IRS HSPD-12 PIV I PROCEDURES MANUAL

1 Purpose

This document will describe the procedures to be followed by the Internal Revenue Service (IRS) for Personal Identity Verification (PIV) and the issuance of identity credentials (badges) for Federal employees and contractors in IRS facilities, effective October 27, 2005. These procedures are in accordance with the requirements to implement Homeland Security Presidential Directive 12 (HSPD-12) as set forth by the Federal Information Processing Standards Publication 201 (FIPS 201), dated February 25, 2005, and the Office of Management and Budget (OMB) Memorandum M-05-24, dated August 5, 2005.

2 HSPD-12 Overview

2.1 What is HSPD-12?

HSPD-12 was signed on August 27, 2004. This directive instructs all Federal agencies to develop a common procedure for secure and reliable forms of identification to be used by Federal employees and contractors to gain access to Federal facilities. This new procedure will enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy.

HSPD-12 directed the Department of Commerce to develop FIPS 201, which defines the standards to be used in developing a common procedure across all government agencies. In addition, the OMB issued M-05-24 which further clarifies the schedule and implementation plan for this standard, which will be implemented in two major phases – PIV-I and PIV-II.

2.2 PIV I and PIV II

The first phase, or PIV-I, is the focus of this document and must be implemented by all Federal agencies on October 27, 2005. It establishes the minimum requirements for a process to meet control and security of objectives of HSPD-12, including personal identity proofing, registration, and issuance. It does not address the interoperability objectives of PIV Cards and systems among departments and agencies, which will be addressed in PIV-II, with new cards being issued starting on October 27, 2006.

2.3 Applicability

Long-term - The IRS must conduct a background investigation; adjudicate the results, and issue identity credentials to all employees and contractors who require long-term access to IRS facilities and/or information systems. Long-term access is defined as equal to or greater than six (6) months. Candidates that apply for appointments that are long-term, will be required to undergo the PIV process defined in this manual.

Temporary - Temporary employees or contractors will be classified in two categories: Temporary short-term and Temporary long-term.

- **Temporary short-term** employees or contractors will be defined as working 180 calendar days or less. Fingerprints will be taken and the Federal Bureau of Investigation (FBI) Criminal check will be completed on temporary short-term employees or contractors, however a background investigation will not be required. Employees or contractors requiring routine access to the IRS for less than 180 days over a period of time may also be considered in this category. Individuals in this category will be issued a visitor badge. However, the IRS may make a risk-based decision depending on the risk level of the work to be performed, that additional screening and background checks may be required.

- **Temporary long-term** employees or contractors will be defined as working more than 180 calendar days. Individuals in this category will adhere to the same criteria as defined in the Long-term access paragraph above, and must adhere to the PIV process.

Contractors who will work more than 30 days and require access to the facility or to IRS systems will be required to adhere to the PIV requirements, depending on the risk level assessment.

Short-term - Short-term contractors, volunteers, commissions, and panels will be defined as working 1 month or less. For individuals in this category, a visitor badge will be issued and no FBI Criminal check or background investigation will be conducted. However, the IRS may make a risk-based decision depending on the risk level of the work to be performed, that fingerprints, additional screening, and background checks will be required.

Visitors - HSPD-12 does not apply to occasional **visitors** to the IRS facilities, such as volunteers or family members. Visitors will be issued a visitor badge.

Foreign Nationals – Contractors and sub-contractors and their employees may be allowed to work at the IRS if they are US citizens or have lawful permanent resident status. A foreign national is defined as a person who was born in a foreign country, is NOT a US citizen, and has a lawful permanent resident status. Background investigations for foreign nationals will be conducted on all contractors according to the procedures outlined in the Treasury Security Manual – TDP 71-10, Chapter 2, Section 2 - Contractor Investigations. IRS hiring policy states that an individual must be a US citizen in order to be considered for employment eligibility. Therefore, foreign nationals are currently not IRS employees.

2.4 Certification & Accreditation

The PIV processes outlined in this document for identity proofing and registration, as well as for issuance and maintenance of PIV Cards, will be submitted and incorporated in the Business Process Accreditation Template for approval and accreditation by the proper authorities within the IRS and the Department of the Treasury. All of the processes outlined here satisfy the requirements of FIPS 201 and OMB M-05-24. The requirements for this certification are outlined in the National Institute of Standards and Technology (NIST) Special Publication 800-79 (SP 800-79). The Designated Accreditation Authority (DAA) has given the IRS an Authorization to Operate (ATO) effective October 27, 2005.

3 Requirements for PIV-I

Requirements for personal identity verification are specified in Federal Information Processing Standards Publication 201 - Personal Identity Verification of Federal Employees and Contractors, issued by the National Institute of Standards and Technology (NIST). This standard contains requirements for PIV-I and PIV-II. An appendix to the standard contains two example identity proofing, registration and issuance process sets which meet the requirements for PIV: a role-based model and a system-based model. The role-based model is recommended for organizations which do not have a pre-existing PIV system.

3.1 Control Objectives

HSPD-12 established control objectives to establish what is meant by "secure and reliable forms of identification"; FIPS 201 expands those control objectives to the following set of high-level requirements:

- Credentials are issued to individuals whose true identity has been verified and after a proper authority has authorized issuance of the credential;
- Only an individual with a background investigation initiated or on record is issued a credential; If background check is not completed within 5 days, an interim credential can be issued based on a successful fingerprint check;
- An individual is issued a credential only after presenting two identity source documents, at least one of which is a valid Federal or State government issued picture identification document (ID);
- Fraudulent identity source documents are not accepted as genuine and unaltered;
- A person suspected or known to the government as being a terrorist is not issued a credential;
- No substitution occurs in the identity proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked against databases, is the person to whom the credential is issued;
- No credential is issued unless requested by proper authority;
- A credential remains serviceable only up to its expiration date. More precisely, a revocation process exists such that expired or invalidated credentials are swiftly revoked;
- A single corrupt official in the process may not issue a credential;
- An issued credential is not modified, duplicated, or forged.

3.2 Identity Proofing and Registration Requirements

Identity proofing is the process of providing sufficient information (to a PIV Registrar or trusted agent) to establish a person's identity. Identity registration includes the collecting and recording of relevant attributes of that person, and associating that information with the unique identifier of that person.

- The process shall begin with initiation of a National Agency Check with Written Inquiries (NACI) or other OPM or National Security investigation required for Federal employment. This requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI, or other OPM or National Security investigation required for Federal employment. Additional OMB guidance in M-05-24 states that, if the results of the NAC are not received in 5 days, the identity credential can be issued based on the FBI National Criminal History Check (fingerprint check).
- 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.
- The PIV identity proofing, registration and issuance process shall adhere to the principal 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.

3.3 Issuance and Maintenance Requirements

Issuance of a PIV credential includes creation and personalization of the credential and giving the credential (in person) to the Applicant after verifying that the individual who collects the credential is in fact the Applicant for whom the credential is intended.

- The process shall ensure completion and successful adjudication of a National Agency Check (NAC), NACI, or other OPM or National Security investigation as required for Federal employment. The PIV credential shall be revoked if the results of the investigation so justify. Additional OMB guidance in M-05-24 states that, if the results of the NAC are not received in 5 days, the identity credential can be issued based on the FBI National Criminal History Check (fingerprint check).
- At the time of issuance, verify that the individual to whom the credential is to be issued (and on whom the background investigation was completed) is the same as the intended Applicant/recipient as approved by the appropriate authority.
- The organization shall issue PIV credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing.

4 PIV-I Roles

With the implementation of FIPS 201 requirements, several new roles have been identified that are key elements of the PIV process. These new roles are described below and are also outlined in the example role-based model included in Appendix A. of FIPS 201.

4.1 Role Requirements

One of the requirements of the PIV identity proofing, registration, and issuance process is to ensure that the principal of separation of duties is met. In order to distinguish a clear separation of responsibilities between roles, the IRS will adopt the first four role names and descriptions that are outlined in the FIPS 201 Section A.1.1.1 Roles and Responsibilities.

Named individuals within the existing IRS and contractor organizations may be designated to a role that they will perform in the PIV process. These individuals must complete training in their designated role. A list of individuals within each role will be maintained by the IRS HSPD-12 Program Office. This list will be distributed to each of the card issuing facilities. Individuals may be designated to more than one role, however they may not perform more than one role for a single PIV Card Applicant (as defined below). All individuals performing a PIV role must have a completed and favorably adjudicated NACI check on record.

Per the FIPS 201 requirements, each PIV role performed will be mutually exclusive from any other role performed for each PIV Card Applicant. In the FIPS 201 requirements, Appendix A, an example of a Role Based Model is illustrated as an approved example of PIV Identity Proofing, Registration and Issuance. The IRS will be adopting a similar model, using the roles described in the FIPS 201 requirements Appendix A, however slight variations have been made to accommodate the specific business needs of the IRS. The variations in the IRS model adopt the use of an approved identity proofing and registration process as outlined in Section 2.2 of the FIPS 201 requirements and satisfy the PIV objectives and requirements.

4.2 Role Descriptions

The following describes the five critical roles that will be employed at the IRS for identity proofing and issuance: The PIV Sponsor, Registrar, and Issuer will be named individuals that have been certified and trained to perform their designated role. A list will be maintained for individuals serving in these roles and a record of their completed background investigation will be kept on file. The PIV Applicant Representative is also a new IRS role that serves to protect the Applicant's rights.

4.2.1 Applicant

This is the individual to whom a PIV credential potentially needs to be issued.

4.2.2 PIV Sponsor

This is the individual who substantiates the need for a PIV credential to be issued to the Applicant, and provides sponsorship to the Applicant. The PIV Sponsor requests the issuance of a PIV credential to the Applicant.

4.2.3 PIV Registrar

This 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 initial issuance of a PIV credential to the Applicant.

4.2.4 PIV Issuer

This 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. The PIV Issuer is also responsible for maintaining records and controls for PIV credential stock to ensure that stock is only used to issue valid credentials.

4.2.5 PIV Applicant Representative

The PIV Card Applicant Representative is the entity that represents the interests of current or prospective Federal employees and contractors who are the Applicants for PIV Cards. They should represent the privacy concerns of applicants, assist an applicant who is denied a PIV Card because of missing or incorrect information in an Identity Source document, or act as a surrogate for an applicant that is not available for performing required actions.

