The card issuer will verify the cardholder's identity against the biometric information stored on the expiring card. The expired PIV Card must be collected and destroyed.

The same biometric data may be reused with the new PIV Card while the digital signature must be recomputed with the new Federal Agency Smart Credential Number.

The expiration date of the PIV authentication certificate and optional digital signature certificate cannot be later than the expiration date of the PIV Card. Hence, a new PIV authentication key and certificate shall be generated. If the PIV Card supports the optional key management key, it may be imported to the new PIV Card.

16.0 Changes to Access Authorizations

16.1 Upgrades or Downgrades to Access Authorizations / Clearance Level

The Applicant's Office Director must approve the request for an access authorization upgrade or downgrade.

For employees and consultants, the Sponsor must complete an NRC Form 236, *Personnel Security Clearance Request and Notification*.

For contractors with clearance, contractors requesting clearance, and Licensees the Sponsor must complete and NRC Form 237, *Request for Access Authorization*.

For IT Level II contractors upgrading to IT Level I, the Sponsor must submit a Request for NRC Access Authorization (not the NRC Form 237) and a new NRC Form 89, *Badge Request.*

The PSB will follow the procedures appropriate to the access authorization or clearance level requested. PSB will require the Applicant to update his/her SF-86 via e-QIP if appropriate for the requested access/clearance type upgrade.

16.1.1 Create a record in the PCI system

Division of Facilities and Security directs the Applicant to the PSB. The Security Processing Analyst will:

1. Login to PCI
2. Click the "People Menu"
3. Click the "Add Person" button and enter the Applicant's information in the following fields
   - First Name
   - Middle Name (if applicable)
   - Last Name
   - Date of Birth
   - Agency
   - E-mail
   - Agency Clearance
   - Contractor Clearance (if applicable)
   - Location
   - Social Security Number
4. Click the "Position" tab at the top of the screen and select the Applicant [Affiliation] from the drop down
5. Click the "Sponsor" tab at the top of the screen and verify Sponsor data is pre-populated and correct

6. Click “Save” and then click “Yes” to confirm sponsorship
7. Click “Enroll Person” and search the Applicant
8. Click on the Applicant’s name to open the Applicant’s record
9. Click the "Biometrics" tab
10. Capture the Applicant’s biometrics electronically (photograph and fingerprints) and record their biographic data
11. Click the "Applications" tab
12. Capture the Applicant’s two I-9 documents
13. Upon verifying all the required information is both captured and valid, click “Save” and then click “Yes” to confirm enrollment.

The Applicant must present the same photo identification that was provided during the photo capture process and sign the Personal Identity Verification (PIV) Card Holder Responsibilities form in order to pick up their PIV card.

16.1.2 Badge Issuance- Applicant

The Applicant shall be notified via e-mail of when and where to report for the issuance of their PIV credential.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) at their designated time to collect the PIV credential.

The Applicant shall bring two valid identification documents to the PIV Issuer as specified in the I-9 document.

The Applicant shall provide an 8-digit numeric pin that he/she will be prompted to enter at the time of issuance. It is imperative for the Applicant to remember their unique 8-digit numeric pin number since only he/she will know the number and consequently must appear at an issuance station to have it reset.

The Applicant (now PIV credential holder) shall sign the Cardholder Agreement, attesting to their acceptance of the PIV credential and the related responsibilities.

16.1.3 Badge Issuance- Issuer

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential.

Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

- The individual shall present a state of Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the

appearance of the individual matches the picture being printed on the PIV credential.
- The PIV Issuer (or an authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

The Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV request
- The approval notice from the PIV Registrar
- The name of the PIV credential holder (Applicant)
- The credential identifier, the Agency Card Serial Number
- The expiration date of the PIV credential
- The signed acceptance form from the PIV credential holder

16.1.4 PACS Activation

The physical access to NRC facilities on the PIV credential will be activated through PACS post issuance.

