This directive has been cancelled by GSA Order, ADM 2181.1, dated March 18, 2020.

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO P 2181.1
October 20, 2008

GSA ORDER

SUBJECT: Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing

1. Purpose. This order issues and transmits the GSA HSPD-12 Personal Identity Verification and Credentialing Handbook.

2. Agency Goal. GSA's goal is to implement the requirements of HSPD-12.

3. Cancellation. CIO IL-07-02 (Homeland Security Presidential Directive (HSPD) -12, Personal Identity Verification and Credentialing) and ADM 7640.2 (Credentials and Passes) are cancelled.

4. Applicability. This handbook provides policies and procedures for issuing and maintaining GSA credentials.

5. Forms. This handbook provides for the use of the following:

a. CIW – Contractor Information Worksheet.

b. DHS 176T – Statement of Personal History for Contract and Childcare Personnel.

c. FD-258 – Fingerprint Card (Used for GSA Contractors).

d. GSA 1380 – National Security Position.

e. GSA 3648 – Public Trust Position.

f. GSA 3687 – HSPD-12 Personal Identity Verification and Credentialing Handbook Revision Request.

g. OF-306 – Declaration for Federal Employment.

h. Quick Name Check Form.

i. SF75 – Request for Preliminary Employment Data.

j. SF85 – Questionnaire for Non-Sensitive Positions.

k. SF85P – Questionnaire for Public Trust Positions.

l. SF85P-S – Supplemental Questionnaire for Selected Positions.

m. SF86 – Questionnaire for National Security Positions.

n. SF87 – Fingerprint Card (Used for GSA Employees).

Casey Coleman
Chief Information Officer

Attachments

GENERAL TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

CHAPTER 2 GSA HSPD-12 REQUIREMENTS

CHAPTER 3 CREDENTIALING PROCEDURES FOR EMPLOYEES

CHAPTER 4 CREDENTIALING PROCEDURES FOR CONTRACTORS

CHAPTER 5 PIV CARD MAINTENANCE AND RENEWAL

CHAPTER 6 PROVIDING LOGICAL ACCESS TO GSA IT SYSTEMS AND NETWORKS

CHAPTER 7 PROVIDING PHYSICAL ACCESS TO GSA-CONTROLLED FACILITIES

CHAPTER 8 GSA HSPD-12 PIV HANDBOOK REVISION PROCESS

ATTACHMENT A LIST OF HSPD-12 RELATED FORMS

ATTACHMENT B GSA SPECIFIC INFORMATION FOR SF85

ATTACHMENT C MSO ROLES DESCRIPTION

ATTACHMENT D FIPS 201 ROLES DESCRIPTIONS

ATTACHMENT E STEP-BY-STEP PROCESS FOR ENTERING DATA INTO CHRIS-PSTS

ATTACHMENT F OMB FORM I-9, 1115-0136, EMPLOYMENT ELIGIBILITY VERIFICATION

ATTACHMENT G FPS HQ AND REGIONAL OFFICES

ATTACHMENT H GSA HSPD-12 PIV HANDBOOK REVISION PROCESS DETAILED DESCRIPTION

ATTACHMENT I STATUS OF CHILD CARE CENTERS LEGAL OPINION

ATTACHMENT J FEDERAL CHILD CARE CENTER WORKERS FACILITIES ACCESS CREDITIALING

ATTACHMENT K DEFINITION OF TERMS

ATTACHMENT L ACRONYMS

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION

Paragraph Title	Paragraph Number
Acknowledgement.	1
Background.	2
Purpose and scope of document.	3
Overview of HSPD-12 process.	4

CHAPTER 2. GSA HSPD-12 REQUIREMENTS

General Requirements. 1
Who needs GSA personnel security investigations and credentials? 2
Available GSA credentials. 3
Required background checks. 4
Privacy considerations. 5
Additional considerations. 6

CHAPTER 3. CREDENTIALING PROCEDURES FOR EMPLOYEES

Roles and responsibilities in employee process. 1
Starting a new job at GSA. 2
Changing jobs within GSA. 3
Leaving a job at GSA. 4

CHAPTER 4. CREDENTIALING PROCEDURES FOR CONTRACTORS

Roles in contractor process. 1
Joining a new GSA contract. 2
Changing GSA contracts. 3
Leaving a GSA contract. 4
Help for HSPD-12 related questions. 5

CHAPTER 5. PIV CARD MAINTENANCE AND RENEWAL

Types of situations in which a PIV card may be reissued. 1

PIV card renewal.....2
PIV card replacement.....3
PIV card re-issuance. 4
Reset PIN on PIV card.....5

CHAPTER 6. PROVIDING LOGICAL ACCESS TO GSA IT SYSTEMS AND NETWORKS

General requirements.....1
Initial vs. full IT access.....2
Granting access to IT systems by authorizing officials upon personnel investigation verification. 3
Initial IT access waiver requests for contractors.....4
Change in employment status 5

CHAPTER 7. PROVIDING PHYSICAL ACCESS TO GSA-CONTROLLED FACILITIES

General requirements.....1
Access control on construction sites.....2

CHAPTER 8. GSA HSPD-12 PIV HANDBOOK REVISION PROCESS

Type of Handbook changes. 1
Handbook Revision process description.....2

CHAPTER 1. INTRODUCTION

1. Acknowledgement. The following policy document supersedes GSA HSPD-12 Personal Identity Verification – I (PIV-I) Standard Operating Procedure (SOP) – June 7, 2007 - Version 2.1.

2. Background. Homeland Security Presidential Directive 12 (HSPD-12) is a directive establishing a common identification standard for Federal employees and contractors. HSPD-12 requires all Federal Executive departments and agencies to conduct personnel investigations, adjudicate the results, and issue identity credentials to all Federal employees and contractors who require routine access to their building facilities and information technology (IT) systems. In response to HSPD-12, the National Institute for Standards and Technology (NIST) issued Federal Information Processing Standard 201 (FIPS 201), entitled “Personal Identity Verification of Federal Employees and Contractors” on February 25, 2005. FIPS 201 specifies the

architecture and technical requirements for a common identification standard for Federal employees and contractors, with the goal of achieving appropriate security assurance for multiple purposes by efficiently verifying the identity of individuals.

a. FIPS 201 assigns Federal agencies a clear set of responsibilities with regard to identity credentialing:

(1) Federal departments and agencies shall implement government-wide identity proofing, registration, and issuance functions that accomplish the following:

(a.) Identification is issued based on sound criteria for verifying an individual employee's identity.

(b.) Identification is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation.

(c.) Identification can be rapidly authenticated electronically.

(d.) Identification is issued only by providers whose reliability has been established by an official accreditation process.

(2) Each agency's PIV [Personal Identity Verification] implementation shall meet the four control objectives (a) through (d) listed above such that—

(a.) Credentials are issued only 1) to individuals whose true identity has been verified and 2) after a proper authority has authorized issuance of the credential.

(b.) Only an individual with a personnel investigation on record is issued a credential.

(c.) 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 ID.

(d.) Fraudulent identity source documents are not accepted as genuine and unaltered.

(e.) A person suspected or known to the government as being a terrorist is not issued a credential.

(f.) 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.

(g.) No credential is issued unless requested by proper authority.

(h.) 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.

(i.) A single corrupt official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential.

(j.) An issued credential is not modified, duplicated, or forged.

b. To meet the responsibilities and implement the HSPD-12 requirements, the Heads of Services and Staff Offices (HSSOs) and Regional Administrators (RAs) agreed to establish procedures to ensure compliance with the Presidential Directive and the General Service Administration (GSA) Handbook ADM P 9732.1C (Suitability and Personnel Security). (The GSA's Directives can be found at http://insite.gsa.gov/ "Reference & Resources" tab, under Directives or access directly through: http://insite.gsa.gov/Insite/gsa/ep/portletView.do?subTabId=0&pageTypeId=8683&channelPage=%2Fep%2FportletView.do%3FsubTabId%3D0&channelId=-8790.)

c. Implementing these procedures has required an integrated effort across many parts of GSA:

(1) The Personnel Security Requirements Division (CPR) of the Office of the Chief Human Capital Officer (OCHCO) has overall responsibility for personnel security requirements at GSA and manages the processing and adjudication of personnel investigations for GSA employees.

(2) The Public Building Service (PBS) has by far the largest number of individuals within GSA using the HSPD-12 personnel investigation and credentialing process. PBS has provided guidance and expertise on procedures, physical access requirements, and building security.

(3) The HSPD-12 Project Management Office (PMO) of the Office of the Chief Information Officer (OCIO) is responsible for coordinating the activities of Services and Staff Offices (SSOs) and RA offices responsible for requesting personnel investigations and credentials for job candidates, employees, and contractors.

(4) The HSPD-12 Stakeholders Group includes representatives of all SSOs and works with the HSPD-12 PMO to coordinate implementation of the HSPD-12 credentialing process. It helps communicate issues and suggestions between the SSOs and the PMO. It also advises the HSPD-12 PMO on changes to the HSPD-12 credentialing process.

d. These various groups within GSA are working together to ensure that the appropriate personnel investigation and credentialing requirements and procedures are followed.

3. Purpose and scope of document. This document, the GSA HSPD-12 PIV Handbook, covers requirements and procedures for personnel investigations, credentialing requests, and the issuance of PIV cards. This Handbook supplements instructions contained in the following documents and takes precedence while these more authoritative documents are in the process of being revised to be compliant with HSPD-12 requirements:

- GSA Handbook ADM P 9732.1C (Suitability and Personnel Security)
- CIO P 2100.1D, GSA Information Technology Security Policy
- General Services Acquisition Manual (GSAM)

a. The purpose of this document is to provide both a broad overview of the personnel investigation and credentialing process at GSA and a set of detailed, step-by-step instructions for all of the participants in the HSPD-12 process.

b. Note: In many cases there are other documents, including the ones mentioned above as well as instructions from other organizations such as Office of Personnel Management

(OPM), GSA HSPD-12 Managed Service Office (MSO) and DHS Federal Protective Service (FPS) that contain detailed and authoritative information for their areas of responsibility. For example, ch. 2 of this document outlines various requirements for issuing credentials to employees and contractors. It summarizes the requirements in the text and covers informally the most common cases. Nonetheless, it is the GSA Handbook ADM P 9732.1C (Suitability and Personnel Security) that is the authoritative source for personnel security and suitability requirements. Wherever appropriate in this document, the more detailed and/or authoritative sources will be cited for use by GSA staff as needed. (See fig. 1-3 for an annotated list of resources and documents.)