5 *New PIV Forms*

With the implementation of the new PIV process, two new forms and an informational guide have been developed by the IRS. These forms will assist in tracking and documenting the PIV process through the various roles / organizations and provide assurance that all of the proper steps have been taken in meeting PIV I compliance. A description of each of these documents is provided in this section and copies of the forms are provided in Appendix B. All of these documents satisfy the privacy requirements outlined in Section 8 of this manual and will adhere to current IRS record retention policies.

5.1 PIV Applicant Rights and Responsibilities Guide

The PIV Applicant Rights & Responsibilities Guide (Applicant Guide) will be given to each individual at the start of the hiring process. The Applicant Guide explains what to expect in the PIV process, the Applicant's privacy and appeal rights, and who to contact for questions. A copy of Applicant Guide is included in Appendix B.

5.2 PIV Request Form

A new tracking form will be utilized to ensure that each step in the process is completed satisfactorily. The PIV Request Form will be signed by each of the roles mentioned in Section 3.1.2 and will document the authorizations for sponsorship, registration, and issuance of the PIV credential for the life of the credential. Finally, the new form will allow for a signature from the Applicant, indicating that important information about his/her rights was provided and that his/her permission to participate in the PIV process was granted.

The PIV Request Form will be checked by the PIV Issuer, who will ensure that the requirement for separation of duties has been met and that all of the steps in the process were completed. The completed PIV Request Form will authorize the Issuer to create a PIV credential for the Applicant. The original, signed PIV Request Forms will be stored in Physical Security in a secure location and follow current security and privacy procedures. The PIV Request Forms will be kept for the life of the PIV credential itself.

5.3 Contractor Risk Assessment Checklist

This new form will be used to document and communicate the risk for the type of background investigations to be performed on contractors. All new investigation packages will require this checklist to be submitted to the Procurement Sponsor Team. A copy is included in Appendix B.

6 PIV-I Processes

The PIV-I processes contain detailed step-by-step instructions and are organized into three main process streams: 1) Identity proofing and registration, 2) PIV Card issuance, and 3) PIV Card maintenance. This structure follows the organization of the FIPS 201 requirements and together, they form the entire PIV life cycle for employees and contractors.

Throughout these processes, identity documents, investigation paperwork, and the PIV Request Form are passed through various organizations performing specific roles in the process. In every instance where an Applicant's private information is indicated on a form, the document must be transferred in a secure manner to protect the Applicant's privacy rights. Secure manner includes the following forms of transmission: hand-delivery, secure e-mail, fax (if the fax machine is in a secure location), courier, registered USPS mail, and UPS delivery.

6.1 Identity Proofing and Registration

6.1.1 New Employees

The processes of identity proofing and registration are applied to Applicants for employment with the IRS as part of the hiring process, so that successful Applicants can be issued credentials promptly at Entry On Duty (EOD) for facility access. Specifics of the hiring process at IRS vary depending on the type of position being filled, and as a result there are slight variations in how the PIV identity proofing and registration is performed. The elements of identity-proofing and registration processes which are common to most types of hiring are presented here, with indications given where variations occur in some hiring types. It is important to ensure that in all hiring situations, the NACI or other relevant background investigation is initiated at least 5 days prior to Entry on Duty (EOD). All applicable existing privacy and record retention policies will be applied to this process. Refer to the Section 8 Privacy Considerations.

Step 1: Applicant Applies for Federal Credential/Position - The Applicant applies for a position by submitting an application for a current vacancy announcement. The submission can be online (via CareerConnector), or a paper application via mail or fax. The vacancy announcement includes wording on the requirements for a PIV credential, the privacy statement, as well as wording that the position requires a probationary period.

Step 2: Initial Assessment of Qualification - In most cases Human Resources (HR) makes an initial assessment of the Applicant's qualifications relative to the vacancy announcement/position requirements. This can be done based on the application materials, through a test administered online (CareerConnector), or through a test/assessment administered in person at an IRS test site. In this step, HR determines whether to proceed to perform identity proofing and take fingerprints for a Fingerprint Check.

Step 3: Initiate PIV Request Form - In a face to face meeting with the Applicant, the Registrar (HR) initiates the PIV Request Form for the Applicant. The Registrar provides the Applicant Guide to the Applicant. The optional information in Section 1 of the PIV Request Form is not needed, since that information is collected as part of the fingerprinting process (Step 5). The Applicant's signature will verify that he/she agrees to undergo the PIV process. If the Applicant has not already received the Applicant Guide describing the PIV process, a copy will be provided at this step. The Applicant Guide will contain information about the Applicant's appeal rights, privacy, and contact information. Section 1 of the form is completed and then signed by the Applicant. The Sponsor signature will be left blank until the final determination is made in a later step.

Step 4: In-Person Identity Proofing - The Registrar (HR) checks a state or federal government-issued picture ID, as well as one other form of ID in accordance with the I-9 process. The I-9 form and other necessary forms are verified. If the Applicant does not present a valid ID, the Applicant is escorted from the building. If a document is thought to be fraudulent, the Registrar will notate on the PIV Request Form that there is reason to suspect the document is fraudulent and the reason why. The Applicant will be notified at a later time that the identity documents were not valid. ID verification is logged on the PIV Request Form by the Registrar.

Step 5: Obtain Fingerprints - The Registrar (HR) verifies that the Applicant completes the Consent for Fingerprint Check form and the Declaration for Federal Employment. Fingerprints are taken from the Applicant using Livescan or Ink & Roll. If any further information relating to PIV is required from the Applicant, notice is given at this point with a suspense date for providing the missing information. Please refer to IRM 1.23.3 Background Investigations Guide for additional details on how to take fingerprints.

Step 6: Initiate FBI Criminal Check - Fingerprints are transmitted to OPM by the Registrar (HR), in most cases by electronic means. The PIV Request Form is updated by the Registrar with the date that the FBI Criminal check was initiated. Please refer to IRM 1.23.3 Background Investigations Guide for additional details on how to transmit fingerprints to OPM.

Step 7: Results of Checks - If the FBI Criminal check results are favorable, the results are entered on the PIV Request Form and the form is signed by the Registrar. If the results are non-favorable, the results are entered on the PIV Request Form, and the form is signed by the Registrar. Please refer to Policy 67, Objections and Passovers on Suitability Issues and Suitability Adjudicative Determination Procedures for additional details on how to adjudicate the FBI Criminal check results.

Step 8: Decision on Hiring/Need for Credential - HR and/or Business Unit makes a determination on hiring, including: certifying the Applicant, determining suitability, evaluating selection criteria, and making the job offer. A decision to make a job offer requires a favorable outcome from the FBI criminal check.

In addition, any concerns over a fraudulent identity document that were noted on the PIV Request Form, must be resolved prior to making a job offer. If the fraudulent identity document question has not been resolved, HR and/or Business Unit must contact the Applicant and ask them to correct the situation by bringing in a valid identity document and having it re-verified. When the Applicant presents a new, valid identity document, HR and/or Business Unit will update the notation on the PIV Request Form that the suspected document has been cleared.

In the event of an unfavorable decision on hiring, HR retains the forms and the application information at least through the duration of the hiring season.

Step 9: Initiate Background Investigation - The Registrar (HR) initiates the Background Investigation – National Agency Check with Inquiries and updates the PIV Request Form. The package of investigation paperwork, including the required form SF-85, SF-85P, or SF-86, is mailed to OMB or NBIC depending on the type of background investigation. NBIC provides notification of receipt of the package back to the Registrar. Please refer to IRM 1.23.3 Background Investigations Guide for additional details on how to initiate a Background Investigation.

Step 10: Final Determination - The Sponsor (usually another HR official within the same Employment Branch office as the Registrar) signs the PIV Request Form indicating a final determination on the validity of a need for a PIV credential.

Step 11: Notify Issuer - The Registrar verifies that all applicable sections of the PIV Request Form have been completed properly and that 5 days have elapsed from the initiation of the background check. The Registrar then forwards the form via secure means to the Issuer. The Issuer (Physical Security) is notified by the Sponsor (HR) to initiate credential issuance, at a date no earlier than 5 days from the initiation of the background investigation.

Step 12: Complete Background Investigation - When the Registrar is notified that the final adjudication of the background investigation has been completed; the Registrar will notify the Issuer of the final disposition in a secure manner.

6.1.2 New Contractors

Individuals assigned to perform work under IRS contracts, and who require physical access, or access to systems and information, need identity credentials. The process of identity proofing and registration for these contractors varies depending on the type of work being performed, and the contractor organization. The elements of identity proofing and registration which are common to most types of contractors are presented here, with indications given where variations occur. All applicable existing privacy and record retention policies will be applied to this process. Refer to the Section 8 Privacy Considerations. In this section, the Contracting Officer's Technical Representative (COTR) is the person responsible for assembling and transferring information to and from the Sponsor and the Registrar, however this individual is not designated to perform either of these roles. The COTR may reside in any organization within the IRS that manages a contract for services.

Step 1: Apply for Credential - The Applicant/employee submits a request through the contractor organization for a credential under a valid contract/task order to the COTR for that contract. The applicant provides identity information (First Name, Middle Initial (MI), Last Name, Social Security Number (SSN), contractor company name, contract number) to the COTR.

Step 2: Validate Need and Risk Level - The COTR validates the need for a credential under the contract/task order terms and statement of work, and makes a determination of the appropriate risk level and investigation type based on the duties to be performed. The COTR completes a risk assessment checklist for the Applicant which includes the identity information from Step 1, as well as the Risk Level/Investigation Type, Contractor Duties, and Duty Location/Issuing Office. The risk assessment checklist is included in the Appendix.

Step 3: Initiate Investigation Request - The COTR initiates a PIV Request Form for the Applicant and provides the Applicant with the PIV Applicant Guide. The Applicant Guide will contain information about the PIV I process, the Applicant's appeal and privacy rights, and contact information. The COTR completes the Applicant Information (Section 1) of the PIV Request Form, and obtains the Applicant's signature, leaving the Sponsor signature line blank.

Step 4: Initiate Investigation Record - The COTR sends the PIV Request Form and risk assessment checklist to the Procurement Sponsor Team (PST) using secure means to initiate the investigation record in the Procurement Background Investigation Process (PBIP) system, and provides the following information:

- Standard Employee Identifier (SEID) of the COTR or Point of Contact in the Automated Background Investigation System (ABIS).
- Fingerprinting source: IRS Human Resources (HR) and / or External Trusted Agent (ETA).