16.2 Termination or Separation of Access Authorization

Pursuant to NRC MD 12.3, *NRC Personnel Security Program Handbook*, access authorization will be terminated and a security termination statement (NRC Form 136) must be signed when:

- An NRC employee, consultant, or contractor is separated from employment with NRC
- An individual who is not an NRC employee is separated for a period of 30 days or more from activities for which he or she was granted an access authorization
- Access authorization is no longer required

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

- Provide prompt notification of the termination of employment to the PSB
- Ensure that all classified and sensitive unclassified documents charged to the person are accounted for and properly disposed of
- Arrange for the immediate return of badges, passes, and other forms of official identification to the responsible NRC security point of contact
- Notify the Division of Facilities Security to remove the individual's name from all access lists

- Ensure that combinations are changed to which the person had access
- Arrange for the person's name to be removed from access permissions to critical or sensitive areas, such as telephone closets and computer rooms

Upon completion of a security termination statement, the signed copy of the security termination statement must be forwarded to the PSB.

16.2.1 Termination of Access Authorization in the Case of Disability

In the case of a disability of an individual when it is apparent that the disability will render them unable to perform their duties for at least 6 months, prompt notification must be made to the PSB and measures similar to those specified for voluntary or involuntary separation must be employed.

16.2.2 Termination of Employment in the Interest of National Security

A security clearance may be suspended or revoked when such action is considered to be in the best interest of national security in accordance with 5 U.S.C. 7532.

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

16.2.3 Termination of Contractor Unescorted Building Access, IT Access, Power Reactor Access, and SGI Access

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

16.2.4 PIV Card Termination

The termination process is used to permanently destroy or invalidate the use of the card, including the data and the keys on it, such that it cannot be used again. The PIV Card shall be terminated under the following circumstances:

- An employee separates (voluntarily or involuntarily) from Federal service
- An employee separates (voluntarily or involuntarily) from a Federal contractor
- A contractor changes positions and no longer needs access to Federal buildings or systems
- A cardholder is determined to hold a fraudulent identity
- A cardholder passes away

FSB personnel will ensure proper card revocation during PIV card re-issuance and termination. The termination process to destroy and invalidate the use of the PIV card is as follows:

- FSB personnel will revoke the physical PIV card
- FSB personnel will revoke the digital certificates on the PIV card

- Databases containing Federal Agency Smart Credential Number (FASC-N) values will be updated to reflect the change in status
- The Certification Authority (CA) will be informed and CRLs will be updated
- Online Certificate Status Protocol (OCSP) responders will be updated so that queries with respect to certificates on the PIV card are answered appropriately
- FSB personnel will revoke their physical access through PACS
- The PIV card is place in the FSB vault located on TWFN floor 6 until destruction
- FSB personnel will dispose the PIV cards locked in the FSB vault with the NRC's classified waste on a monthly basis

Upon PIV Card termination, the NRC enforces a standard methodology of updating systems of records to indicate employee termination, and this status is distributed effectively throughout systems used for physical and logical access to NRC facilities and resources.

If the PIV Card cannot be collected and destroyed, normal operating procedures are completed with 18 hours of notification.

16.2.5 Separation for Cardholders with Leave Without Pay Status

If a PIV cardholder separates from the agency with Leave Without Pay (LWOP) status for less than three months, the cardholder can retain their card with active certificates.

If a PIV cardholder separates from the agency with Leave Without Pay (LWOP) status for greater than three months, the cardholder will be directed to turn in their PIV credentials to the FSB. The FSB will deactivate the certificates on the card and suspend their physical access through PACS. FSB will retain the card in the FSB vault located on TWFN floor 6. After 2 years or once the card expires, whichever occurs first, the PIV card will be terminated, following the above procedures.

17.0 Reciprocity of Access Authorization

An access authorization may be granted by NRC if a pre-existing equivalent investigation is less than 7 years old for top secret and 10 years for secret, and meets the required level for the clearance requested. A current SF-86, *Questionnaire for National Security Positions* is also required.