Figure 1-3. Other resources: HSPD-12 related policy documents and instructions

Document Type	Document Title	Document Location	Publication Date
Policy Documents	Homeland Security Presidential Directive – 12 (HSPD-12)	http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html☐	08/2004
	Federal Information Processing Standards 201-1 (FIPS 201-1)	http://insite.gsa.gov/graphics/staffoffices/fips201.pdf☐	03/2006
	National Institute of Standards & Technology Interagency Reports	http://csrc.nist.gov/publications/nistir/☐	06/2007
	National Institute of Standards & Technology Special Publications	http://csrc.nist.gov/publications/nistpubs/☐	06/2007
	OMB Guidance M-07-06 Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials	http://www.whitehouse.gov/omb/memoranda/fy2007/m07-06.pdf☐	01/2007
	OMB Guidance M-06-18 Acquisition of Products and Services for Implementation of HSPD-12	http://www.whitehouse.gov/omb/memoranda/fy2006/m06-18.pdf☐	06/2006
	OMB Guidance M-05-24	http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf☐	08/2005

	Implementation of HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors		
	GSA Order ADM 9732.1C Suitability and Personnel Security Implementation of GSA personnel security policies and procedures	http://insite.gsa.gov, GSA Insite > Reference & Resources > Directives, Tab "Directives By Number"	01/1998
	GSA Order CPO 1878.1 GSA Privacy Act Program Implementation of GSA privacy policies and procedures	http://insite.gsa.gov, GSA Insite > Reference & Resources > Directives, Tab "Directives By Number"	10/2003
	GSA Order CIO P 2100.1D GSA IT Security Policy Implementation of GSA IT security policies and procedures	http://insite.gsa.gov, GSA Insite > Reference & Resources > Directives, Tab "Directives By Number"	06/2007
Technical Guides	GSA Data Release Policy Instructional Letter – HCO IL	http://insite.gsa.gov, GSA Insite > Reference & Resources > Directives, Tab "Instructional Letters"	07/2007
	Requesting OPM Personnel Investigations (IS	http://www.opm.gov/extra/investigate/IS-15.pdf	05/2001
	OPM Investigations Reimbursable Billing for FY-08	http://insite.gsa.gov, GSA Insite > Information Technology > HSPD-12 Implementation > Policy & Guidance Resources	10/2007
	GSA Information Breach Notification Policy, HCO IL-07-02	http://insite.gsa.gov/Insite/gsa/ep/portletView.do?pageTypeId=8683&subTabId=6&channelId=-8790&redirectUrl=http%3A%2F%2Finternotes.gsa.gov%2Finsite%2Fgsad.nsf%2FInsiteInstructionalLettersDisplay%2F73218CF25140BDC58625735D00641B65%3FOpenDocument	09/2007

c. This document covers personnel investigation and credentialing requirements and procedures in the following way:

(1) Ch. 2, "GSA HSPD-12 Requirements," covers requirements for issuing credentials, describes what types of credentials can be issued and what type of personnel investigations should be conducted, and discusses privacy and other considerations.

(2) Ch. 3, "Credentialing Procedures for Employees," covers the step-by-step procedures for requesting personnel investigations and credentials for GSA employees.

(3) Ch. 4, "Credentialing Procedures for Contractors," covers the step-by-step procedures for requesting personnel investigations and credentials for GSA contractors.

(4) Ch. 5, "PIV Card Maintenance and Renewal," covers step-by-step procedures for renewing expired PIV cards and replacing them when they are lost, damaged, stolen, or otherwise unusable.

(5) Ch. 6, "Providing Logical Access to GSA IT Systems and Networks," covers additional requirements and procedures for obtaining access privileges to GSA IT systems and networks.

(6) Ch. 7, "Providing Physical Access to GSA-Controlled Facilities," covers additional requirements and procedures for accessing GSA-controlled facilities, campuses, and buildings.

(7) Ch. 8, "GSA HSPD-12 PIV Handbook Revision Process," describes the process for keeping the GSA HSPD-12 PIV Handbook up to date.

(8) Attachments cover a variety of information, including a list of all the forms used in HSPD-12 procedures and where to find them (Attachment A), and GSA-specific advice on how to fill out the SF85 form (Attachment B).

4. Overview of HSPD-12 process.

a. HSPD-12 and identity management. The HSPD-12 process is part of a larger identity management and security effort at GSA. At GSA, "identity management" is concerned with the identity of individuals who need to (or try to) access GSA-controlled resources such as IT systems, IT networks, GSA buildings, or other GSA-controlled facilities. Identity management begins with having in place a well-designed agency-wide security framework for identifying GSA resources and their particular security requirements.

b. When accessing a GSA resource (e.g., when entering a building or logging onto an IT system), an individual must usually provide some form of credential as a proof of identity. Credentials come in many forms and can include a photo ID card used as a flash-pass to enter a building, or a user name and password used to logon to a GSA IT system, among others. In the future, the GSA PIV card will used to access both GSA buildings and IT systems.

c. The important point to note is that in order for the credential to be trustworthy, it must accurately identify the individual to whom it was issued. The credential has to be trustworthy and issued to the correct person, because it will be used to validate an individual's request to access a GSA resource. Therefore, GSA must take care when determining what kinds of credentials are issued, who is receiving the credentials, and what access rights are granted to individuals holding those credentials.

d. The HSPD-12 program is an effort to improve the quality and reliability of GSA credentials by issuing a new agency-wide GSA ID card called the PIV card. The card uses smart card technologies: it has a computer chip embedded in the ID card that electronically stores credential information including biometric. This improved ID card will be used in the future to provide better controlled access to GSA buildings and IT systems.

e. The new GSA PIV card will support the identity management goal of providing the framework for linking three artifacts:

(1) An individual person

(2) Their issued credentials, where each credential represents a separate "identity"

(3) The access privileges granted to use GSA resources

f. In order to get these three linkages set up and working, there are five major steps. (See fig 1-4.1):

(1) Making a request for credentials and access privileges. In this step, an individual works with the designated GSA staff to make a request to be granted routine access to GSA resources; this usually happens when a new employee or contractor joins GSA, though requests for additional privileges or credentials can be made later as needed.

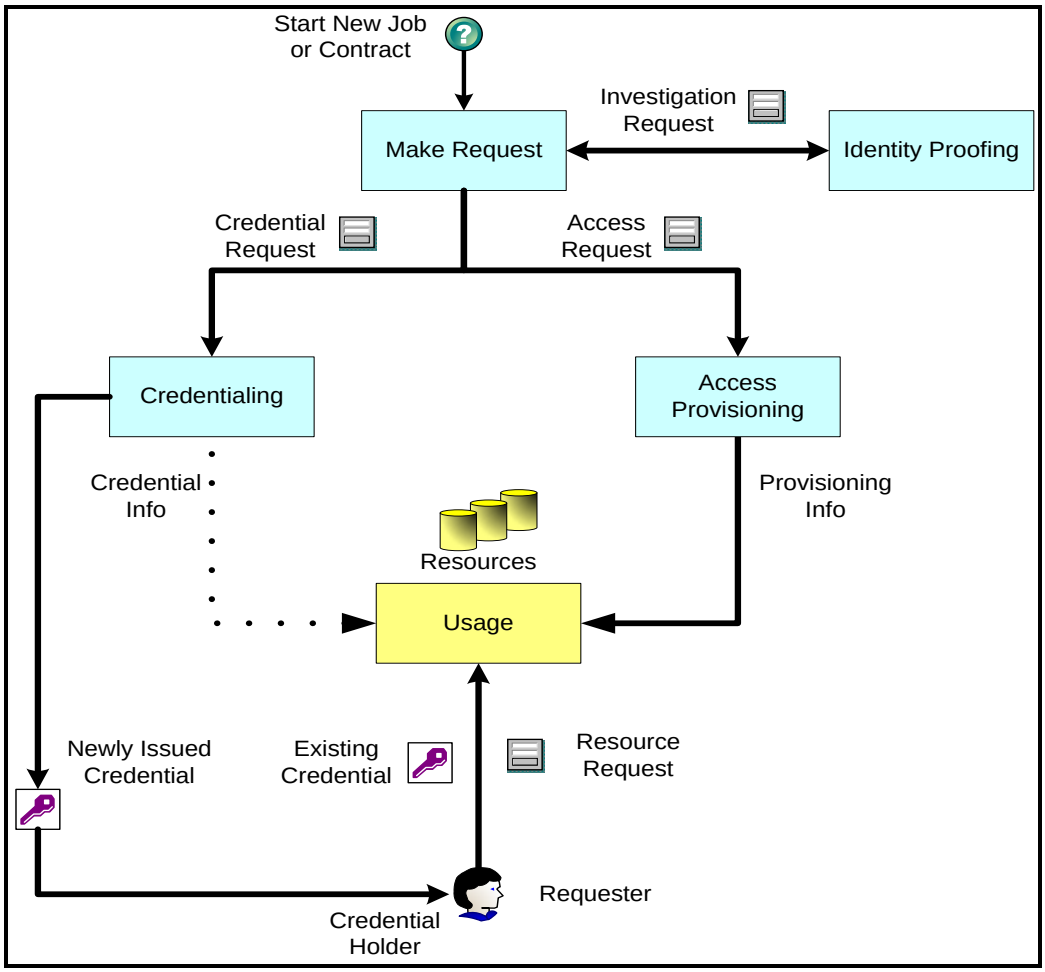
(2) Identity proofing. In this step, GSA verifies the identity of the individual requesting access; this usually involves doing name and fingerprint checks against multiple Federal and state databases, as well as conducting an OPM personnel investigation in most cases.

(3) Credentialing. In this step, if the identity proofing step has produced favorable results from the database checks and personnel investigation, GSA issues the appropriate credentials to the individual requesting access.

(4) Access provisioning. In parallel with the credentialing step and prior to using any credentials issued, GSA security staff grant ("provision") access to specific IT systems and, in some cases, to specific GSA-controlled building and facilities.

(5) Usage. Finally, if an individual presents his or her credentials and requests to use or access specific GSA resources, and if the appropriate access privileges have been set up in advance (especially in the case of IT systems access), then the individual's usage request is granted.

Figure 1-4.1. Stages in identity management



g. HSPD-12 and job and PIV card lifecycles. Another way to understand the HSPD-12 process is to look at the triggering events that initiate different kinds of process activity. These events fall into two categories:

(1) Job lifecycle events, e.g., start a new job, change jobs, leave a job

(2) PIV card lifecycle events, e.g., issue a new card, replace a card, and renew a card

h. At each step in these lifecycles, different procedures need to be followed. Recently, most of the focus has been on the issuance of new PIV cards, but consideration also needs to be given to the full range of lifecycle events possible.

i. Fig. 1-4.2, below, sets out the various HSPD-12 related business processes for employees and contractors. It shows which chapters of the Handbook cover the procedures for events related to changes in employment. It also sets out where in the Handbook to find the maintenance and renewal procedures for PIV cards.