Step 5: Create Investigation Record in PBIP - The PST, acting as the Sponsor, initiates an Applicant record in PBIP. The PST signs the PIV Request Form as the Sponsor, and returns the form to the COTR.

Step 6: Perform Identity Proofing and Fingerprinting - When IRS (HR) performs the function as Registrar for identity proofing and fingerprinting, the COTR will contact HR to schedule an appointment for the applicant. The COTR will also forward the PIV Request Form, either in person or via secure mail, to the appropriate HR office. (Note: The PIV Request Form should never be brought to the appointment by the applicant as the chain of custody of the document would no longer be secure.) The COTR notifies the Applicant of the time and location of the appointment and the required identity documents that must be brought by the applicant to the appointment.

- In a face-to-face meeting with the Applicant, the Registrar (HR) checks a state or federal government-issued picture ID, as well as one other form of ID from the list of documents accepted per the I-9 (Employment Eligibility Verification) process.
- If the Applicant does not present a valid ID the identity proofing and fingerprinting does not proceed. The applicant is informed of the acceptable forms of ID and is given the opportunity to reschedule the appointment.
- If any document is thought to be fraudulent, it will be notated on the PIV Request Form that there is reason to suspect the document is fraudulent and the reason why. The Applicant will be notified at a later time that the identity documents were not valid.

The Registrar (HR) completes and signs Section 2A of the PIV Request Form. The Registrar (HR) verifies that the Applicant has completed Form 12333, Consent for Fingerprint Check. HR sends the PIV Request Form and Form 12333 to Personnel Security and Investigations (PS&I) Contractor Program via secure mail.

HR will obtain fingerprints from the Applicant using Livescan or Ink & Roll. HR will transmit fingerprints directly to OPM or will send the FD 258 ink & roll fingerprint card directly to PS&I Contractor Program to ensure that a secure chain of custody of the print images. PS&I will forward the fingerprint cards to OPM.

HR emails the PST with the Registrar's SEID, together with the Applicant information: First Name, MI, Last Name, the last four digits of SSN, Contract Number, and date of Identity Proofing/Fingerprinting (IPFP). The PST enters the Applicant fingerprint information and Registrar's SEID into PBIP. HR copies the COTR and PS&I on this email to inform the COTR that the fingerprints have either been transmitted to OPM or the card has been sent to PS&I.

If identity proofing and fingerprints are performed by an accredited external trusted agent (ETA) (e.g. contractor organization's security office, police department), the ETA performs the Registrar role for this step. (Note: the process definition for this case is not complete, but in outline should be similar to the

above. In a face-to-face meeting with the Applicant, the ETA checks a state or federal government-issued picture ID, as well as one other form of ID in accordance with the I-9 process. ID verification information is sent to the COTR. The ETA obtains fingerprints, and the fingerprints are forwarded either directly to PS&I, or to the COTR for inclusion with the background investigation request package which will be sent to PS&I.

Step 7: Review Package for Completeness - The COTR reviews the background investigation paperwork completed by the Applicant to ensure it is complete. If necessary, it is returned to the Applicant for correction; the Applicant returns the corrected package to the COTR.

Step 8: Upload to ABIS - The COTR uploads the investigation request information into the PS&I Automated Background Investigation System (ABIS), which will also generate a background investigation request memorandum.

Step 9: Forward to NBIC - The COTR will assemble the background investigation request package which will include forms completed by the Applicant: SF-85P or SF-86, copy of Form I-9, Form 13340 Fair Credit Reporting Act, a copy of the email from HR regarding the fingerprints, the PIV Request Form with original signature of Applicant, the risk assessment checklist, and the background investigation request memorandum. The COTR mails the background investigation paperwork package to PS&I Contractor Program.

Step 10: Notify PST Package Sent - The COTR emails the PST with the "Sent to PS&I" date.

Step 11: Update "Sent to PS&I" Date - The PST enters the "Sent to PS&I" date into PBIP.

Step 12: Initiate Background Investigation - PS&I will initiate the background investigation for the appropriate risk level, with a minimum of NACI. The date and type of background investigation will be recorded on the PIV Request Form. The package of investigation paperwork, is mailed to OMB or PS&I - NBIC depending on the type of background investigation. PS&I - NBIC provides notification of receipt of the package back to the Registrar. Please refer to IRM 1.23.3 Background Investigations Guide for additional details on how to initiate a Background Investigation.

Step 13: Decide Interim Approval - PS&I makes a determination on Interim Approval. The investigation interim decision (not applicable on revalidation and high risk root systems access and/or system administrator positions) is entered by PS&I into ABIS. PS&I Contractor Program completes and signs the relevant portions of the PIV Request Form, verifies that all applicable sections of the PIV Request Form have been completed properly, and that 5 days have elapsed from the initiation of the background check. PS&I Contractor Program forwards the

information (interim approval letter if favorable and scanned copy of the PIV Request Form) to the COTR and the PST via secure email. The PST enters the investigation decision date and the Approval/Denial Registrar (AD) SEID into the PBIP system. (Note: PS&I Contractor Program will retain the original PIV Request Form until the final investigation is completed.)

If there was a notation on the PIV Request Form that a fraudulent identity document was suspected, interim access will be denied. In this case, PS&I will initiate the necessary contacts to verify the suspected fraudulent document, contact the subject for a personal interview, if necessary, and forward a report to PS&I National Security Programs to adjudicate the issue.

- **If Interim Approval is granted** - The COTR schedules an appointment for the contractor with the Issuer to issue a credential. The COTR saves the interim approval memo and forwards the interim approval memo and a scanned copy of the PIV Request Form to the Issuer via secure means.

- **If Interim Approval is not granted** - PS&I Contractor Program notifies the COTR and the PST via secure email. The PST enters the decision date into PBIP. PS&I will continue the investigation until an interim approval or Proposal to Deny is determined.

Step 14: Decide Final Approval - PS&I conducts the adjudication process and makes a determination on Final Approval and notifies the COTR and the PST via secure email.

- **If Final Approval is granted**: - PS&I Contractor Program or National Security Programs (NSP) notifies the COTR and the PST by email attaching the final approval memorandum and the PIV Request Form with background information completed.. PST enters the Final Approval date into PBIP. PS&I then forwards the original signed PIV Request Form to the Issuer (Physical Security) in a secure manner.

- **If Final Approval is not granted**: - NSP notifies the COTR and the PST of the Proposal to Deny Access and mails a memo to the COTR with a package for delivery to the Applicant/Contractor. The PST enters the Proposal to Deny date into PBIP. The COTR delivers the package to the contractor and notifies NSP & the PST of the delivery date. NSP sets a 15 day tickler starting from when the contractor receives the Proposal to Deny package. At the end of the 15 day waiting period, NSP completes the adjudication for approval or denial.

    - **If Approved** – NSP notifies the COTR of the final approval and mails a memo to the COTR with a package for delivery to the Applicant/Contractor. NSP emails the PST of the decision. The PST enters the decision into PBIP.

- **If Final Denial -** NSP notifies the COTR of the final denial and mails a memo to the COTR with a package for delivery to the Applicant/Contractor. NSP emails the PST of the decision. The PST enters the Final Denial date into PBIP. NSP returns the final background investigation report to PS&I Contractor Program. PS&I Contractor Program completes and signs as the Registrar the background investigation section of the PIV Request Form. PS&I Contractor Program forwards by email a scanned copy of the completed PIV Request Form to the COTR and the PST. PS&I Contractor Program will mail the original completed PIV form to the Issuer (Physical Security) in a secure manner.

Step 15: Notify Issuer of Decision - The COTR notifies the Issuer (Physical Security/Mission Assurance) of Final Approval or Final Denial. The COTR forwards the PIV Request Form to the Issuer via secure mail.

6.1.3 Current Employees and Contractor Employees

Current Employees and Contractor Employees are required to have a successfully initiated or adjudicated background investigation on file by October 27, 2007 (October 27, 2008 for employees with more than 15 years of service). The IRS will continue to use existing processes in place prior to October 27, 2005, for re-issuance or replacement of employee and contractor badges.

6.1.3.1 Employees

The IRS currently tracks background investigations for employees through SETS. A bi-weekly report will be generated from SETS to determine which employees do not have a background investigation initiated or completed. These employees will then be contacted to confirm that a background investigation was not completed. They will be informed of the process and time frame for completing these records, or in some cases initiating the NACI or other applicable investigation. If the record of investigation was completed, the OPF should be requested to verify completion of a background investigation. After all employees have been notified once, the SETS report listing all employees without an initiated or adjudicated background investigation should be run again with a reconciliation against the first report. Initial research has shown that the percentage of employees without a current background investigation is well under 1%, so no significant deviation from current processes is needed to insure that all employees have a background investigation on file by the October 27, 2007 and 2008 dates.

Note: With the implementation of PIV I, there is now an ongoing process in place to ensure that all new employees have the proper background investigation initiated. Thus the number of employees without a background investigation will not increase. The bi-weekly SETS report is the control mechanism for insuring that the current PIV I processes are working and that all IRS employees will have a background investigation completed by the October 27, 2007 and 2008 dates.

6.1.3.2 Contractors

Every six months, the COTR must certify that the contractor ID is still needed. This is supplied in writing to the Physical Security office.

For Contractors, all contracts will include a clause for insuring that all personnel employed on the contract have a successfully adjudicated background investigation on file. Insuring that this clause is included must start immediately and Procurement is aware of this requirement.

Additionally, all current contracts need to be reviewed to see which contracts extend beyond October 27, 2007. The companies with which these long term contracts are in place with must be contacted and informed of this requirement. A

plan to insure that all personnel working on IRS contracts have the adjudicated background investigation complete by October 27, 2007 must be in place for each long term contract.

6.2 PIV Card Issuance

Step 1: Notify PIV Issuer - For new hires, HR will provide a list of selected candidates to the Issuer (Physical Security) prior to EOD. The PIV Request Forms for all of the candidates on the list will also be provided to the Issuer.

For contractors, the COTR or a designated individual within the Procurement organization will send a completed and signed PIV Request Form to Physical Security. The identity proofing and registration steps on the PIV Request Form must be completed.