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

17.1 Investigations from Another Federal Government Department

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

17.2 Reciprocity of "Q" and "L" Access Authorization

An NRC "Q," "L," and "L(H)" access authorization may be granted by NRC if a pre-existing equivalent investigation is less than 5 years old and is the required level for the clearance requested and less than 2 years break in service. A current SF-86 or SF-86C[2] is also required.

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

17.3 Personnel Security Branch Procedure

The Security Processing Unit performs the preliminary database checks as part of the initial suitability determination for the Applicant. The CVS and JPAS checks will identify existing clearances on the Applicant in OPM and DOD records. The CPCI check will identify existing clearances in DOE records.

If the Applicant has a current clearance from any federal government agency, the Adjudicator will call the agency security office to get verbal confirmation, or send a Clearance Verification Form via fax.

---

[2] The SF 86C is a certification document that allows the reporting of changes in previously reported information on the SF 86. This certification will be in lieu of completing a new SF 86 and will allow the individual to indicate that there have been no changes in the data provided on the most recently filed SF 86. Or it will allow the individual to easily provide new or changed information.

17.3.1 Favorable Response from Reciprocating Agency

Provided that a favorable response has been received from the agency, the investigation is the required level and less than 5 years old, and any break in service is less than two years, the Adjudicator can make an access authorization determination using the previous clearance and the Applicant's current security forms package received from HR (NRC Forms 236 and 176, OF-306, and reference checks).

The Adjudicator will update and sign NRC Forms 236 (granting access authorization) and 225 (file summary sheet), obtain PSB Branch Chief approval and signature on the file summary sheet, and notify HR via email that the Applicant can enter on duty with a clearance. (There is no requirement for approval of reciprocity clearances by the Director of the Division of Facilities Security and the Executive Office Director.)

The Security Processing Unit will update IPSS and file the Applicant's folder to the EOD shelf.

17.3.2 Previous Clearance Not Sufficient for NRC Position

If the previous investigation was for a lower level of clearance than is required for the current NRC position, the Applicant is notified to complete a security forms package and SF-86 via e-QIP. The PSB will then process the Applicant for a new investigation at the higher level.

17.3.3 Unfavorable Response From Reciprocating Agency

If the Adjudicator determines that the previous investigation is insufficient or the agency security office reports problems, reciprocation of access authorization will be denied. The Adjudicator can conduct a new investigation via the NRC procedures for new employees, or can make a determination that the Applicant is not suitable for the position at the NRC.

18.0 The Reinvestigation Program

The NRC reinvestigation program is designed to ensure the continued eligibility for access authorization of individuals employed by the NRC. The PSB must reevaluate the continued eligibility of individuals who have been granted access authorization.

18.1 Renewal of Access Authorizations

PSB will initiate a reinvestigation every 5 years for "Q" and "L(H)" (high public trust) clearances and every 10 years for "L" clearances. Table 15.1 summarizes the reinvestigation requirements for each security clearance/access type.

PSB will notify the individuals who are to be reinvestigated and the dates by which they are to complete the security forms packet. PSB will advise the former Chairman and Commissioners who have retained their NRC security clearances, congressional staff members, and contractor organizations directly.

Each individual must complete a security forms packet and return it to the PSB by the specified date. Contractor personnel should return forms through their security office.

A new set of fingerprint cards may be requested on a case-by-case basis.

Further investigative coverage may be undertaken on a case-by-case basis if the scheduled coverage is insufficient to obtain the required information. The investigation may be expanded as necessary to determine if access is clearly consistent with national security.

Upon favorable review of the investigation, PSB will provide a copy of the certification of investigation to be retained in the employee's personnel file.

If a contractor fails to submit forms by the specified date, the NRC security clearance or access for the contractor may be administratively terminated.