Figure 1-4.2. Job & PIV card lifecycles and process & events triggers

Lifecycle Management Type	BP #	Handbook Chapter	Process	Process Descriptions	Events that Trigger Process
Employee Job Lifecycle Management	BP 1.1	Handbook Ch. 3-2	Starting New Job at GSA	Investigate and provide appropriate agency credentials for new employee.	• Agency accepts new employee to staff a position, when the individual has no existing active job with GSA. • Agency accepts employee to staff a position when the employee had been a GSA contractor. • Employee onboard before Oct. 2005 does not have an existing personnel investigation.
	BP 1.2	Handbook Ch. 3-3	Changing Jobs within GSA	Adjust agency credentials for existing employee working in a new position with the agency.	• Employee switches from an existing position to a new position. • Employee is staffed against a new position while continuing to work on an existing job. • Cardholder's organizational affiliation has changed.
	BP 1.3	Handbook Ch. 3-4	Leaving Job at GSA	Revoke credentials when ending agency employment.	• Agency terminates employee.
Contractor Job Lifecycle Management	BP 2.1	Handbook Ch. 4-2	Joining New GSA Contract	Investigate and provide appropriate agency credentials for new contractor.	• Agency accepts new contractor to staff a contract when contractor has no existing active contract. • Agency accepts contractor to staff a contract when the contractor had been an employee. • Contractor onboard before Oct. 2005 who does not have an existing personnel investigation.
	BP 2.2	Handbook Ch. 4-3	Changing GSA Contracts	Adjust agency credentials for existing contractor working on a new contract within the agency.	• Contractor switches from an existing contract to a new contract. • Contractor is staffed against new contract while continuing to work on an existing contract. • Cardholder's organizational affiliation has changed.
	BP 2.3	Handbook Ch. 4-4	Leaving GSA Contract	Revoke credentials when ending GSA employment as a contractor.	• Agency terminates contract.. • Contractor company terminates contractor, e.g. resignation, retirement, death. • Contractor company reassigns contractor to other work outside the agency.
PIV Card Renewal Lifecycle Management	BP 3.1	Handbook Ch. 5-2	Card Renewal	Issue new PIV card to cardholder with an expired card.	• PIV card has expired or is within six (6) weeks of expiring.
	BP 3.2	Handbook Ch. 5-3	Card Replacement	Return old PIV card and issue new PIV card to same cardholder.	• PIV card has been damaged. • PIV card has been broken. • PIV card is unreadable. • PIV card is not usable. • Cardholder name or other card data has changed.
	BP 3.3	Handbook Ch. 5-4	Card Re-issuance	Issue new PIV card to cardholder without returning old PIV card.	• PIV card has been lost. • PIV card has been stolen. • PIV card has been destroyed. • PIV card has been compromised.

CHAPTER 2. GSA HSPD-12 REQUIREMENTS

1. General Requirements.

a. GSA must use an approved identity-proofing and registration process that complies with FIPS 201 for all employees and contractors requesting a GSA PIV card.

b. Identity proofing is required to firmly establish an individual's identity. For individuals receiving a PIV card, this is accomplished by conducting a personnel security investigation and an FBI National Crime History Check (NCHC), known as the fingerprint check, as well as other similar checks as deemed appropriate by GSA. Requirements for individuals not receiving a PIV card, such as visitors, certain temporary contractors, child care workers, etc., are described in par. 2. The results of an investigation and background check are reviewed and adjudicated by GSA or organizations designated by them. Employment at GSA is subject to an employee or contractor having favorable adjudication results. The PIV card and other GSA credentials must be withheld or revoked if the appropriate national security or job suitability decisions are unfavorable.

c. The type of personnel investigation required varies according to an individual's job responsibilities and access to classified or sensitive information (i.e., Personally Identifiable Information (PII)). Likewise, the choice of GSA credentials to be issued is based on an individual's job responsibilities, work location, and access to IT systems. (See par. 2, below, for more information on the groups to whom GSA issues credentials; par. 3 for the types of credentials issued; and par. 4 for the kinds of investigations required.)

d. All employees and all long-term contractors must be issued a PIV card; other GSA personnel may be issued a PIV card as needed. (See par. 2, below, for specific information on what credentials are needed for different categories of individuals.) Issuance of a PIV card requires favorable results on an FBI fingerprint check and the initiation of a personnel security investigation at the level of the National Agency Check with written Inquiries (NACI) or higher. If final adjudication of the personnel investigation results is unfavorable, the PIV card is revoked.

e. The PIV identity-proofing and credentialing process must adhere to the principle of separation of roles. No single individual may have the ability to both request issuance of a new PIV card and approve the same request.

f. During the credentialing process, the employee or contractor requesting a PIV card must appear at least once in person in front of an authorized PIV official, the MSO/GSA Enrollment Officer. This happens when the employee/contractor appears to have fingerprints and a photo taken. At that time, the employee/contractor must provide two identity source documents in original form. These documents must be on the list of acceptable documents included in I-9, Office of Management and Budget (OMB) No. 1115-0136, "Employment Eligibility Verification." (See Attachment F). One of the documents must be a valid (not expired) picture ID issued by a State government or the Federal Government.

g. GSA must use an approved and certified ID card, card issuance, and card maintenance process. GSA must issue credentials through systems and third-party providers whose reliability has been established by GSA, documented, and approved in writing.

h. Personnel who receive a PIV card should keep their PIV card in an electromagnetically opaque sleeve that is on the FIPS 201 Approved Products List. The electromagnetically opaque sleeves are distributed along with the PIV cards.

i. PIV cards or other GSA credentials should be worn above waist level and be clearly visible at all times by GSA personnel and other personnel at GSA-occupied space. (See ch. 7 for additional information on credential requirements for physical access to GSA-controlled facilities.)

j. Special privileges letter codes such as "P" for property removal and "C" for child care parent/employee that were previously issued on GSA credentials are discontinued for GSA PIV cards.

2. Who needs GSA personnel security investigations and credentials?

a. All employees and contractors.

(1) GSA initiates personnel investigations, adjudicates the results, and issues appropriate identity credentials to all its employees and contractors who require "routine access" to its controlled facilities and/or its information systems.

(2) Routine access is defined as regularly scheduled access. For example, a contractor who reports to the facility on a regular basis in the performance of ongoing responsibilities has routine access and a personnel investigation must be conducted. A contractor who is summoned for an emergency service call is not required to have a personnel investigation and is treated as a visitor. GSA contractors who require regularly scheduled access to one or more GSA-controlled facilities, even under multiple contracts, should be treated as having routine access to GSA facilities.

(3) Personnel investigations for employees are conducted by OPM, and the results are adjudicated by the GSA Personnel Security Requirements Division (OCHCO/CPR).

(4) The Department of Homeland Security's Federal Protective Service (DHS/FPS), under memorandums of agreement (MOAs) with Public Building Service (PBS) and GSA, processes and adjudicates personnel investigations for GSA contractors. Personnel investigations for contractors are conducted by the Office of Personnel Management at the request of FPS.

(5) Requirements for GSA contractors differ according to whether their employment is expected to be long-term or temporary:

(a.) Long-term contractors are those employed for more than 6 months.

(b.) Temporary contractors are those employed for 6 months or less.

b. Employees and long-term contractors.

(1) All employees and those long-term contractors requiring routine access to GSA facilities and/or IT systems must have a personnel investigation appropriate for their job responsibilities in order to be issued a PIV card. The agency must initiate a minimum of a

National Agency Check with Written Inquiries (NACI) and must have received favorable results on the FBI fingerprint check before a PIV card can be issued and access to GSA facilities granted.

(2) Initial or full access to GSA Information Technology (IT) systems may be granted by the authorizing official for IT systems (known as the Designated Approving Authority (DAA)). Authorizing officials may grant initial or full access to GSA IT systems after verifying through the GSA OCHCO/CPR that an employee or contractor has an Access National Agency Check and Inquiries (ANACI), National Agency Check with Law and Credit (NACLC), Single Scope Background Investigation (SSBI), or other acceptable level of investigation or clearance. (The list of authorizing officials can be found at http://insite.gsa.gov/ Information Technology tab, under IT Security > Points of Contact or access directly through: http://insite.gsa.gov/graphics/staffoffices/poc.xls.)

(3) If the authorizing official does not grant an employee or contractor initial or full access to GSA IT systems, the same personnel investigation requirements based on an employee's or contractor's job responsibilities to obtain a PIV card will apply to obtain initial and full IT access. Initial IT access shall be defined by the authorizing official commensurate with the employee or contractor's job function and the risk and magnitude of harm that can be done. Contracting Officers (COs), Contracting Officer Technical Representatives (COTRs), or their designees may submit waiver requests to grant contractors initial IT access before GSA receives the results of the fingerprint check. (See ch. 6-4 for additional information, including guidelines and procedures for submitting waiver requests.) Full IT access is provided upon completion of a personnel investigation with favorable results. (See par. 4 and ch. 6 for more details on risk levels and access to IT systems.)

c. Temporary contractors.

(1) Temporary contractors are defined as those contractors employed for 6 months or less.

(2) Generally, temporary contractors do not receive a GSA PIV card unless they require access to GSA IT systems. Temporary contractors needing issuance of a GSA PIV card and/or access to IT systems must abide by the same personnel investigation requirements as those for long-term contractors. This includes the requirement that initial or full IT access is granted by the authorizing official after verifying an existing ANACI, NACLC, SSBI, or other acceptable level of investigation or clearance. If the authorizing official does not grant an employee or contractor initial or full access to GSA IT systems, initial IT access is granted only after receiving a favorably adjudicated FBI fingerprint check, and full IT access is granted only after a favorably adjudicated personnel investigation (at the minimum level of a NACI). COs, COTRs, or their designees may submit waiver requests to grant contractors initial IT access before GSA receives the results of the fingerprint check. (See ch. 6-4 for additional information, including guidelines and procedures for submitting waiver requests.)

(3) The CO, COTR, project manager, or other designated representative designated to handle contractor staffing decisions for a given contract is responsible for making determinations regarding whether a contractor is a long-term contractor or a temporary contractor. They are also responsible for monitoring the duration of projects, and should

the work exceed 6 months, all temporary contractors must be required to submit the personnel investigation documentation required of long-term contractors.