Step 2: Confirm PIV Request - The Issuer **(**Physical Security) will verify the signature of the Sponsor on the PIV Request Form, approving the issuance of a PIV Card to the Applicant. Physical Security will verify that the fingerprint check was completed, that the fingerprint check was completed at least 5 days prior to the date that the card will be issued, and that the Registrar has approved and signed the PIV Request Form, authorizing the issuance of a PIV credential. The Issuer will verify that the Sponsor and the Registrar approvals are from different individuals and that they are on the list of IRS certified Sponsors and Registrars.

Step 3: Appear in Person - The Applicant will appear in person to the badge issuance station (physical security). The Applicant will present one form of identification document that is a state or Federal government-issued picture identity document. This identity document must also be the same document that was presented to the Registrar and recorded on the PIV Request Form,.

Step 4: Check Identity - The Issuer will verify that the Applicant appearing in person is the same person as recorded on the PIV Request Form. This will be done by checking the name, picture, and identification number on the identification document presented by the Applicant, and verifying that it is the same as the name and identification number on the PIV Request Form. The Issuer will also visually verify that the picture on the state or federal government-issued ID is the same as the Applicant appearing in person.

Step 5: Create Badge - The Issuer will take a picture of the Applicant. The Issuer will then create a PIV credential containing the picture of the Applicant. The issue date is recorded in the system. An expiration date that is equal to 5 years from the issue date is recorded in the system. For contractors, the expiration date of the badge will be the lesser of one year from the issue date or the contract expiration date.

Step 6: Issue PIV Credential - The Issuer will then sign and date the PIV Request Form and give the PIV badge to the Applicant. If applicable, the Applicant may also receive a proximity card for automated access to a designated IRS facility equipped with a card-entry system.

Step 7: Receive PIV Credential - Applicant will receive the badge and verify the information is accurate. Applicant will then sign the PIV Request Form to acknowledge that the badge was received.

Step 8: Store PIV Request Form - The Issuer will then store the PIV Request Form in a secure container in accordance with local procedures.

6.3 PIV Card Maintenance

PIV Card maintenance includes all of those activities that can take place after the PIV Card is issued. Some of these activities include a damaged card that needs to be replaced, a stolen card, and a name change due to marriage or divorce. Other activities included in this category include the revocation of a card due to separation from the IRS due to retirement, or resignation, or dismissal. A third class of activities occurs when a badge is not needed for a period of time, as with a suspension, furlough, or leave while actively employed.

6.3.1 PIV Card Re-Issue (Lost, Damaged, Stolen or Name Change)

Step 1: Identify Need for Replacement - The employee or contractor identifies the need for a replacement card. An employee would notify their manager. A Contractor would notify their COTR who will then contact Procurement. A core group within the Procurement office will perform this function for contractors. The employee's manager or the Procurement contact will be the Sponsor for the employee.

Step 2: Complete PIV Request Form - The Sponsor completes the Sponsor section of the PIV Request Form. Forms 5520, 6028, or a comparable form must also be completed by the Sponsor for name change, lost card, or stolen card. . For a name change, the employee must show the Sponsor, a valid legal document authorizing the name change, such as a new driver's license, a marriage certificate, a divorce decree, or other court document. If a new badge is required, a new PIV Request Form must be completed. There will be one PIV Request Form per badge issued. The Sponsor will sign and date the PIV Request Form in the appropriate blocks.

Step 3: Forward PIV Form to Issuer - The PIV Request Form must be taken to Physical Security (Issuer) in a secure manner. The Sponsor must either walk the form to Physical Security or send it to security via secure mail.

Step 4: Identify Employee – The Physical Security Department (Issuer) must verify the identity of the individual using 2 valid forms of identification and verify that it is the individual who originally possessed a badge. Physical Security would also verify that the original badge had not expired.

Step 5: Verify NACI or equivalent on Record - Physical Security must verify with Personnel Security, or through the SETS application, that there is a NACI or equivalent initiated or completed. If there is a NACI record date on file, then the badge may be issued.

If the individual was an employee or contractor starting on or after October 27, 2005, then the NACI should be on file or should have been initiated. The badge may be issued providing the FBI Criminal check has been completed.

Step 6: Issue Replacement Badge - Physical Security may issue a replacement badge, but with the same expiration date as the badge that was lost or damaged. Physical Security should sign the PIV Request Form and file it.

Step 7: Complete PIV Request Form - Physical Security will update the PIV Request Form with the Identification shown by the employee and will sign and date the form. The PIV Request Form will be stored in a secured container in accordance with local procedures.

Step 8: Update Badge Logically - Physical Security must update their systems to show the appropriate disposition for the badge and insure that all permissions associated with the badge have been revoked within 72 hours.

Step 9: Collect Damaged Badge - If the badge was damaged, Physical Security will collect the badge from the employee and destroy the badge. The date that the old badge was revoked should be entered on the old PIV Request Form.

6.3.2 Revocation

Step 1: Identify Need for Revocation - The need to revoke either an employee's or contactor's badge is identified. This can be initiated by the employee / contractor or can be a decision made by the IRS to terminate an employee.

Step 2: Collect Badge - The employee's manager or the contractor's COTR is responsible for collecting the employee's / contractor's badge. Once collected, physical security will revoke access to the facility within 72 hours. If the employee / contractor is terminated due to conduct reasons, and a potentially hostile environment exists, physical security may be contacted to escort the individual from the premises and building access privileges are revoked immediately, debarring the individual from the building.

Step 3: Return Badge to Security - The responsible manager or COTR needs to return the badge to Physical Security

Step 4: Failure to Recover Badge – If the employee's manager or the contractor's COTR is unable to recover the badge, they must inform the Physical Security office in writing that the badge was not recovered. Physical Security will then determine how to proceed with the missing badge in concurrence with existing procedures.

Step 5: Update PIV Request Form - Physical Security will update the PIV Request Form with the date of the returned badge and the appropriate disposition. The date that the badge was revoked should be entered on the PIV Request Form.

Step 6: Delete Badge Logically - Physical Security must update their systems to show the appropriate disposition for the badge and insure that all permission associated with the badge have been revoked within 72 hours.

Step 7: Destroy Badge - Physical Security is responsible for destroying the badge so that it can not be used again.

Step 8: Verify Badge upon Entry - Physical security is responsible for access control only in those facilities where the entrances are controlled by IRS. In those facilities, contract guards visually check ID cards. Current cards do not have expiration dates. Card keys are deleted from the system upon notification to the physical security office that such action is necessary.

6.3.3 Suspension / Furlough / When Actively Employed (WAE)

Step 1: Identify Temporary Leave - The employee's manager must identify the situation where an employee will not be continuously employed due to suspension, furlough, or other reason.

Step 2: Collect Badge - The employee's manager is responsible for collecting the employee's badge.

Step 3: Return Badge to Security - The responsible manager is required to return the badge to Physical Security with an explanation that there is a high probability that the employee will return to active duty.

Step 4: Failure to Recover Badge – If the employee's manager is unable to recover the badge, then they must inform the Physical Security office in writing that the badge was not recovered. Physical Security will then determine how to proceed with the missing badge in concurrence with existing procedures.

Step 5: Update PIV Request Form - Physical Security will attach a note to the PIV Request Form to communicate that the badge has been returned, but the expectation is that the employee will return to active duty and the badge will be returned. The attachment should be signed and dated.

Step 6: Delete Badge Logically - Physical Security must update their systems to show the appropriate disposition for the badge and insure that all permission associated with the badge have been revoked within 72 hours.

6.4 Special Situations - Hiring Employees in Remote Locations

Step 1: Identify Hire in Remote Location - The remote location identifies the person they would like to hire for a position at the remote location.

Step 2: Contact Employment (HR) - The hiring manager at the remote location calls the Employment team to get assistance with the PIV process.

Step 3: Conduct Training - The employment organization identifies a Commissioners Representative, an Administrative Officer or a manager to serve as the Designated Registrar. The HR office ensures that the Designated Registrar is trained and certified as a Registrar and assists them in the PIV process. The needed paperwork is forwarded from Employment to the designated Registrar.

Step 4: Perform Identity Proofing - The Designated Registrar performs identity proofing on the Applicant by viewing 2 forms of identification as specified by I9.

Step 5: Complete Forms - The Designated Registrar verifies that the Applicant completes the Consent for Fingerprint Check form and the Declaration for Federal Employment. Also the Applicant completes the Applicant section of the PIV Request Form.

Step 6: Fingerprinting - The Designated Registrar accompanies the Applicant to the Fingerprinting operation. Fingerprints are taken from the Applicant using Livescan or Ink & Roll. The Designated Registrar obtains the fingerprints from the fingerprinting station and puts it with the PIV Request Form.

The Registrar in the Employment Office would work with the Designated Registrar on a case-by-case basis to determine the best location of the fingerprinting operation. This could be in a local Criminal Investigation unit, or another Federal agency located in the same building, or the local law enforcement office.

Step 7: Send Forms / Data to Employment - The Designated Registrar securely mails all of the completed forms and the fingerprints to the Employment / HR Office.

Step 8: Initiate FBI Fingerprint Check- Fingerprints are transmitted or mailed to OPM by the Registrar (Employment).

Step 9: Receive Results FBI Criminal Check - If the FBI Criminal Check is favorable, the results are entered on the PIV Request Form and signed by the Registrar. If results are non-favorable, the results are entered on the PIV Request Form, and signed by the Registrar.

Step 10: Decision on Hiring/Need for Credential - HR and /or Business Unit makes determination on hiring, including certifying Applicant, suitability determination, selection and job offer.

Step 11: Initiate Background Investigation - The Registrar (Employment / HR) initiates the background investigation – NACI and updates the PIV Request Form.

Step 12: Final Determination - The Sponsor signs the PIV Form indicating the final determination and the validity of the need for a PIV credential.

Step 13: Notify Issuer - The Registrar verifies that all applicable sections of the PIV Request Form have been completed properly and forwards the form to the Issuer. The Issuer (Physical Security) is notified to initiate credential issuance, at a date no earlier than 5 days from the initiation of a background investigation.

7 Appeals Processes

Appeals processes for applicants, non-bargaining unit employees, and bargaining unit employees, who receive less than favorable background investigation results, are documented in 5 CFR 1201, PPD Policy Number 67, CFR 731, 5 CFR 752 and the National Agreement between IRS and NTEU, accordingly. Guidance for Contractors is referenced below.