Table 15.1 – Summary of Reinvestigation Requirements

Security Clearances/Access Types	Reinvestigation Requirement
Q - Top Secret	SSBI-Periodic Reinvestigation (SSBI-PR) every 5 years[3]
L - High Public Trust (L(H)) (Secret)	National Agency Check with law and credit (NACLC) every 5 years
L - Secret	NACLC every 10 years
U - Top Secret	SSBI-PR every 5 years
R - Secret	NACLC every 10 years

[3] An exception is provided for the Chairman, Commissioners, and the Inspector General, who instead are subject to a Federal Bureau of Investigation reinvestigation in connection with their Presidential appointment

IT Level I	NACLC every 10 years
IT Level II	NACLC every 10 years
Building Access	NACI every 5 years
Daycare	CNACI every 10 years

19.0 Reinstatement of Access Authorization

Federal employees who have left the NRC for a period of time, had their access authorization terminated, and are now returning to duty, must request a reinstatement of their access authorization.

The requirements for reinstatement of access authorization at NRC depend on the length of time the employee had been separated from duty.

19.1 Reinstatement Within 90 days of Separation

If the federal employee was separated from duty at NRC temporarily and is returning within 90 days, they must complete an SF-86C. A PSB Adjudicator can make a determination to reinstate the employee's access authorization based on the SF-86C. The Adjudicator may request additional information as needed to make a determination.

The SF 86C is a certification document that allows the reporting of changes in previously reported information on the SF 86. This certification will be in lieu of completing a new SF 86 and will allow the individual to indicate that there have been no changes in the data provided on the most recently filed SF 86. Or it will allow the individual to easily provide new or changed information.

19.2 Reinstatement Greater Than 90 days of Separation

If the federal employee was separated from duty at NRC and is returning after 90 days but within the 2 year time frame, they must complete an SF-86C and provide new fingerprints. The Security Processing Unit will perform Fingerprint and name checks via PIPS, and a credit check. A PSB Adjudicator can then make a determination to reinstate the employee's access authorization based on the SF-86C and checks. The Adjudicator may request additional information as needed to make a determination.

19.3 Reinstatement After 2 Years of Separation

If the federal employee was separated from duty at NRC and is returning after 2 years, they must complete a new security forms package. The Security Processing Unit will perform all checks required for new employee suitability determinations. The Adjudicator can make a determination to reinstate the employee's access authorization based on the checks as long as the employee's existing OPM investigation is less than 5 years old. If a new investigation is required, the procedures are the same as for a new employee (the 145B Process.)

20.0 Sensitive Compartmented Information (SCI) Access

Requests for access to sensitive compartmented information (SCI) are not adjudicated by the PSB.

An NRC Office Director must write a letter recommending an employee for SCI access. PSB will forward the letter along with the employee's full SF-86 and background investigation to the Office of Nuclear Security and Incident Response (NSIR). If the Applicant's SF-86 is older than one year, a new SF-86 will be required.

NSIR will send the Applicant's information to the Central Intelligence Agency for approval. If approval is received, NSIR will send the approval letter to PSB for the Applicant's file. There is no update to IPSS required.

Appendix A - Information Types

Non-Classified Information

Non-classified information includes publicly available information with no requirement for an access authorization. However, non-classified information also includes information that must be protected from loss, misuse, or unauthorized access or modification. Such information requires an access authorization based on need-to-know.

Personally Identifiable Information (PII)
Information about an individual which can be used to distinguish or trace an individual's identity

Sensitive Information
Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Safeguards Information (SGI)
Safeguards information is a special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act to be protected. Safeguards information concerns the physical protection of operating power reactors, spent fuel shipments, strategic special nuclear material, or other radioactive material.

While SGI is considered to be sensitive unclassified information, its handling and protection more closely resemble the handling of classified confidential information than other sensitive unclassified information.

Sensitive Unclassified Non-Safeguards Information (SUNSI)
Sensitive unclassified non-safeguards information (SUNSI) is information that is generally not publicly available and encompasses a wide variety of categories (e.g., personnel privacy, attorney-client privilege, confidential source, etc.)