(4) Temporary contractors who will be working up to 6 months and need routine access to nonpublic areas of GSA-controlled facilities shall either undergo a law enforcement check or must be escorted, at the minimum. Escorts are defined as employees and contractors who have received a favorable initial suitability decision and possess valid identification credentials (either a current PIV card or temporary badge and I-9 document).

(5) Temporary contractors who will receive a law enforcement check are required to submit form DHS176T or SF85P and undergo a law enforcement check. These forms shall be submitted by the contractor to the designated GSA staff prior to the commencement of work. These materials will be forwarded to DHS/FPS for the processing of the law enforcement check. (See ch. 4 for procedures on credentialing temporary contractors.)

(6) Escorts are required for temporary contractors awaiting the results of the law enforcement check.

(7) The following general procedures must be followed for temporary contractors who will be working in a facility and needing routine access:

(a.) Apply adequate controls to systems and facilities: ensure temporary staff has limited/controlled access to building facilities and information systems (See chs. 6 and 7).

(b.) Provide temporary contractors with clear documentation on the rules of behavior and consequences for violation before granting access to facilities and/or systems.

(c.) Document any security violations involving temporary contractors, and report them to the appropriate authorities within 24 hours. (For IT systems, "authorities" would be the DAA, ISSM or ISSO, as well as the GSA IT Security office. For buildings, "authorities" would be the GSA building manager and building security office.)

(d.) Any credentials issued to temporary contractors must be visually and electronically distinguishable from GSA PIV cards and consistent with the technical guidance provided in FIPS PUB 201-2 and ID Management.gov.

d. Non-US Citizens

(1) OPM issued final guidance on their credentialing standards through memorandum "Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12" on July 31, 2008.

(2) Per OPM guidance, GSA will not request background investigations for non-US citizens who have not been a US resident for three consecutive years. Instead, GSA will request the following checks to receive initial access or entry of duty determination:

(a.) FBI Fingerprint and Name Check

(b.) National Crime Information Center (NCIC)/Interstate Identification Index (III)/National Law Enforcement Telecommunications System (NLETS)/Wanted Person Check

(c.) Citizen and Immigration Services Check (CIS)/e-Verify

(3) Non-US citizens who do not meet the three-year resident requirement and receive a favorable result on the required checks for initial access or entry of duty determination will receive a facility access card rather than a PIV card. GSA is currently developing the plan to issue facility access cards to such non-US citizens and other personnel groups.

(4) When a non-US citizen who previously did not meet the three-year resident requirement meets that requirement, the written inquiries portion of the NACI is required to be performed and a final determination decision made. The non-US citizen will then receive a PIV card.

e. Visitors.

(1) Visitors must comply with each GSA-controlled facility's access requirements.

(2) Some facilities may require a visitor to obtain a visitor badge (see par. 3c) and be provided with an escort while in the facility. Escorts are defined as employees and contractors who have received a favorable initial suitability decision and possess valid identification credentials (either a current PIV card or temporary badge and I-9 document). The escort is responsible for the whereabouts of the visitor.

(3) If the visitor leaves the premises, their visitor badge should become invalid and require them to reapply for a new visitor badge in order to reenter the facility.

f. Agencies supported by GSA.

(1) Certain small agencies, national committees, and presidential commissions are supported by GSA in handling their personnel processing. This support is coordinated through GSA's Agency Liaison Division (ALD).

(2) The employees and contractors of these agencies, committees, and commissions are subject to the same HSPD-12 requirements and procedures that are in use for GSA employees and contractors as described in this document.

g. Child care workers.

(1) All child care workers in Federal work places must meet the investigative requirements of the Crime Control Act of 1990, PL 101-647, Subtitle E, "Child Care Worker Employee Background Checks," as amended by PL 102-190. The background check must be:

(a.) Based on fingerprints taken by a law enforcement officer and other identifying information

(b.) Conducted through the FBI's Identification Division and through the State criminal history repositories in each state in which the child care employee has been resident or has listed in an employment application;

(c.) Initiated through the personnel program of the applicable employing agency

(2) The GSA Child Care Operations Division has worked with the Office of Homeland Security, Federal Protective Service (FPS) to ensure that all child care workers in Federal work places have gone through the security check process mandated by the Crime Control Act. However, the criminal history check is not the equivalent of the FIPS 201-mandated minimum NACI because it lacks the written inquiries component. Therefore, child care workers are not eligible for PIV credentials.

(3) Child care workers in Federal workplaces will receive facility access cards (FAC) to enable access to local facilities. The facility access cards will be compatible with, but both physically and electronically distinct from, the PIV card. GSA is currently developing the plan to issue facility access cards to child care workers and other personnel groups.

h. Volunteers. All volunteers who are affiliated with GSA and require access to federally controlled information systems and facilities must abide by the identity-proofing and registration requirements for GSA employees and contractors as defined in this guidance.

i. Retirees. In the past, special provisions were made to issue retirees with retired ID cards or alter their existing credentials so as to indicate that they were no longer active Federal employees. However, under the current HSPD-12 guidelines, retirees are no longer issued special retiree credentials, nor can they retain their existing credentials, even if the credentials are disabled (for example, punching a hole through the smart card chip) and/or altered (for example, stamping "Retired" across the face of the credential).

j. Foreign government visitors (J-visa holders).

(1) On occasion, GSA has foreign government visitors working for periods of up to 18 months on an exchange basis. The rules governing this program are managed by the Department of State Exchange Visitor Program (http://exchanges.state.gov/). Participants in this program are investigated by the State Department. Personnel investigation information on the participants can be accessed through the Student and Exchange Visitor Information System (SEVIS) of the Department of Homeland Security.

(2) Participants in this program with favorable investigations may be issued a contractor PIV card. J-visa holders are a different personnel group than non-US citizens and have different personnel investigation and credentialing requirements.

k. Employees and contractors detailed from other Federal agencies.

(1) Federal employees and contractors on detail from other Federal agencies with routine access to GSA-occupied facilities and/or IT systems must have the same level of personnel investigation as would be required of a GSA employee or contractor. If the detailee has already received a public trust certification or national security clearance at the appropriate level, then their manager or COTR should contact the OCHO/CPR (for employees) or HSPD-12 POC (for contractors) to request verification. Otherwise, the detailee's manager should follow the processes described in chs. 3 and 4 of this document to request the appropriate personnel security investigation and adjudication.

(2) Detailees will retain the credentials issued by their parent agency, including their agency-issued PIV-2-compliant card. Until such time as interagency authentication of Federal PIV cards becomes available, there may be instances where detailed employees and contractors need to be issued GSA PIV cards or other GSA credentials in order for

them to have access to GSA-occupied facilities and IT systems. In these cases, the individual's personnel investigation and prior adjudication with the parent agency must be verified before a GSA PIV card is issued to them. (See ch. 2-6, which identifies CPR as the office that verifies the prior investigations and adjudication results.)

l. Presidential transition staff. Presidential transitions staffs include large numbers of campaign staff, security personnel from various Federal agencies, and volunteers. GSA provides administrative support to the transition, including acquisition of office space, IT support, and payment of official transition staff. GSA will coordinate with all campaigns to ensure that credentialing requirements are known prior to Election Day. Official transition staff will require PIV cards immediately, and GSA will make arrangements to provide credentialing enrollment and activation equipment and personnel security representatives as close to the transition site as possible to expedite fingerprint capture and personnel investigation submission. Volunteers will follow standard HSPD-12 guidelines or be treated as visitors requiring escort, depending on duties assigned by the transition staff.

m. Federal Emergency Response Official (FERO). Requests for Federal Emergency Response Officials (FERO) designation for GSA Central Office employees and contractors are submitted by their PIV sponsor and approved by the Office of Emergency Response and Recovery (OERR). Requests for FERO designation for all other GSA employees and contractors are submitted by their PIV sponsor and approved by the regional emergency coordinator for that individual's region. If a request for FERO designation is approved, the card holder will have "Emergency Response Official" printed within a red stripe at the bottom of their PIV card. A FERO designation is restricted to government-wide emergency responders who will staff a Multi-Agency Coordination Center as identified by Federal agencies to the DHS Federal Emergency Management Agency (FEMA) or otherwise when approved by the regional emergency coordinator.

3. Available GSA credentials.

a. PIV card.

(1) The PIV card is the Federal identity card mandated for use in authenticating access to physical and logical agency resources in accordance with Homeland Security Presidential Directive 12 (HSPD-12). (See http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html for the complete directive) The PIV card is credit-card sized, with one or more embedded integrated circuit chips (ICCs) that provide memory capacity and computational capability. Its form and functionality are defined by NIST standards and publications including FIPS 201-1, and NIST publications SP800-73, SP800-76, and SP800-78. (See link to NIST Special Publications in fig. 1-3).

(2) Data stored in the card or displayed on its face include a digital photograph, name, agency affiliation, contact information, fingerprint templates, expiration date, and other data associated with the cardholder. Multiple PKI digital certificates that can be used for electronic authentication, digital signing, and digital encryption are included on the PIV card.

(3) The fingerprints captured during the enrollment process are placed as a digital file on the chip of the PIV card. This biometric data is used to identify cardholders uniquely

by comparing the cardholder's fingerprints with the fingerprint data stored on the PIV card. A successful comparison guarantees a very high level of trust in the identity of the cardholder, thus confirming that the person presenting the card is the actual cardholder. The scanned fingerprints are stored as "minutiae templates" (key points for comparison) on the chip of the card and can only be read from the card after providing the card PIN. To protect cardholder privacy, the actual fingerprint images are not stored on the card. Minutiae templates cannot be used to reconstruct the original fingerprint images, thus mitigating concerns of privacy even if the card is lost or stolen.

(4) The PIV card should be issued to all GSA employees and to all contractors who need routine access to GSA IT systems and GSA-occupied facilities for more than 6 months. It can be issued to other contractors and affiliates as deemed necessary for GSA as described in this document.

(5) The PIV card cannot be issued until an individual has received favorable results of an initial suitability check that includes an FBI fingerprint check and the submission of a personnel investigation request at the minimum level of a NACI.

(6) The maximum expiration date for a GSA PIV card is 5 years from the date of issuance.

(7) PIV cards do not contain any company-specific information for contractors. As a result, a contractor may reuse an unexpired PIV card when moving between contractor companies without a break in work at GSA. If there is a break, the PIV card must be returned to GSA. GSA may then reissue the same card or a new card to the contractor when they start working for a new company.