7.1 Adjudication Guidance

The IRS shall use suitability criteria outlined in 5 CFR 731 or the adjudicative guidelines for determining eligibility for access to classified information when making adjudicative determinations for all federal applicants being considered for issuance of an identity card under HSPD-12.

7.2 Appeal Rights for Applicants

The IRS shall follow appeal rights found in PPD Policy Number 67 and 5 CFR 1201.22 (b) as applicable, when the background investigation is not favorably adjudicated.

7.3 Appeal Rights for Non-Bargaining Unit Employees

The IRS shall follow OPM appeal rights found in either 5 CFR 731 or 5 CFR 752 as applicable, when the background investigation is not favorably adjudicated.

7.4 Appeal Rights for Bargaining Unit Employees

The IRS shall follow appeal procedures in accordance with the National Agreement between IRS and NTEU when the background investigation is not favorably adjudicated..

7.5 Adjudicating Suitability for Contractors

The IRS shall use 5 CFR 731 or the adjudicative guidelines for determining eligibility for access to classified information suitability criteria when making adjudicative determinations on contractors. Adjudicating offices or bureau officials will abide by the appeal procedures described below when an unfavorable adjudication decision results in a contractor being found ineligible for a credential.

7.6 Appeal Rights for Contractor Employees

IRS or office officials adjudicating the investigation shall provide the contractor employee the reason(s) for the unfavorable decision in writing. A copy of the decision shall not be provided to the company. The contractor employee may request a review. The request must be in writing and faxed or, if mailed, postmarked within 10 calendar days of receipt of the unfavorable decision. The request shall be addressed to the adjudicating office. The adjudicating office will review the request and determine if the adjudication decision should be sustained, modified, or

reversed, and notify the contractor of the decision. The contractor shall also be informed that the decision is final. If the final determination is unfavorable, the COTR will be informed by letter that the contractor is ineligible for a PIV Card. Due to privacy requirements, no other information about the decision will be provided to the COTR or contractor's employer. If the adjudicating office does not receive a request from the contractor employee to review an unfavorable decision, the decision shall become final 15 calendar days after issuance.

8 Privacy Considerations

8.1 HSPD-12 Privacy Directive

HSPD-12 specifically states that "this directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans." FIPS 201 further states that "all departments and agencies shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in this standard, as well as those specified in Federal privacy laws and policies including but not limited to the E-Government Act of 2002 [E-Gov], the Privacy Act of 1974 [PRIVACY], and Office of Management and Budget (OMB) Memorandum M-03-22, as applicable."

8.2 IRS Privacy Officer Responsibilities

The IRS Privacy Officer is responsible for ensuring that IRS privacy policies provide protection and adherence to Federal Privacy Act requirements. The IRS Privacy Officer shall "oversee privacy-related matters in the PIV system and is responsible for implementing the privacy requirements in the standard."

8.3 HSPD 12 Staff Responsibilities

Individuals implementing HSPD-12 should have a thorough understanding of the IRS Privacy policy. PIV Applicants will be informed as to the purpose of information collected, their rights, benefits and obligations. The IRS shall "write, publish, and maintain a clear and comprehensive document listing the types of information that will be collected (e.g., transactional information, personal information in identifiable form [IIF]), the purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency."

8.4 Additional IRS Responsibilities

Further, the IRS will ensure records are accurate, relevant, timely, and complete, permit individuals access to and amendment of these records, and provide reasonable safeguards regarding disclosures and protections against security and integrity threats. The IRS shall "…maintain appeals procedures for those who are denied a credential or whose credentials are revoked."

The IRS shall "…ensure that only personnel with a legitimate need for access to IIF in the PIV system are authorized to access the IIF, including but not limited to information and databases maintained for registration and credential issuance."

APPENDIX A - References

A-1 Acronyms

Acronym	Definition
ABIS	Automated Background Investigation System
ALERTS	Automated Labor and Employee Relations Tracking System
AON	Consulting Firm
ARSI	Automatic Reimbursable Suitability Investigation
ATO	Authorization to Operate
BITS	Background Investigation Tracking System (Local procedures)
CARS	Competitive Automated Recruitment System
CC	Career Connector
CCT	OPM Case Closing Transmittal – Results of Fingerprint check request
Control Sheet	Qualifications Sheet/Job Aid checklist depending on Employment Office
COTR	Contracting Officer's Technical Representative
DAA	Designated Accreditation Authority
E-Gov	E-Government
EOD	Enter on Duty
ETA	External Trusted Agent
F 13340	Information Provided Concerning the Disclosure and Authorization Pertaining to Consumer Reports pursuant to the Fair Credit Reporting Act (FCRA)
F 11-99 DD	Direct Deposit
F 12333	Consent for Fingerprint Check
F 13340	Fair Credit Reporting Act Disclosure and Authorization Statement
F 13362	Consent to Disclosure of Return Information
F 256	Self Identification of Handicap
F 5520	IRS Identification Card Request
F 6028	
F 9620	Race and National Origin Identification
F AD349	Address Form
FBI	Federal Bureau of Investigation
FD258	Applicant Fingerprint Card
F I-9	Employment Eligibility Verification Form
FIPS	Federal Information Processing Standards
FOH	Federal Occupational Health
Form A	Qualifications and Availability
GRAPES	General Recruitment and Placement External System
HITS	Hiring Inventory and Training System
HR	Human Resources
HSPD12	Homeland Security Presidential Directive 12
IATO	Interim Authorization to Operate
ID	Identification Document
IDRS	Integrated Data Retrieval System
IIF	Information in Identifiable Form
IRS	Internal Revenue Service
LBI	Limited Background Investigation – Investigation for Moderate Risk Position

Acronym	Definition
LR	Labor Relations
MI	Middle Initial
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NARA	National Archives and Records Administration (location of OPF)
NBIC	National Background Investigations Training Center
NHO	New Hire Orientation
NSP	National Security Program
NIST	National Institute of Standards and Technology
NOR	Notice of Rating
OF306	Declaration for Federal Employment
OF612	Optional Application for Federal Employment
OFI-86A	Request for Determination or Advisory
OMB	Office of Management and Budget
OPF	Official Personnel Folder
OPM	Office of Personnel Management
OPM F 1603	Answer Booklet
PAR	Personnel Action Request (HR Connect)
PBIP	Procurement Background Investigation Program
PIPS	Personnel Investigations Processing System
PIV	Personal Identify Verification
PPD	
PS&I	Personnel Security and Investigations
PST	Procurement Sponsor Team
SEID	Standard Employee Identifier
SETS	Security Entry and Tracking System
SF 39	Request for Referral of Eligibles
SF 62	Agency Request to Pass over a Preference Eligible or Object to an Eligible
SF 85	Questionnaire for Non-Sensitive Positions
SF 85P	Questionnaire for Public Trust Positions
SF 86	Questionnaire for National Security Positions
SF 87	Fingerprint Card
SQS	Supplemental Qualifications Statement
SSN	Social Security Number
TAP	Telephone Assessment Program (administered by AON Consulting)
TDP	Treasury Department Publication
TIMIS	Totally Integrated Management Information System
TPC	Transactional Processing Center
US	United States
WAE	When Actively Employed

A-2 PIV Essential Systems Reference

ABIS (Automated Background Investigation System)

ALERTS	(Automated Labor and Employee Tracking System)
ARSI	(Automatic Reimbursable Suitability Investigation)
BITS	(Background Investigation Tracking System)
Badge Equipment	
CARS	(Competitive Automated Recruitment System)
CC	(Career Connector)
CCT	(Case Closing Transmittal/OPM)
CI	(Criminal Investigations)
DMS	(Document Management System) Repository
GRAPES	(General Recruitment and Placement External System)
HITS	(Hiring Inventory and Training System)
HR Connect	
IDRS	(Integrated Data Retrieval System)
Identix Livescan	
LAN/Access Database/Server	
Online 5081 Repository	
PBIP	(Procurement Background Investigation Process)
PIPS	(Personnel Investigations Processing System)
SEC	(Separating Employee Clearance) System
SETS	(Security Entry and Tracking System)
Selective Service Website	
STAT	(schedules/tracks drug test)
TAPS	Totally Automated Personnel System)
TIMIS	(Totally Integrated Management Information System)
USAJOBS	

LAN/Access Databases, Excel Spreadsheets
Phone, Fax, E-mail for communications

APPENDIX B – Forms

B-1 PIV Applicant Rights & Responsibilities Guide

B-2 PIV Request Form

B-3 Contractor Risk Assessment Checklist

Homeland Security Presidential Directive-12 (HSPD-12)
Personal Identity Verification (PIV)
Applicant Rights & Responsibilities Guide

This document describes the rights and responsibilities of an IRS Applicant in the Federal Personal Identity Verification (PIV) process. It addresses responsibilities regarding identity proofing, registration/enrollment, and issuance of a PIV Identification Card, as well as appeal rights if denied a PIV card. The term **Applicant** refers to the individual to whom a new PIV card will be issued. Applicants may be prospective Internal Revenue Service **(**IRS) employees or contractors.

Introduction to HSPD-12
On August 27, 2004, President Bush signed **Homeland Security Presidential Directive-12 (HSPD-12),** ***Policy for a Common Identification Standard for Federal Employees and Contractors***. Based upon this Directive, the National Institute for Standards and Technology (NIST) developed **Federal Information Processing Standards Publication** (FIPS Pub) 201 including a description of the minimum requirements for a Federal Personal Identity Verification (PIV) system. The HSPD-12 Directive directs the implementation of a new standardized credentialing process, which is designed to enhance security, reduce identity fraud, and protect the personal privacy of those issued government identification. The IRS will begin implementation of an HSPD-12 PIV compliant process for all new employees and contractors on October 27, 2005.

Along with this new process are new requirements:

1. Everyone issued an ID card must have a favorable background investigation, including an FBI fingerprint check. For most people, this will include a National Agency Check with Inquiries (NACI).
2. All personnel must be "identity-proofed," that is, they must present two forms of identification, one of which must be a state or federally issued photo ID.
3. No one person can be the sole official that requests, authorizes, and issues an ID card for an Applicant. There must be a clear distinction of duties per Applicant.