Information about a Licensee's or Applicant's physical protection or material control and accounting program for special nuclear material not otherwise designated as Safeguards Information or classified as National Security Information or Restricted Data is required by 10 CFR 2.390 to be protected in the same manner as commercial or financial information, i.e., they are exempt from public disclosure.

Classified Information

Information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

Classified information at the NRC and at the facilities it regulates is primarily of two types, National Security Information (NSI) and Restricted Data (RD)

National Security Information

Information classified by an Executive Order whose compromise would cause some degree of damage to the national security.

Restricted Data
Information classified by the Atomic Energy Act whose compromise would assist in the design, manufacture, or utilization of nuclear weapons.

Sensitive Compartmented Information (SCI)
Classified information concerning or derived from information intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

Appendix B - Information Classification

Confidential
Such material would cause "damage" or be "prejudicial" to national security if publicly available.

Secret
Such material would cause "serious damage" to national security if publicly available.

Top Secret
The highest level of classification of material. Such material would cause "exceptionally grave damage" to national security if publicly available.

Appendix C - Position Sensitivity Designations

MD 12.3 specifies the criteria for determining whether a person in an NRC position requires need-to-know access to certain types of information.

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

People in positions of a high degree of importance or designated as special-sensitive would have access to Secret or Top Secret-Restricted Data or Top Secret National Security Information. These positions include the following:

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

Positions of a Critical-Sensitive Designation

People in certain critical-sensitive positions which have one or more of the following characteristics:

- Access to Secret or Top Secret-Restricted Data or Top Secret National Security Information
- Access to Confidential Restricted Data involving broad naval nuclear propulsion program policy or direction (e.g., preliminary safety analysis reports, final safety analysis reports, and amendments thereto)

Positions of High Public Trust

People in positions of high public trust perform functions which include one or more of the following characteristics:

- Final approval of plans, policies, or programs that directly affect the overall operations and direction of the NRC
- Responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or the capability to access a computer system during its operation or maintenance in such a way that could cause, or that has a relatively high risk of causing, grave damage; or the capability to realize a significant personal gain from computer access
- Resident inspectors
- Such other duties requiring high public trust as determined on an as-needed basis by the Deputy Executive Director for Management Services (DEDM)

Positions of a Noncritical-Sensitive Designation

Persons in any NRC position who are not covered by any of the three position sensitivity criteria above, but who require access, on a need-to-know basis, to

SECRET and CONFIDENTIAL National Security Information or CONFIDENTIAL Restricted Data not related to broad naval nuclear propulsion program policy or direction (e.g., preliminary safety analysis reports, final safety analysis reports, and amendments thereto).

Table C-1. Summary of Position Sensitivity Designations

Position	**Type**	**National Security Information**	**Restricted Data**
Special Sensitive Positions of a High Degree of Importance or Sensitivity for Sensitive Compartmented Information	"Q"	TOP SECRET SECRET CONFIDENTIAL	TOP SECRET SECRET CONFIDENTIAL
Positions of a Critical-Sensitive Designation	"Q"	TOP SECRET SECRET CONFIDENTIAL	TOP SECRET SECRET CONFIDENTIAL
Positions of High Public Trust	“L(H)”	SECRET CONFIDENTIAL	CONFIDENTIAL
Positions of a Noncritical-Sensitive Designation	"L"	SECRET CONFIDENTIAL	CONFIDENTIAL

Appendix D - IPSS Fields

The Integrated Personnel Security System (IPSS) tracks and manages the personnel security (security clearances, investigative and access authorizations data) and badging data associated with the issuance of permanent and temporary badges; drug program data associated with Applicant drug testing and employee random drug testing; incoming and outgoing classified visit data; and facility clearance data associated with contractor companies that must have a facility clearance.