(8) Note: In the future, for the PKI digital certificates on a GSA PIV card to work properly for logging onto GSA IT networks, the UPN (User Principal Name) data field in the MSO PIV card request must be set properly. It must match the individual's unique identifier in the GSA IT network directory service. As a result, the GSA HSPD-12 PMO will generate the UPN for each PIV card applicant and provide the data to IT security.

b. <u>Temporary credentials.</u>

(1) Temporary badges may be issued to individuals who have received at least a favorable initial suitability decision and are eligible to receive a PIV card. Employees and contractors awaiting issuance of their PIV card can use the temporary badge in place of a PIV card when entering GSA-managed buildings after signing in and providing a suitable government-issued photo ID. In addition, if an employee or long-term contractor forgets his/her card on a particular day, or if the person is waiting for a replacement PIV card, they can also be issued a temporary badge after their identity has been confirmed.

(2) The design of temporary badges must make the badges physically and electronically unique and easily differentiated from a PIV card. The badge holds no photo or biometric data for the employee/contractor. This practice eliminates the possibility of mistaking temporary badges for valid PIV cards.

(3) When accessing a GSA-controlled facility that restricts entry, the process of using a temporary badge must include identity verification of the individual. A government-issued picture ID must be verified before allowing individuals with temporary badges

into GSA facilities. Any sign-in procedures established for that facility should be followed.

(4) Employees and contractors can request a temporary badge directly from a regional credentialing officer (RCO). Regional credentialing officers must verify the individual's identity and that the individual has received a favorable initial or final suitability decision. A temporary badge must be returned in order to receive a PIV card and should not be used for more than 30 days without verifying the need for its continued use.

(5) Credentialing officers can obtain a supply of temporary badges from the HSPD-12 PMO.

c. Visitor credentials.

(1) Visitor credentials should be issued in accordance with the procedures approved by the facility's Building Security Committee (BSC). GSA employees and contractors without their GSA-issued credentials should follow the procedures for visitors.

(2) In some GSA-occupied spaces, visitors are required to be issued a visitor badge. Before issuing a badge, the visitor's identity should be checked by visual and/or electronic inspection of a government picture ID, a state driver's license, or other photo ID.

(3) If the visitor leaves the premises, their visitor badge should become invalid and require them to reapply for a visitor badge in order to reenter.

d. Regional credentials.

(1) Regional credentials are identity cards issued by regional organizations within GSA. They indicate the regional affiliation of the cardholder and have been authorized for use by RAs and/or HSSOs. In some cases, regional cards also function as physical access cards for opening door locks or entry/exit gates to GSA buildings and facilities.

(2) Over time, regional credentials will be phased out in favor of the agency-wide PIV card. Nonetheless, regional cards that are used for physical access will be retained until the associated building physical access systems (PACSs) are upgraded to be compatible with the national PIV card.

e. Local and building-specific credentials.

(1) Local credentials and building-specific credentials are cards used for access to specific buildings and/or GSA-controlled facilities. They may or may not indicate the identity of the registered cardholder on their face. They are issued in accordance with BSC rules for individual buildings and facilities as well as any applicable RA- and SSO-defined requirements.

(2) Over time, these cards will be phased out as their associated building or facility PACS are upgraded to be compatible with the national PIV card.

f. Older, noncompliant GSA PIV cards.

(1) GSA has issued national identity cards over many years, many of which are still held by current GSA employees and contractors. The FIPS 201 standard defines two levels of PIV cards, called PIV-1 and PIV-2. Between October 2005 and September

2007, GSA issued PIV-1 compliant cards. Since then, GSA has issued PIV-2 complaint cards.

(2) Beginning in September 2007, GSA has been issuing PIV-2 compliant cards provided through the GSA HSPD-12 MSO and phasing out the issuance of all other PIV-1 and PIV-2 cards.

(3) In accordance with HSPD-12 guidelines, all older national identity cards, PIV-1 cards, and non-MSO PIV-2 cards at GSA must be replaced by MSO-provided PIV-2 cards by April 1, 2009. In order to comply, current PIV cardholders will have to be "enrolled" into the MSO system. This involves being refingerprinted and photographed in order to have this biometric data placed on the new MSO-issued PIV-2 cards.

(4) Current PIV cardholders without a favorable personnel investigation on record will also have to have an appropriate personnel investigation submitted and receive favorable results on the FBI fingerprint check before receiving a replacement MSO-issued PIV-2 card.

g. Retiree credentials. In the past, special provisions were made to issue retirees with retired ID cards or alter their existing credentials so as to indicate that they were no longer active Federal employees. However, under the current HSPD-12 guidelines, retirees are no longer issued special retiree credentials, nor can they retain their existing credentials, even if the credentials are disabled (for example, punching a hole through the smart card chip) and/or altered (for example, stamping "Retired" across the face of the credential).

4. Required background checks.

a. National security positions vs. suitability positions.

(1) GSA positions that require employees to work with classified national security information are called "national security positions." All other positions fall under the government's suitability program and are called "suitability positions." Suitability positions can have three levels of risk: low, moderate, or high. Suitability positions with a moderate or high risk level are known as "public trust positions." The GSA Central Office Human Resources Division (CPS) and CPR assign levels of risk to the suitability positions for employees according to the impact their incumbents may have on the public trust.

(2) GSA managers can decide whether their positions require higher suitability levels than those assigned by CP. Further, managers can decide whether their positions require national security designations.

(3) GSA requires all employees to undergo personnel investigations to determine their basic suitability for Federal employment. In addition, employees getting national security clearances must meet the security criteria established under EO 12968 and Director of Central Intelligence Directive 6/4. Those persons receiving special clearances from other agencies must satisfy those agencies' criteria.

(4) GSA only employs persons who are suitable for Federal employment (in accordance with guidelines defined in 5 CFR 731.101), and grants national security clearances only to persons whose employment is clearly consistent with the national

security interest. GSA makes suitability and security determinations based on the investigations and any subsequent due process.

(5) The types of personnel investigations that can be requested are set out in fig. 2-4.1, below.

Figure 2-4.1. Types of personnel investigations

Type of Personnel investigation or Check	Description
ANACI: Access National Agency Check and Inquiries	An investigation meeting the requirements of EO 12968 for granting a Secret or Confidential national security clearance.
BI: Background Investigation	An investigation covering specific areas of a person's background. The BI consists of record searches, credit search, and a NAC. The investigating agency interviews the candidate and selected sources.
LBI: Limited Background Investigation	An investigation covering specific areas of a person's background. The investigating agency interviews the candidate and selected sources. The agency also conducts record searches and credit checks covering the past 5 years, and completes a NAC.
MBI: Minimum Background Investigation	The investigating agency interviews the candidate and completes an NACI with Credit.
NACI: National Agency Check with Inquiries	An investigation consisting of a NAC and written inquiries covering specific areas of a person's background during the past 5 years.
NACLC: National Agency Check with Law and Credit	An investigation for recertifying Secret and Confidential national security clearances.
PRI: Periodic Reinvestigation	An investigation completed every fifth year on persons in high public trust and police officer positions. It includes a NAC, subject interview, record searches, credit check, and resolution of issues raised since the last investigation.
PPR: Phased Periodic Reinvestigation	An investigation for re-certifying Top Secret national security clearance.
SSBI-PR: Periodic Re-Investigation for SSBI	An investigation for re-certifying Top Secret national security clearance.
SSBI: Single Scope Background Investigation	An investigation meeting the requirements of EO 12968 for granting a Top Secret security clearance.

b. Risk levels for suitability positions.

(1) Employees and contractors are evaluated for suitability positions in accordance with the suitability standards and criteria described in 5 CFR Part 731. Suitability refers to character and behavior. It does not include a person's qualifications, such as experience or ability. To determine whether a person satisfies the suitability criteria, GSA assigns risk levels and requests the appropriate investigations.

(2) GSA assigns one of three risk levels to each employee position. The level of risk associated with a specific employee position is determined by the position description for

employees and the actual duties assigned. The level determines what investigation the agency requests for the candidate for the position. GSA uses the investigation to decide whether the person is suitable for Federal employment. The position's risk level determines the relative seriousness with which adjudicators view issues developed in the investigation.

(3) In general, contractors should be assigned the same risk level as a GSA employee performing the same duties. The level of risk for a contractor position is determined by the contracting officer or a GSA employee designated to act for the contracting officer such as a Contracting Officer's Representative (COR) or COTR and is dependent upon the actual duties assigned, the risk level of a comparable employee position, and any relevant language specified in the related contract.

(4) Those individuals whose duties require a higher degree of trust, such as IT system administrators, those who handle financial transactions, or those who deal with PII, and other sensitive information (e.g., building drawings, etc.), will continue to require investigations associated with higher levels of trust such as the Minimum Background Investigation (MBI) or the Limited Background Investigation (LBI). (See figs. 2-4.2 and 2-4.3 for computer related positions.)

Figure 2-4.2. Minimum risk levels for suitability positions

(from GSA Order ADM P 9732.1C)

Risk Level	Criteria
Level 6 **High Risk** **Public Trust Position**	Positions with duties especially critical to GSA • Senior Executive Service positions and Board Of Contract Appeals judges • Criminal Investigator, occupation series 1811 • Schedule C positions in the Office of the Administrator • GSA-wide policy development and implementation • Higher level management assignments • Independent spokespersons with authority for independent action • Major computer systems positions with broad scope and authority that are especially critical to GSA's mission (see fig. 2-4.3)
Level 5 **Moderate Risk** **Public Trust Position**	Positions with duties of considerable importance to GSA • Police, occupation series 0083 (require LBI) • Auditing, occupation series 0511 (require BI) • All Schedule C positions not in the Office of the Administrator • Assistants to GSA-wide policy development and implementation • Mid-level management assignments • Positions with authority for independent or semi-independent action • Major computer systems positions involving duties of considerable importance to GSA's mission (see fig. 2-4.3)
Levels 2-4	**National Security Positions (not part of Suitability Positions)**, see fig. 2-4.4 below.
Level 1 **Low Risk**	All other positions.

Figure 2-4.3. Risk Levels for Computer System Positions

(from GSA Order ADM P 9732.1C)

Risk Level	Criteria
High	Develops and administers computer security programs, and directs and controls risk analyses or threat assessments. Significantly involved in life-critical or mission-critical systems. High risk for doing grave damage to a sensitive system or realizing significant personal gain, even if the positions duties do not include personal access to the system. High risk assignments that involve accounting for or disbursing: • At least $10 million per year; or • Any amount if a higher authority does not do technical reviews of the employees activities on the system. Major responsibility for directing, planning, designing, testing, maintaining, operating, monitoring, or managing systems hardware and software.
Moderate	Designs, operates, tests, maintains, or monitors systems that are under technical review by higher authority and that involve: • Accounting for or disbursing less than $10 million per year; • Accessing data protected under the Privacy Act of 1974 (employees who are accessing their own identifying information do not require this risk level).; or • Accessing proprietary data or Government-developed privileged information involving contract awards. Moderate risk for damaging a system or realizing personal gain.
Low	All other positions.