Undergoing the PIV Process
On or before the first day of employment, Applicants will be asked for information that will be used to complete a PIV Request Form, which begins the PIV process. Applicants must bring two forms of ID which will be reviewed for authenticity. One form of ID must be a valid state or federally issued picture identification. The other form must be a document listed on the back of the Form I-9, "Employment Eligibility Verification". A

current government issued employee identification badge may not be used as a picture ID. Fraudulent or altered

identification documents are not accepted as being authentic. No photocopies are acceptable. Failure to provide the documents means the Applicant failed to comply with the PIV requirements.

Applicants will also be asked to complete the appropriate paperwork in order for the IRS to initiate a background investigation. Applicants will be afforded three (3) opportunities prior to the entry-on-duty to provide the documents required for identity verification and for initiation of the background investigation.

At one of the IRS facilities, Applicant provided forms of identity will be authenticated by individuals trained and certified to perform this authentication. Applicants will also be fingerprinted and have their photograph taken. It is vital that Applicants bring all forms and paperwork with them as requested. Failure to comply with the PIV process may result in the loss of consideration for employment.

Documents Utilized in Identity Proofing
Under the PIV process, Applicants must provide appropriate documentation to verify their identity. A list of approved identification is available on the back of the Form I-9, "Employment Eligibility Verification." All documents provided must be unexpired.

Responsibilities of a PIV Card Holder/Applicant
Individuals issued a PIV card have the following responsibilities:

1. Shall cooperate fully in the PIV process.
2. Shall not attempt to copy, modify or obtain data from any PIV card.
3. Shall not assist others in gaining unauthorized access to Federal facilities or information systems.
4. Shall wear the PIV card properly at all times during work hours.
5. Shall report the loss or theft of an issued PIV card to their supervisor or Contracting Officer's Technical Representative (COTR) within 24 hours of noting its disappearance.
6. Shall return the PIV card when placed in a non-work status or upon termination of employment.
7. Must protect the PIV card at all times.

Wearing of PIV Cards
All individuals must wear PIV cards when in IRS facilities. All PIV cards shall be worn with an approved clip fastened to either an item of clothing or to an approved chain worn around the neck or in an approved transparent plastic card holder.

All PIV cards must be worn above the waist (on the torso) in such a manner that the photo is clearly visible from the front at all times. No mementos or other items may be attached to the PIV card that would obscure the information on the card.

NOTE: Exceptions to these instructions for reasons of health, safety, or religion must be approved by the employee's supervisor or COTR and the IRS Security office.

Rights of Prospective Employee Applicants Denied a PIV Card
In the event that a prospective employee Applicant is denied a PIV card based on PIV requirements, or a PIV card is revoked after issuance, Applicants have the option of appealing the decision. If the Applicant elects to appeal the decision, the following process will be initiated:

1. The Applicant will receive a letter stating the reason for the unfavorable decision.
2. The Applicant will have 30 calendar days from the date of the proposed action letter to review and provide additional information.
3. After the information provided is reviewed, the Applicant will be informed by letter of the final decision. The decision shall become final 30 calendar days after issuance of the letter.

NOTE: The IRS shall follow appeal rights found in Policy Number 67 and Title 5, Code of Federal Regulations (CFR), Part 1201.22 (b) as applicable, as a result of an unfavorable adjudication of the FBI criminal history record check and any disqualifying factors found in 5 CFR 731. To view the entire appeal process, an applicant may refer to Title 5 CFR 731 and 1201.22(b).

Rights of Prospective Contractor Applicants Denied a PIV Card
Prospective contractors denied a credential based on PIV requirements have the right to appeal the decision. If the Applicant elects to appeal the decision, the following process will be initiated:

1. The Applicant will receive a letter stating the reason for the unfavorable decision.
2. The Applicant will have 10 calendar days from the date of the proposed action letter to review and provide additional information.
3. After the information provided is reviewed, the Applicant will be informed by letter of a decision. The decision shall become final 15 calendar days after issuance of the letter.

PIV Card Applicant Representative
The IRS will assign a PIV Card Applicant Representative (PCAR) to represent the interests of prospective Federal employees and contractors who are the Applicants for PIV Cards. The PCAR will represent the privacy concerns of Applicants, assist an Applicant who is denied a PIV Card because of missing or incorrect information in an identity source document, or act as a surrogate for an Applicant that is not available for performing required actions.

NOTE: Applicants have the right to reapply for the current position or for other Federal or contractor positions if not accepted unless disqualified from eligibility under Title 5 CFR 731.

Privacy Notice
During the hiring process, Applicants will be asked to provide certain personal information to designated government personnel trained and certified in the PIV process. The information provided will be recorded on a PIV Request Form.

Title 5 U.S.C. § 301 and 31 U.S.C. § 321 provides authority for collecting the requested information. Executive Order 9397 (November 22, 1943) provides the authority for requesting your social security number. The purpose for collecting the requested information is to enable the IRS to produce and distribute identification cards to allow entry into their facilities.

The information collected may only be disclosed in accordance with the Department of the Treasury's published routine uses and as otherwise permitted under the Privacy Act of 1974 (5 U.S.C. § 552a), including disclosure to:

1. The United States Office of Personnel Management, the Merit Systems Protection Board, the Equal Employment Opportunity Commission, and the Federal Labor Relations Board upon an authorized request;
2. Agencies, contractors, and others to administer personnel and payroll systems, for debt collection and for employment or security investigations;
3. A law enforcement agency if the IRS becomes aware of a possible violation of a law or regulation;
4. A Congressional office in response to requests made on your behalf;
5. The Department of Justice, courts, and counsel during litigation;
6. Unions if needed to perform their authorized duties;
7. Other agencies under approved computer matches; and
8. Organizations otherwise authorized by law or regulations.

The PIV Request Form complies with the Privacy Act of 1974 and is needed to meet the policy requirements of the Department of the Treasury. The information on this form will be used to satisfy the requirements of HSPD 12, FIPS 201-PIV (Personal Identity Verification of Federal Employees and Contractors.)

While the Applicant has the option to refuse to provide any of the information, failure to do so may result in non-issuance of an identification card, thereby preventing them from accessing IRS facilities.

Questions
We thank all prospective employees and contractors for reading this guide and helping to do their part in making us all more secure. If a prospective employee has any questions, they should contact the HR office or PCAR identified in the vacancy announcement.

If a prospective contractor has any questions, they should contact the Contracting Officer Technical Representative (COTR) associated with their contract.

The Department of Treasury

Internal Revenue Service

PIV REQUEST FORM
Page 1

Request for: New Hire: ____ Re-Issue: ____ Employee: ____ Contractor: ____ Contract No.: _____

Section 1: Applicant Information (To be filled out by the Sponsor)

Last Name, First Name, M.I.: _____ SSN: _____

DOB: _____Contact Phone #: _____ Email: _____

Applicant: *I have read the PIV Applicant information packet provided to me and the privacy statement in Section 5 below and agree to participate in the PIV process.*
(Applicant Signature & Date) _____

Sponsor: *I agree to sponsor the above applicant for a PIV credential.*

(Sponsor Name, Title, Signature, Date) _____

Section 2: Registrar

A. Identity Verification

ID #1	**ID #2**
ID Type/Title: _____	ID Type/Title: _____
ID Number: _____	ID Number: _____
ID Exp. Date: _____	ID Exp. Date: _____

(At least one ID must be a valid State or Federal Issued photo ID)

I certify that the above information is accurate to the best of my knowledge.
(Registrar Name, Title, Signature, Date)_____

B. Background Investigation

FBI Criminal Check: Initiated: Date: _____ N/A: ___ Initials: _____

FBI Criminal Check Completed Date: _____

Initial Suitability Adjudicated / OK to issue PIV credential: Yes: _____ No: _____

Background Investigation Initiated Date: _____ N/A: ___ Initials: _____

I certify that the above information is accurate to the best of my knowledge.
(Registrar Name, Title, Signature, Date)_____

Background Investigation Completed Date: _____ N/A: ___ Initials: _____

Background Investigation Discontinued Date: _____ N/A: ___ Initials: _____

I certify that the above information is accurate to the best of my knowledge.
(Registrar Name, Title, Signature, Date)_____

The Department of Treasury
Internal Revenue Service

PIV REQUEST FORM
Page 2

Section 3: Issuer

Applicant identity re-verified (Initial): _____ Credential Issued Date: _____

I acknowledge issuance of a credential to the applicant identified above based on verification of the applicant's identity and verification of the above Registrar's issuance approval. I certify that the above information is accurate to the best of my knowledge.
(Issuer Name, Title, Signature, Date)_____

Credential Revoked Date: _____ Revoked by (signature)_____

Section 4: Applicant Acknowledgement

To be signed by applicant after issuance of credential
I, the Applicant, confirm receipt of the PIV credential and that the information is accurate to the best of my knowledge. I agree to abide by all rules and responsibilities associated with this credential and the PIV process.

Applicant Signature: _____ Date: _____

Section 5: Privacy

5 U.S.C. § 301 and 31 U.S.C. § 321 provide the authority for collecting the requested information. Executive Order 9397 (November 22, 1943) provides the authority for requesting your social security number. The purpose for collecting the requested information is to enable the Bureaus and Offices within the Department of The Treasury to produce and distribute identification cards to allow entry into their facilities.

The information collected by this form may be disclosed in accordance with The Department of The Treasury's published routine uses and as otherwise permitted under the Privacy Act of 1974 (5 U.S.C. § 552a), including disclosure: to the Office of Personnel Management, the Merit Systems Protection Board, the equal Employment Opportunity Commission, and the Federal Labor relations Board upon an authorized request; to agencies, contractors, and others to administer personnel and payroll systems, for debt collection and for employment or security investigations; to law enforcement agency if the Department of The Treasury becomes aware of a possible violation of a law or regulation; to a Congressional office in response to requests made on your behalf; to the Department of Justice, courts, and counsel during litigation; to unions if needed to perform their authorized duties; to other agencies under approved computer matches; and as otherwise authorized by law or regulations.

This form is in compliance with the Privacy Act of 1974. This form is needed to meet the policy requirements of The Department of The Treasury. The information on this form will be used to satisfy the requirements of HSPD 12, FIPS 201-PIV (Personal Identity Verification of Federal Employees and Contractors.)

Furnishing the information on this form, including your social security number, is voluntary, but failure to do so may result in non-issuance of an identification card, thereby preventing you from accessing The Department of The Treasury's facilities.