Personal Data

- Social Security Number
- Full name including suffix (Jr., Sr., etc.), if applicable
- Gender
- NRC Sponsor (for contractor employees: check the box and you will be prompted to enter the NRC Sponsor after the record is modified)
- Date of birth
- City of birth
- State of birth (select from list)
- Country of birth (select from list)
- Primary citizenship (select from list)

Select Modify to save data

Aliases

- Type of Alias (select from list)
- Full name of Alias
- Effective "From" date
- Effective "To" date (optional)

Select Modify to save data

Employment Data

- Employer (select from list)
- Employee type (select from list)
- Position title (if given)
- Employment Start date (entered when employment is approved)

Select Modify to save data

INS Info

- Country (select from list)
- Document Type (select from list)
- INS Authorization # (from copy of document)
- INS Effective Start Date
- INS Effective End Date (if applicable)

Select Modify to save data

Documents & Forms

- Document Type (SF-31 2, Questionnaires, Credit Letters)
- Description

- Date Signed
- Date Received

Select Modify to save data

Clearances/Access

Note: Access information should not be reflected on the same line as clearance request information. Access requests and clearance requests are two different types of requests. For example, 145b is the access requested and "L" is the clearance requested and should not be entered on the same page.

- Specialist Name (name of Adjudicator that case is assigned to)
- Date of Access Request (date access or security clearance packet received in Security)
- Remarks (temporary access or temporary IT access)
- Complete all necessary fields pertaining to the access being requested (Access Type, Access Status, and Access Status Date)
- Complete all necessary fields pertaining to the clearance being requested
- (Clearance Status, and Clearance Type and, once approved, Clearance Approval Date and Clearance Grant Date)

Select Modify to save data

Security checks

- Check Type (select from list)
- Date Requested
- Date Received
- Remarks (enter results of the checks)

Select Modify to save data

Investigation Data

- Name of Investigative Agency (select from list)
- Investigation Type
- Date to Investigative Agency
- When the investigation is completed and received in Security
- Date from Investigative Agency
- Date of Investigation (from the investigation Case Closing Transmittal)
- Date Sent to Specialist

Select Modify to save data

Appendix E - Suitability Checks

What is the Personnel Investigations Processing System (PIPS)?

The Personnel Investigations Processing System is an application managed by OPM to maintain its investigative data and process its cases. PIPS also provides direct access to OPM's records by approved agency security offices. A PIPS report would let you find out what type(s) of investigations a person has had in the past, that have been performed by OPM and/or to which OPM has had access.

Using PIPS, a security office can make on-line SII searches to determine if any investigations have been performed by OPM or other Federal agencies on the Applicant, and also access security clearance information through the CVS and the JPAS.

> The **Security-Suitability Investigations Index (SII)** is maintained by OPM and includes information from other federal agencies regarding investigations conducted.
>
> The **Clearance Verification System (CVS)** is also maintained by OPM and provides information on the status and the level of security clearance granted for federal employees and contractors. The system stores information on current, active, expired, revoked, and cancelled clearances granted by the agency clearance granting authority.
>
> The **Joint Personnel Adjudication System (JPAS)** provides "real-time" information regarding clearance, access, and investigative status to authorized DoD security personnel and other interfacing organizations.

What is the Central Personnel Clearance Index (CPCI)?

The Central Personnel Clearance Index (CPCI) is an automated data base maintained by the Department of Energy (DOE). It contains summary DOE clearance histories and status information on about 500,000 personnel and includes 174,000 active clearances.

Appendix F - Badge Colors by Clearance Designation

Badge Color	Clearance	Permissible Access to Classified Information (on a need-to-know basis)		Escort Required?
Blue	Q Clearance	TS/S/C TS/S/C	National Security Info Restricted Data	No
Yellow	L Clearance	S/C C	National Security Info Restricted Data	No
Red	No Clearance	NO ACCESS to Classified Information		No*
Orange	No Clearance	NO ACCESS to Classified Information		Limited Access and an escort may be required

*Unless the red badge is a visitor badge. Visitors given red badges must be escorted.