(5) For those individuals accessing or administering information systems, risk determination is partly based on security categories from FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems." OPM has issued criteria for determining the risk levels of positions whose duties include working on Federal computer systems. These criteria do not affect employees working on stand-alone computers or on computer systems that do not contain sensitive information as described in the Computer Security Act of 1987 (P.L. 100-235). Criteria for determining risk levels for computer system positions should be based on the sensitivity of the position assigned and not just the FIPS 199 classification of the IT system itself. (See figs. 2-4-b(4)-1 and 2-4-b(4)-2 for suggested levels for computer-related positions.)

(6) See par. 4d for the relationship between risk levels and personnel investigations for employees and contractors.

c. Risk levels for national security positions. Fig. 2-4.4 summarizes the relationship between risk levels, national interest, and required minimum investigation.

(1) Positions whose duties require employees or contractors to work with classified national security information (Top Secret, Secret, or Confidential) are national security positions.

(2) Employees must be granted national security clearances by the GSA CPR, which uses personnel investigations as the basis for granting the clearances. National security clearances for contractors are processed by the Defense Industrial Security Clearance Office (DISCO). (See ch. 4 for more information.)

(3) GSA does not grant security clearances to employees who do not actually access classified information. CPR may cancel security clearances for employees who have not worked with classified information within the past 5 years. If cleared employees have accessed only information classified at a lower level than their security clearances within the past 5 years, CPR may downgrade their clearances.

(4) If the employees do not routinely work with classified information, but their managers feel that they could require access at some time during their tenure, the managers may designate the positions as national security positions, with eligibility for access. GSA does not grant security clearances to these employees, but if the employees ever need access to classified information, their managers contact CPR to activate national security clearances.

(5) All employees must meet GSA's employment suitability requirements in order to work at GSA. In addition, persons whose duties require access to classified national security information must satisfy the security standard and criteria described in EO 10450, Sec. 8(a).

(6) The national security designations replace the default public trust designations, and the candidate completes SF86, "Questionnaire for National Security Positions," rather than the SF85P, "Questionnaire for Public Trust Positions," or SF85, "Questionnaire for Non-sensitive Low Risk Positions." For instance, a criminal investigator position is a high risk position by default. However, if the employee requires access to Secret national security information, the manager converts the high risk public trust position to a noncritical sensitive national security position.

(7) CPR compares the investigative requirements of the default public trust level with the investigation required for the national security designation and requests the higher investigation. Thus, in our example for the investigator, CPR requests a BI. (See subpar. d, below for the relationship between sensitivity levels and personnel investigations for employees.)

(8) The risk level and type of access needed determine whether the candidate may be placed into the position before CPR grants the clearance. GSA uses the personnel investigation to decide whether employing the person is clearly consistent with national security. The position's sensitivity level determines the relative seriousness with which adjudicators view issues developed in the investigation.

Figure 2-4.4. Minimum risk levels for national security positions

(from GSA Order ADM P 9732.1C)

Risk Level	National Interest	Minimum Investigation
Level 4 **Special Sensitive**	Access Under Director of Central Intelligence Director (DCID) 1/14, or a similar special access program. (GSA grants a Top Secret national security clearance.)	SSBI (Pre-appointment for certain SES positions and critical-sensitive Schedule C positions)
Level 3 **Critical Sensitive**	Access to Top Secret national security information (Top Secret clearance); or Eligibility for access to Top Secret information (no security clearance).	SSBI (Pre-appointment for certain SES positions and critical-sensitive Schedule C positions)
Levels 2 **Non critical-Sensitive**	Employment in a High Risk public trust position and access to Secret national security information (Secret security clearance).	BI
Level 2 **Non critical sensitive**	Employment in a Moderate or Low Risk public trust position and access to Secret national security information (Secret security clearance).	LBI or MBI (Depending on position description)

---

d. Personnel investigations and forms. Figs. 2-4.2 and 2-4.4 identify the risk level, sensitivity level, type of investigation, and appropriate standard forms required for national security and suitability positions. Notice that there are separate requirements for employees and contractors.

Figure 2-4.5. Employees: Risk levels, sensitivity levels, investigations & forms

(Standard forms can be found on the GSA Forms Library at http://insite.gsa.gov/ "Reference & Resources" tab, under the GSA Forms or access directly through: http://www.gsa.gov/Portal/gsa/ep/formslibrary.do?formType=SF)

Sensitivity Level	Type of Investigation	SF Required
Low Risk, Non-Sensitive (Level 1)	NACI: National Agency Check with written Inquiries	SF85: Questionnaire for Non-sensitive Low Risk Positions
Non-Critical (Level 2)	ANACI: Access National Agency Check and Inquiries	SF86: Questionnaire for National Security Sensitive Positions
Critical Sensitive (Level 3)	SSBI: Single Scope Background Investigation	SF86: Questionnaire for National Security Positions
Special Sensitive (Level 4)	SSBI: Single Scope Background Investigation	SF86: Questionnaire for National Security Positions
Moderate Risk (Level 5)	MBI: Minimum BI, or LBI: Limited BI	SF85P: Questionnaire for Public Trust Positions
High Risk (Level 6)	BI: Background Investigation:	SF85P: Questionnaire for Public Trust Positions

Figure 2-4.6. Contractors: Risk levels, investigations, & forms

Sensitivity Level & Contract Type	Type of Investigation	Forms Required
Child Care Workers	State Repository Checks Law Enforcement Checks	CIW: Contractor Information Worksheet DHS 176T: Statement of Personal History for Childcare Personnel (DHS 176T is a temporary form and currently under review. The use of this form is subject to change in the future depending on the outcome of the review) Quick Name Check Form Pre-Employment
Low Risk, Non-Sensitive (Level 1) for Temporary Contractors, not needing PIV Cards	Law Enforcement Checks	CIW: Contractor Information Worksheet DHS 176T: Statement of Personal History for Contractors or SF85P: Questionnaire for Public Trust Positions
Low Risk, Non-Sensitive (Level 1) for Temporary Contractors, needing PIV Cards	NACI: National Agency Check with written Inquiries	CIW: Contractor Information Worksheet SF85P: Questionnaire for Public Trust Positions
Low Risk, Non-Sensitive (Level 1) for Long-term contractors	NACI: National Agency Check with written Inquiries	CIW: Contractor Information Worksheet SF85P: Questionnaire for Public Trust Positions
Level 2-4	National Security investigations for contractors, see ch. 4	See ch. 4.
Moderate Risk (Level 5)	LBI: Limited Background Investigation, or MBI: Minimum Background Investigation	CIW: Contractor Information Worksheet SF85P: Questionnaire for Public Trust Positions GSA 3665: Authorization to Obtain Credit Report
High Risk (Level 6)	BI: Background Investigation	CIW: Contractor Information Worksheet SF85P: Questionnaire for Public Trust Positions GSA 3665: Authorization to Obtain Credit Report

e. Reinvestigations.

(1) GSA requires reinvestigations for all employees who hold national security clearances. CPR schedules a periodic reinvestigation for SSBI (SSBI-PR) during the 5th year after the last investigation on every employee in a special- or critical-sensitive position with a Top Secret security clearance or Top Secret eligibility. The CPR

schedules a NACLC during the 10th year after the last investigation on every employee with a Secret security clearance and in the 15th year for every employee with a Confidential security clearance.

(2) For suitability positions, in accordance with the Computer Security Act of 1987 and OMB Circular No. A–130 Revised, agencies may require incumbents of certain public trust positions to undergo periodic reinvestigations. The appropriate level of any reinvestigation will be determined by the agency but may be based on supplemental guidance provided by OPM. (From 5 CFR 731.106 (d) "Suitability reinvestigations")

(3) If a position's minimum public trust level is high risk or if it is a moderate risk law-enforcement position, CPR requests a Periodic Reinvestigation (PRI) instead of the NACLC during the 5th year after the last investigation. (From GSA Order ADM P 9732.1C 2.9 "Periodic Reinvestigation (PRI)." GSA does not reinvestigate other moderate risk positions nor any low risk positions.

5. Privacy considerations.

a. Throughout the HSPD-12 process, PII is being collected, reviewed, and evaluated by GSA staff as well as by external Federal organizations and their staffs, supporting GSA in this process (e.g., DHS ICE/FPS and OPM). It is crucial that an individual's PII data be properly protected at every point in the process and by every person involved. PII data used on forms and included in HSPD-12 personnel investigation and credentialing requests includes Social Security Number (SSN), date of birth (DOB), and place of birth. (From GSA Instructional Letter HCO IL-07-1 "GSA Data Release Policy", 9 "Non-releasable information")

> "Privacy protection is both a personal and fundamental right of individuals, including GSA employees, clients, and members of the public, whose personal information is collected, maintained, and used by GSA organizations to carry out agency mission and responsibilities and to provide services. It is the policy of GSA to safeguard personal information as mandated by law and regulation." (From GSA Order CPO 1878.1 "GSA Privacy Act Program", 2 "Policy")

b. The basic principles to be followed for protecting privacy within the HSPD-12 process are straightforward:

(1) Individuals being asked to provide personal information must be informed as to whether that information is optional or required, what will be done with the information, and what the consequences are of not providing the information.

(2) GSA staff must be specifically designated to handle HSPD-12 related PII data, and these individuals must have specific training appropriate to their access to PII data.

(3) Paper forms containing PII data must be stored and transmitted in accordance with the GSA IT Security Policy and, in general, be protected from any unauthorized disclosure.

(4) GSA IT systems supporting HSPD-12 must store and transmit PII data securely and, in general, protect it from any unauthorized disclosure; in addition, HSPD-12 IT

systems must file a Privacy Impact Assessment (PIA) with the Privacy Office and a System of Record Notice (SORN) in the Federal Register indicating the nature of the data stored, the purpose of its collection, and its use.

c. These principles are implemented in the HSPD-12 process in the following ways:

(1) Privacy Act Statement for all HSPD-12 related forms. All forms used in the HSPD-12 process include a Privacy Act statement that indicates what PII data is to be collected, the purpose for its collection, whether it is optional or required, and what the consequences are of not providing the requested information.

(2) PIA: All GSA IT systems must complete a PIA and file it with the Privacy Office.

(3) SORN for all HSPD-12 related IT systems: All GSA IT systems have and will continue to provide SORNs to the Federal Register as required.