Contractor Risk Assessment Checklist

Provide the information below for all new contractors on your contracts or task orders. All new investigation packages require this checklist to be submitted via email (secure message) to the Procurement Sponsor Team at the email box: *PIVsponsor

Contractor Name	SSN	Contract Number	Work Location	Badge Required/ Issue Location	**System Access**
John L Doe	123-56-7890	TIRNO-59-D-05001	NCFB	Yes/MD0123 Lanham, Md	Email, Washington LAN, OL5081

Contractor Position Risk:

Please check the appropriate level:

____ Low Risk (NACI) – Support functions (Example: Admin, cleaning staff, mail service, warehouse service, etc.)

__X__ Moderate Risk (NACIC) – Responsible for planning, design, development, operation or maintenance of a computer system; security guards.

____ High Risk (BI) – System/Operations Management, System Analyst, Root Access or Network Security

Brief Description of contractor's duties (No more than 2 sentences):

Plan, design, document and maintain test databases.

_____

COTR SEID: _____

Fingerprint Source:

HR (IRS)_____

ETA (External Trusted Agent)_____

C-1 Identity Proofing & Registration Diagram – New Employees

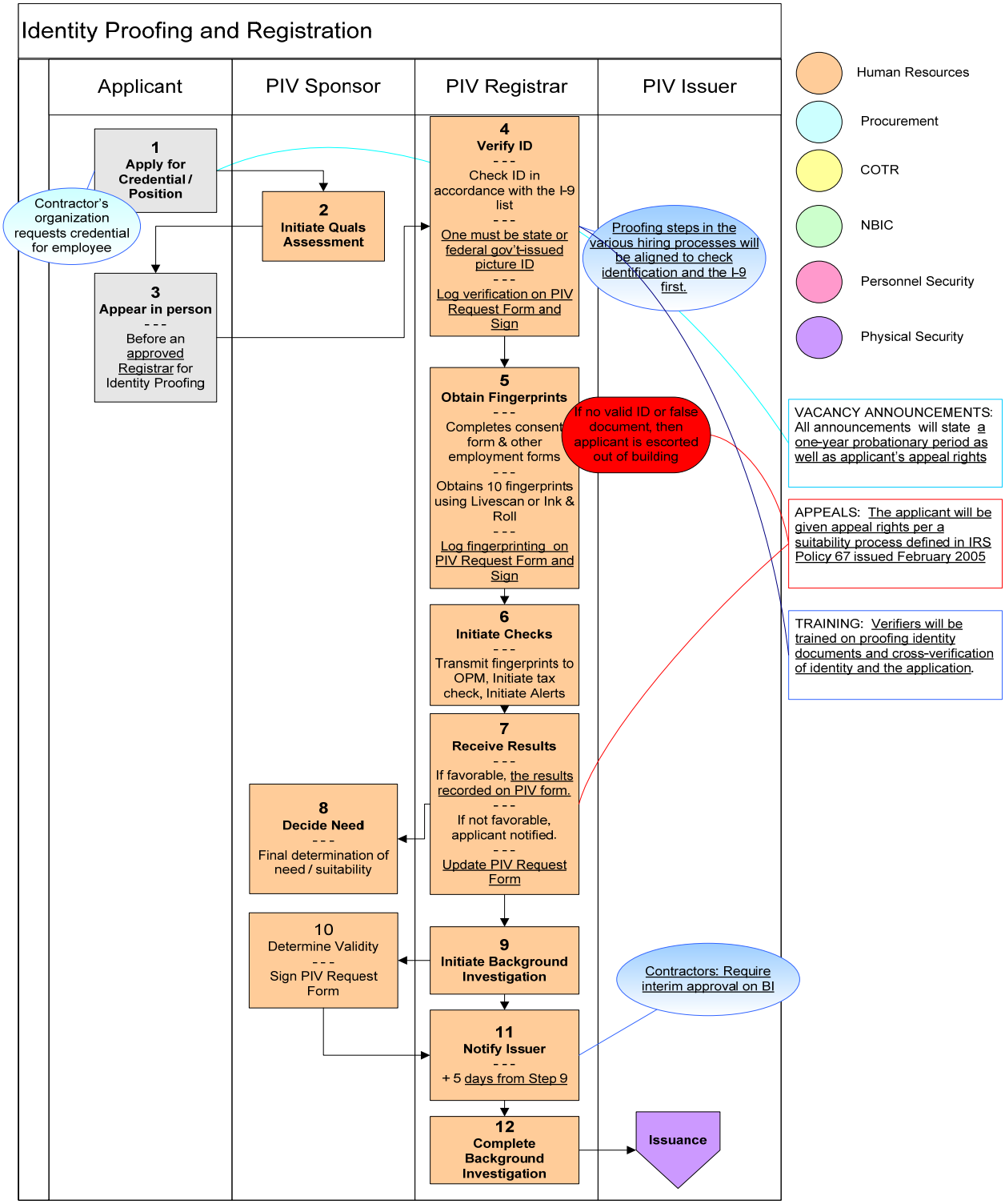
C-2 Identity Proofing & Registration Diagram – Contractors