(4) All HSPD-12 related GSA staff are specifically designated. All GSA staff who have access to HSPD-12 related PII data must be specifically designated to perform their duties by an authorized GSA official.

(a.) For new employees, HROs are designated to collect information for the personnel investigations and the initial credential requests as part of their standard duties; likewise, CPR staff as part of their standard duties are already assigned to assist with personnel investigation requests and make suitability decisions.

(b.) For contractors, COs must designate in writing, for each contract, the GSA employee who is to act as the requesting official for that contract, who is thereby authorized to make all appropriate requests for personnel investigations and credentials; likewise, HSPD-12 Points of Contact (POCs) must be specifically assigned their duties by their SSOs.

(5) Mandatory training for all HSPD-12 related GSA staff. Many GSA staff handling HSPD-12 related PII data already have privacy training as part of the standard training for their positions; this includes HROs, CPR staff, and COTRs/CORs acting as requesting officials for contractor requests. All other requesting officials and all HSPD-12 POCs must have appropriate training in privacy issues and considerations. This means taking the Privacy Training 101 course currently available on the GSA Online University and any additional training programs that are developed in the future. ("Privacy Training 101" course is available through GSA Online University at http://gsaolu.gsa.gov.)

(6) Secure transmission and storage of HSPD-12 related paper forms. Some employees and contractors will continue to provide personnel investigation requests and supporting information on paper to HROs, requesting officials and HSPD-12 POCs. In those cases, GSA staff must store the paper forms in a secure location. Forms must not be left on desktops or in places visible to other GSA staff or visitors. If transmitted by fax, forms must go to a designated and secure location, e.g., at an FPS regional office; if forms are scanned and transmitted by e-mail, form files must be encrypted (e.g., by WinZip); otherwise, they must be sealed securely and sent by a parcel service or messenger to a secure mail reception location.

(7) Recommended use of OPM's e-QIP system. In order to avoid GSA staff handling more PII data than is necessary, applicants for employee and contractor positions should

use the OPM's Electronic Questionnaires for Investigations Processing (e-QIP) system to fill out standard forms such as SF85, SF85P, or SF86. Doing so reduces the amount and nature of information about an individual's background that needs to be handled by GSA staff.

(8) Secure transmission and storage of electronic versions of HSPD-12 related PII data.

(a.) The CHRIS Security Tracking System (STS) tracks personnel investigation requests for employees and has appropriate security and privacy controls in place as documented in its certification and accreditation (C&A) results; this data is not transmitted to any other system. The SORN for this system is GSA/HRO-37 (Security Files – HSPD-12).

(b.) The HSPD-12 GCIM (GSA Credential and Identity Management) system tracks contractor personnel investigation requests and credentialing requests; upon completion, its C&A process will verify that PII data is encrypted while stored in its database and whenever it is transmitted to systems operated by HSPD-12 process partners, MSO, and FPS. The SORN for this system is GSA/CIO-1 (GSA Smartcard Program – HSPD-12).

(c.) Any future system designed by the HSPD-12 PMO will have appropriate requirements and testing for appropriate privacy controls, e.g., encryption of PII data in databases and in Web service messages sent to other Federal organizations.

(9) The above provisions for implementing privacy controls for the HSPD-12 process are incorporated in the appropriate sections of this document.

6. Additional considerations.

a. Individuals with prior investigations at GSA. In general, HSPD-12 implementation guidelines specify that Federal agencies shall not readjudicate employees or contractors with previous personnel investigations. GSA will not require a new personnel security investigation for new employees and contractors provided:

(1) The individual has undergone the same level or higher investigation than the one required for the new job.

(2) The investigation was completed and the adjudication results were favorable.

(3) For employees, there has been less than a 2-year break in service with GSA; for contractors, it has been less than 2 years since the end of their last contract at GSA.

b. Reciprocity with other Federal agencies. In general, HSPD-12 guidelines specify that Federal agencies shall not readjudicate employees or contractors with previous personnel investigations at another Federal agency. GSA will not require a new personnel security investigation and adjudication for new employees and contractors provided:

(1) CPR (for employees) or FPS (for contractors) must be able to verify the prior investigation and the associated adjudication results with OPM and/or the agency that performed the adjudication.

(2) The individual has undergone the same level or higher investigation than the one required for the new job at GSA.

(3) The investigation was completed and the adjudication results were favorable.

(4) For employees, there has been less than a 2-year break in service from the agency that adjudicated the investigation; for contractors, it has been less than 2 years since the end of their last contract with the agency that adjudicated the investigation, unless derogatory information that was not previously adjudicated becomes known to the granting agency.

c. PBS vs. non-PBS contractors.

(1) In general, PBS and non-PBS contractors are subject to the same HSPD-12 requirements for personnel investigations and GSA credentialing.

(2) However, there are minor differences in the handling of personnel investigation requests sent to FPS due to their being administered by separate MOAs and instructions. (See ch. 1-3 for links to FPS instructions). For example, requests are sent to different FPS offices depending on whether a PBS contractor or a non-PBS contractor is to be investigated. Likewise, FPS tracks which requests are for PBS as opposed to non-PBS contractors and bills separately for each under the terms of the appropriate MOA.

(3) Nonetheless, in all essential respects, PBS and non-PBS contractors should be processed and credentialed in the same way and subject to the same GSA and HSPD-12 requirements.

d. Temporary contractors requiring access to GSA IT systems. Temporary contractors (i.e., those requiring routine access for 6 months or less) needing access to GSA IT systems must abide by the same personnel investigation requirements for IT access as GSA employees and long-term contractors. This includes the requirement that initial or full IT access is granted by the authorizing official after verifying that the employee or contractor has an ANACI, NACLC, SSBI, or other acceptable level of investigation or clearance. If the authorizing official does not grant an employee or contractor initial or full access to GSA IT systems, initial IT access is granted only after receiving a favorably adjudicated FBI fingerprint check, and full IT access is granted only after a favorably adjudicated personnel investigation (at the minimum level of a NACI). COs, COTRs, or their designees may submit waiver requests to grant contractors initial IT access before GSA receives the results of the fingerprint check. (See ch. 6-4 for additional information, including guidelines and procedures for submitting waiver requests.)

e. Current employees and contractors without verifiable background check.

(1) All current GSA employees and long-term contractors must to have a suitable personnel investigation completed or in process by October 27, 2008, in accordance with HSPD-12 guidelines.

(2) Many employees and long-term contractors who joined GSA after October 27, 2005 have had an appropriate investigation and adjudication conducted when they joined GSA; those who did not must have one completed or in process by October 27, 2008.

(3) Employees and contractors who joined GSA before October 27, 2005 may not have a NACI or other suitable investigation on record. In some cases, an individual may have already had an investigation but one that cannot be verified, or that investigation may not meet the HSPD-12 minimum standard of a NACI. In particular, since OPM does not

retain investigation results for more than 15 years, employees and contractors for whom OPM conducted an investigation more than 15 years ago will not be able to verify that investigation.

(4) Regardless of the reason, any employee or long-term contractor who does not have a verifiable investigation must have a new investigation completed or at least submitted by October 27, 2008.

CHAPTER 3. CREDENTIALING PROCEDURES FOR EMPLOYEES

1. Roles and responsibilities in employee process. Fig. 3-1 summarizes the roles and responsibilities of the entities involved in the credentialing procedures for employees.

a. Employee. An employee is an individual who is employed by GSA and currently assigned to a position in GSA, or who has accepted a tentative offer of employment with GSA, with final employment offer contingent upon favorable results from the FBI fingerprint check. The appointment may either be permanent or temporary.

(1) Employees must provide all information and biometric data needed for personnel investigations and credentialing requests.

(2) Employees must present themselves at the designated MSO Enrollment Center at the scheduled time; at that time, the employee must provide two identity source documents in original form. The documents must be on the list of acceptable documents included in I-9, OMB No.1115-0136, "Employment Eligibility Verification." (See Attachment F.) One of the documents must be a valid (not expired) picture ID issued by a State government or the Federal Government.

(3) After receiving a favorable initial suitability decision or verification of an existing favorable suitability decision, employees must present themselves at the designated MSO/GSA Activation Point in order to receive their PIV card and activate it, and employees are required to verify their identity upon request.

(4) The employee fulfills the FIPS 201 Applicant role.

b. HRO.

(1) The Human Resource Officer (HRO) requests personnel investigations and credentials for new employees and is responsible for the following:

(a.) Contacting the candidate to make a tentative offer of employment and ensuring that the candidate understands that a final employment offer is contingent upon the return of the completed personnel investigation forms and favorable results from the FBI fingerprint check. The candidate must also be informed that continued employment is contingent upon a favorably adjudicated personnel investigation.

(b.) Reviewing all newly selected employee-provided information and requesting low risk personnel investigations.

(c.) For low risk, non-sensitive positions, ensuring that SF85 and other appropriate security forms are filled out by the new employee, reviewed, and submitted to OPM.

(d.) For moderate/high risk public trust positions and all national security positions, setting up personnel investigation requests in OPM's e-QIP system and ensuring that SF85P/SF86 and other appropriate security forms are submitted to CPR for processing by OPM.

(e.) Requesting a PIV card for a new employee.

(2) Under extenuating circumstances, the HROs can forward fingerprint cards for newly selected Federal employees in advance of submission of SF85 only directly to OPM for advance processing under the GSA and OPM Special Agency Check (SAC) agreement in order to expedite the fingerprint check for initial access entry-on-duty requirements. Remaining documents need to be delivered with 120 days of OPM's receipt of the fingerprint cards.

(3) The HRO will be notified of all adjudication results for new employees.

(4) The HRO fulfills FIPS 201 PIV Sponsor role for new employees.

c. Employee supervisor.

(1) Make requests for renewing or replacing PIV cards for employees under their supervision.

(2) When an employee is separating from GSA, is responsible for the employee returning all GSA-issued credentials.

d. HSPD-12 POC.

(1) The HSPD-12 POC is responsible for assisting HROs in making MSO requests for fingerprinting and PIV card issuance for a new employee.

(2) The HSPD-12 POC is responsible for making all PIV card maintenance requests for employees, including card replacements and renewals.

(3) The HSPD-12 POC fulfills the MSO Sponsor role for all MSO-related fingerprinting and PIV card requests.

e. Personnel Security Requirements Division (CPR).

(1) CPR is the primary GSA office responsible for direction, guidance, and interpretation of HSPD-12 personnel investigation requirements for GSA employees and contractors.

(2) CPR publishes the instructions for processing personnel investigations for employees and contractors.