C-3 PIV Issuance Diagram

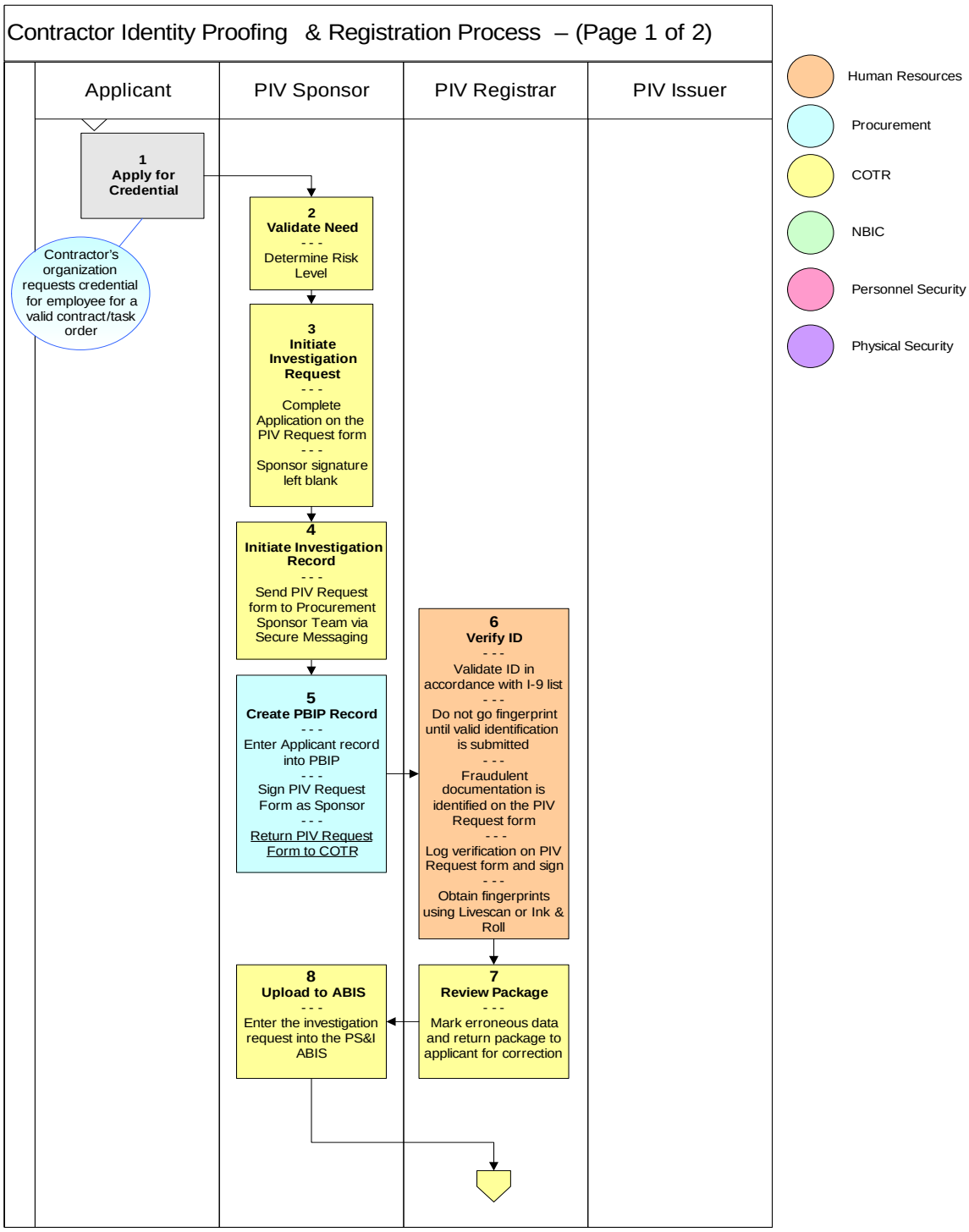
C-4 PIV Maintenance Diagram

C-5 PIV Revocation and Suspension

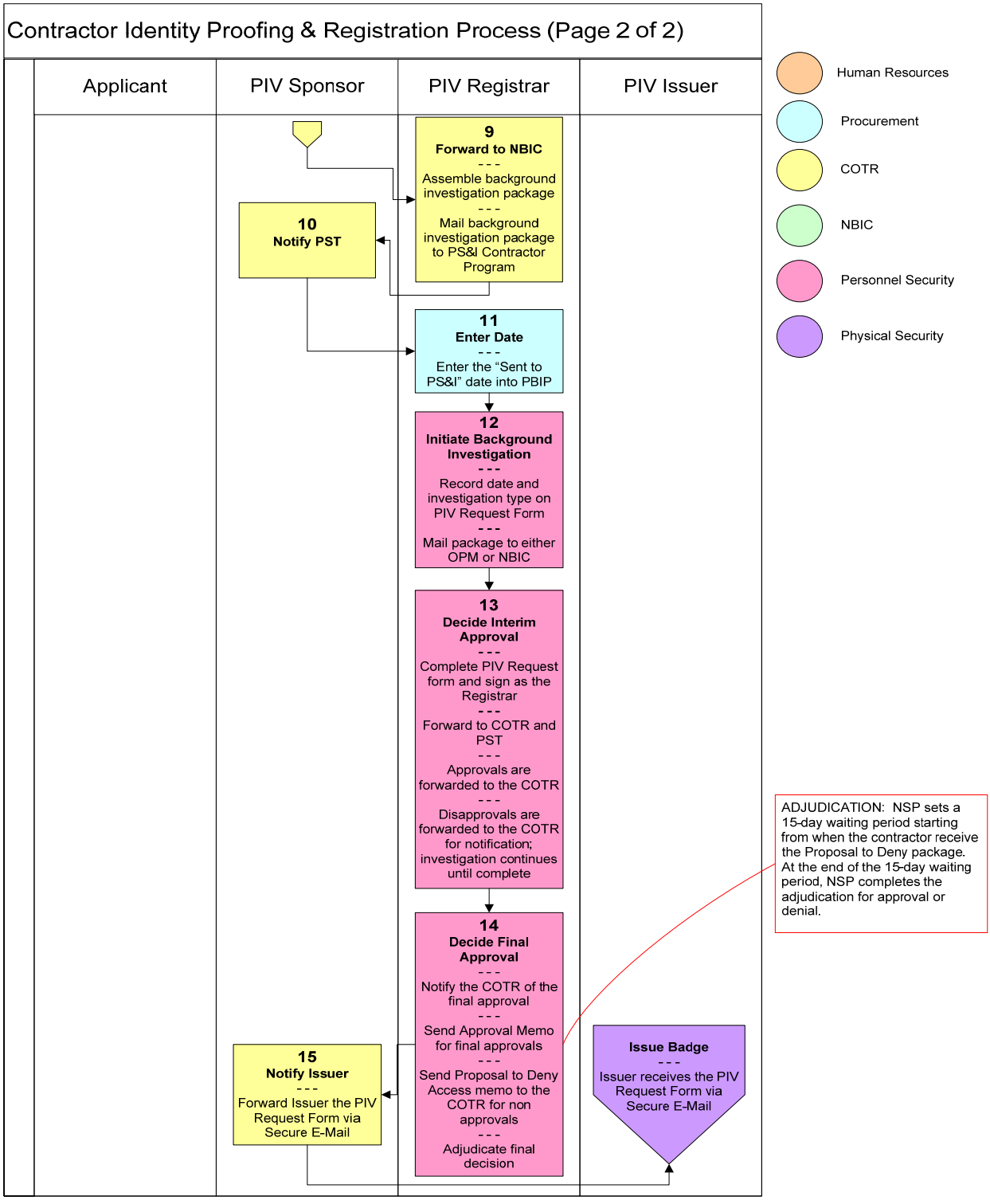
C-1 Identity Proofing & Registration Diagram – New Employees



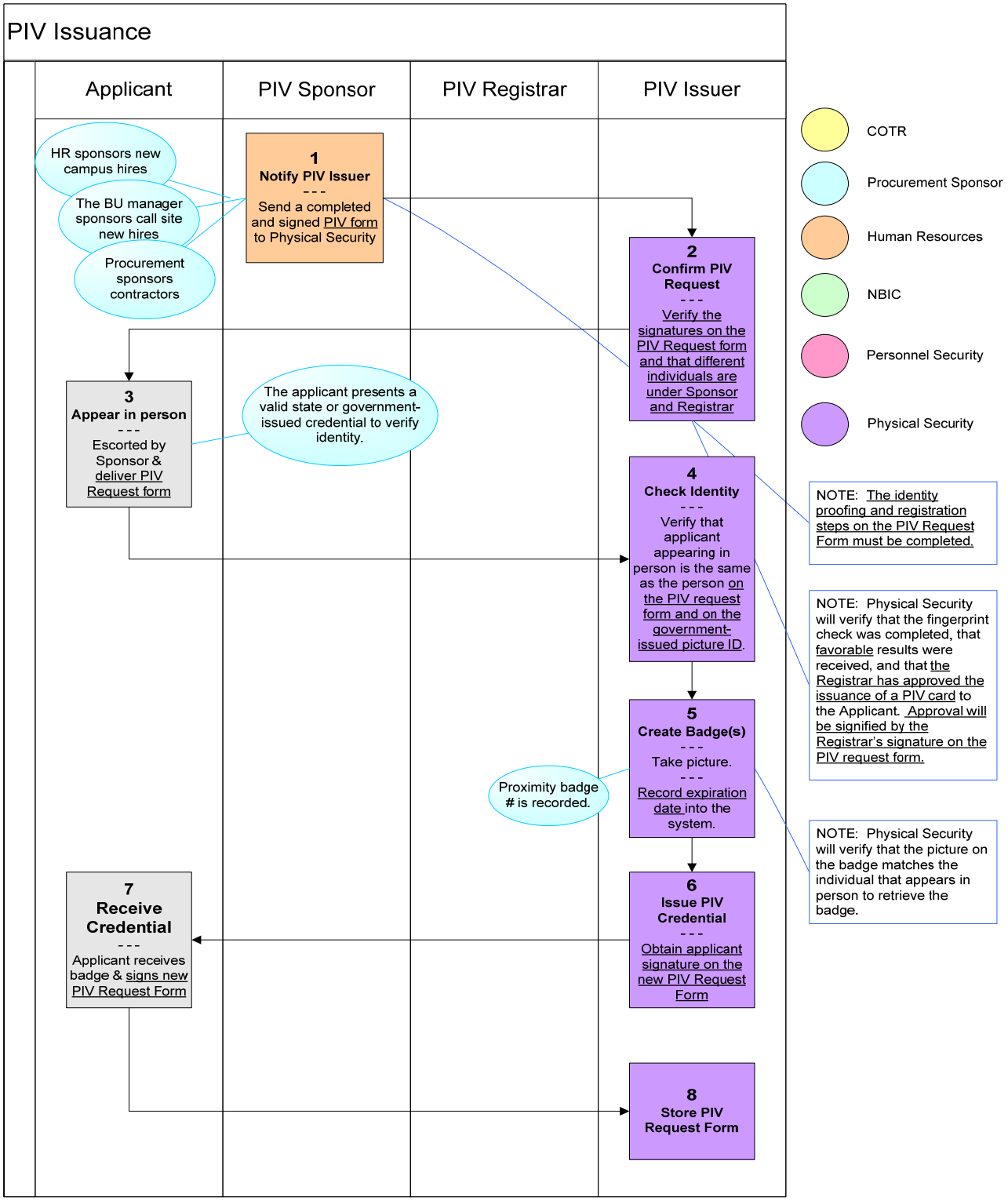
C-2 Identity Proofing & Registration Diagram – New Contractors Page 1



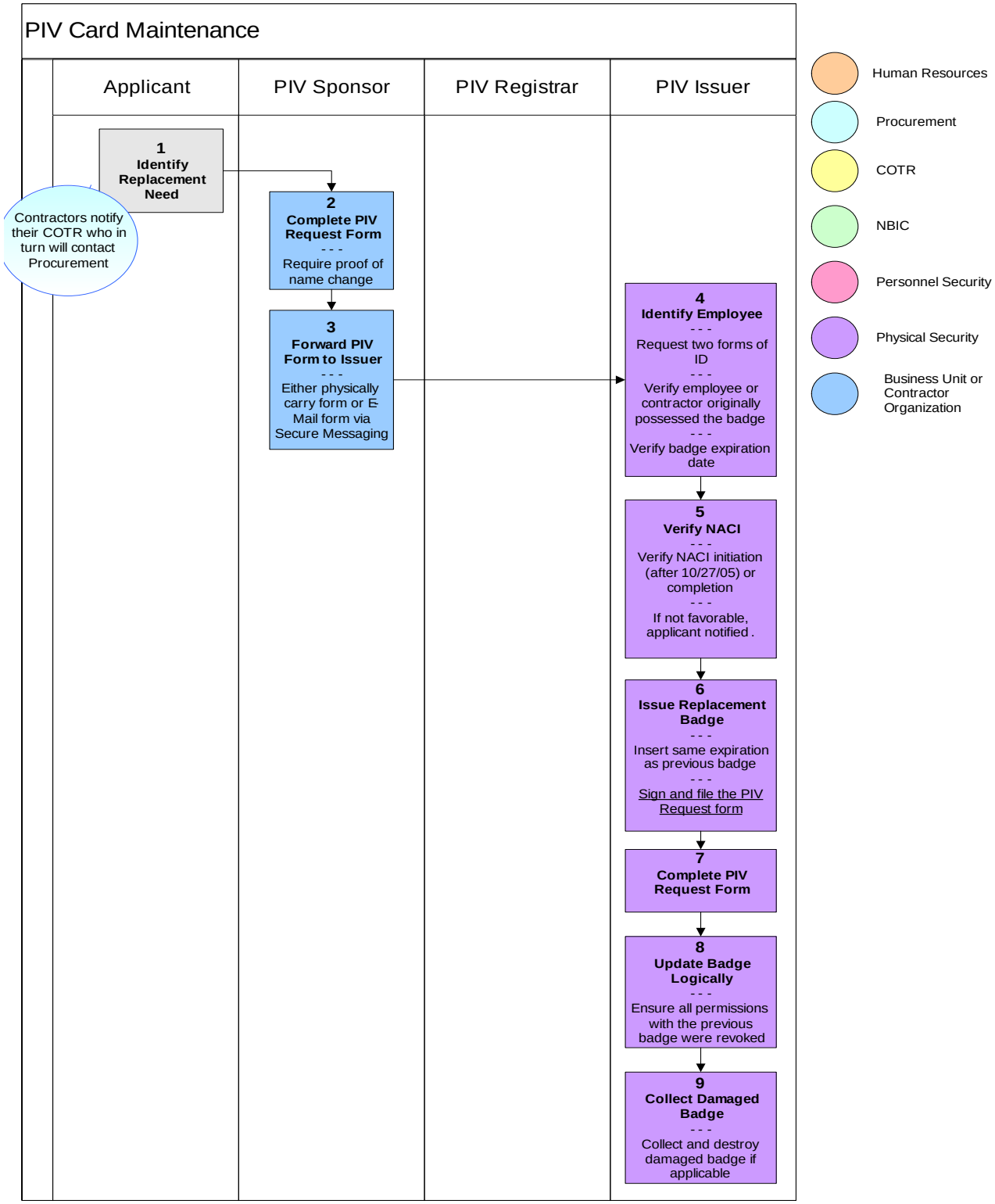
C-2 Identity Proofing & Registration Diagram – New Contractors Page 2



C-3 PIV Issuance Diagram



C-4 PIV Maintenance Diagram



C-5 PIV Revocation & Suspension Diagram