(3) CPR will update, monitor, and maintain security investigation tracking in CHRIS PSTS data system. (Step-by-step instructions for entering information in to CHRIS PSTS are found in Attachment E.)

(4) CPR reviews all moderate risk and higher personnel investigations and all national security clearance requests for employees before forwarding them to OPM; CPR will

notify HROs, or requesting official, when a submitted security package needs additional information or corrections.

(5) All OPM investigation results for employees are sent to CPR and then adjudicated by a Security Specialist.

(6) CPR will report the favorable results of the FBI fingerprint check to the HRO, Staff or Regional HRO Security mailbox, HSPD-12 PMO (hspd12.security@gsa.gov), and IT Security (ITSecurity@gsa.gov).

(7) For employees with a previous personnel investigation, CPR will contact the former Federal agency to determine the current level of security clearance/personnel investigation and obtain the certification date of the investigation. (See par. 2b for details.)

(8) CPR will notify the HRO, Staff or Regional HRO Security mailbox, HSPD-12 PMO, IT Security Office, the individual, and the supervisor when the appropriate personnel investigation is finally adjudicated and completed.

(9) CPR can be reached at gsa.securityoffice@gsa.gov.

(10) CPR fulfills the FIPS 201 PIV Registrar role for GSA employees.

f. Fingerprint service provider. The fingerprint service provider should correctly identify I-9 form credentials and perform fingerprint services as regulated by government procedures. The fingerprint service provider can be any of the following:

(1) Police station

(2) GSA OCHCO

(3) Any other entity entitled to provide fingerprint services

g. MSO.

(1) MSO is responsible for all project, acquisition, and financial management necessary to provide end-to-end service for the production of PIV-2 compliant credentials to GSA employees and contractors.

(2) MSO is responsible for:

(a.) Providing credentialing centers for the enrollment of employees and activation of PIV cards.

(b.) During enrollment, taking and storing an employee's biometrics (fingerprints and photo) after verifying the identity of the employee.

(c.) In the future, after enrollment, sending an employee's fingerprints to OPM and FBI for processing if needed for a personnel investigation.

(d.) Printing PIV cards and securely shipping them to the requested Activation Point.

(e.) At an MSO Activation Point, verifying the identity of the employee, issuing a PIV card, and supervising the activation of the PIV card by the employee.

(f.) MSO fulfills the FIPS 201 roles of PIV Registrar, PIV Issuer and PIV Digital Signatory; its PKI provider is the FIPS 201 PIV Authentication Certification Authority.

h. PMO.

(1) PMO is responsible for overall coordination of the HSPD-12 process implementation at GSA.

(2) PMO receives the employee adjudication results, forwards them on to GSA IT Security as needed, and acts as the MSO Adjudicator recording with the MSO a favorable initial suitability decision, thereby enabling the printing and activation of a contractor's PIV card.

(3) PMO has a help desk that can be reached at HSPD12PMO@gsa.gov.

(4) PMO fulfills the MSO Adjudicator role.

i. OPM. OPM performs the personnel investigations requested by HRO or CPR for GSA employees.

j. FBI. FBI performs the fingerprint and name checks requested by HROs and CPR.

k. MSO security officer. The MSO security officer is a GSA-designated executive responsible for the overall security of the MSO shared solution.

(1) The MSO security officer will be able to view system security reports, investigate, and resolve system security-related issues identified by the MSO shared solution system. For example, when duplicate fingerprints are detected and the scope spans more the one agency, the MSO security officer will investigate the reports and work with other GSA security officials to resolve the duplicate fingerprint issue.

(2) The MSO Security Officer will also be the point of contact to the Office of the Inspector General (OIG) and will respond to requests from agencies for follow-up action on instances of unauthorized use or abuse. The MSO Security Officer will coordinate all necessary investigative and follow-up actions with the OIG, law enforcement, and appropriate agency Office of Human Resources Management (HRM).

l. PIV card activator.

(1) The individual responsible for processing card activations at the Activation Station.

(2) The activator verifies that the applicant is the person to whom the credential is to be issued and guides the applicant through the activation process.

(3) If the PIV card is sent to an MSO activation point, then the PIV card activator role is performed by an MSO employee or contractor; if the PIV card is sent to a GSA activation point, then the PIV card activator role is performed by a GSA RCO.

m. Regional Credentialing Officer (RCO).

(1) Acts as PIV card activator for GSA's own PIV card activation points.

(2) Receives and disposes of old PIV cards.

(3) Provides temporary badges to qualified GSA employees and contractors. (See ch. 2-3-b for details.)

n. GSA IT security.

(1) GSA IT personnel and IT security staff are responsible for granting initial IT access to employees who have received a favorable initial suitability decision; initial IT access usually includes receiving a GSA e-mail account, a network logon account, and access to appropriate shared disk space.

(2) Upon receiving a favorable final suitability decision, GSA IT will grant the employee "full" IT access; full access includes access to all other GSA applications and data required for the employee's specific duties not already provided as part of their initial IT access.

o. Separation of roles.

(1) The roles of employee, HRO, HSPD-12 POC, CPR, and MSO are mutually exclusive. No individual shall hold more than one of these roles in the identity-proofing and registration process.

(2) MSO and PIV card activator roles may be performed by one individual or entity, as well as any other role combination that does not violate the above condition.

Figure 3-1. Summary of roles and responsibilities for GSA HSPD-12 employee process

Role	**Responsibility**	**HSPD-12 Specific Training Required**	**FIPS 201 Role**	**MSO Role**
Employee	Provide personal information & biometrics.	Card holder instructions	Applicant	Applicant
HRO	Request low risk personnel investigations & GSA credentials for new employees.	None	PIV Sponsor	None
HSPD-12 POC	Assist HROs in requesting fingerprinting & GSA credentials for new hires; make PIV card maintenance requests.	POCs must complete MSO Sponsor training	PIV Sponsor	MSO Sponsor
CPR	Request higher-level personnel investigations & adjudicate all employee investigations.	None	PIV Registrar	None
MSO	Support enrollment, PIV Card production, and activation.	None	PIV Registar, Issuer, PIV Digital Signatory	None
PMO	Coordinate overall HSPD-12 process; forward adjudication results to MSO, IT Security.	PIV training on applicable procedures/policies for HSPD-12; MSO Adjudicator training	None	MSO Adjudicator
OPM/FBI	Perform personnel investigations and other background checks.	None	None	None

PIV Card Activator	Activates the PIV card.	MSO Activator training	PIV Digital Signatory	Activator
GSA IT	Creates Windows and email account, as well as granting relevant system access depending on risk level.	None	None	None
MSO Security Officer	TBD	TBD	None	MSO Security Officer

---

2. Starting a new job at GSA (BP 1.1). Fig. 3-2 illustrates the process for credentialing a new employee at GSA.

Figure 3-2. BP 1.1 Employee: starting a new job—main process (Part 1 of 2)

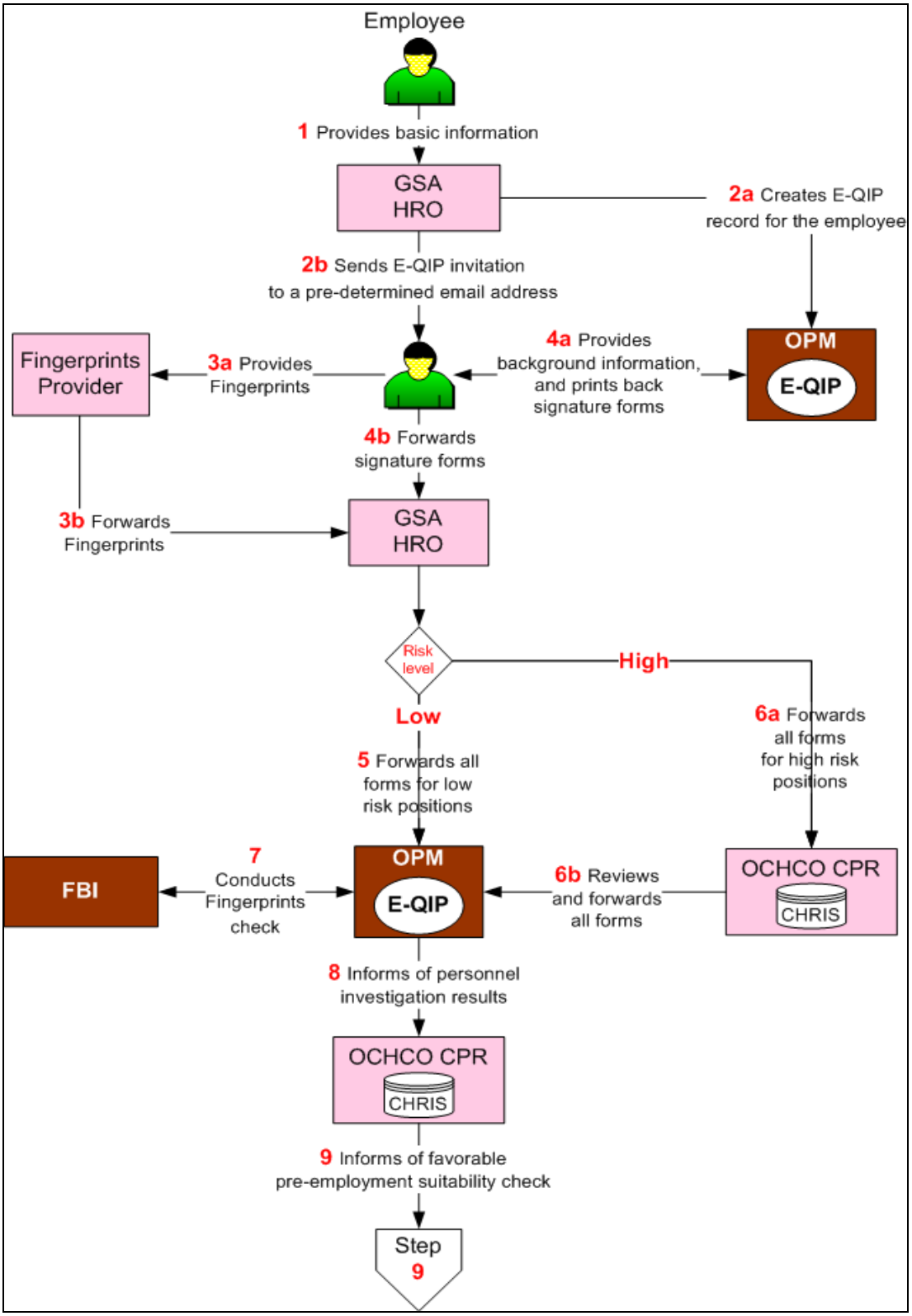
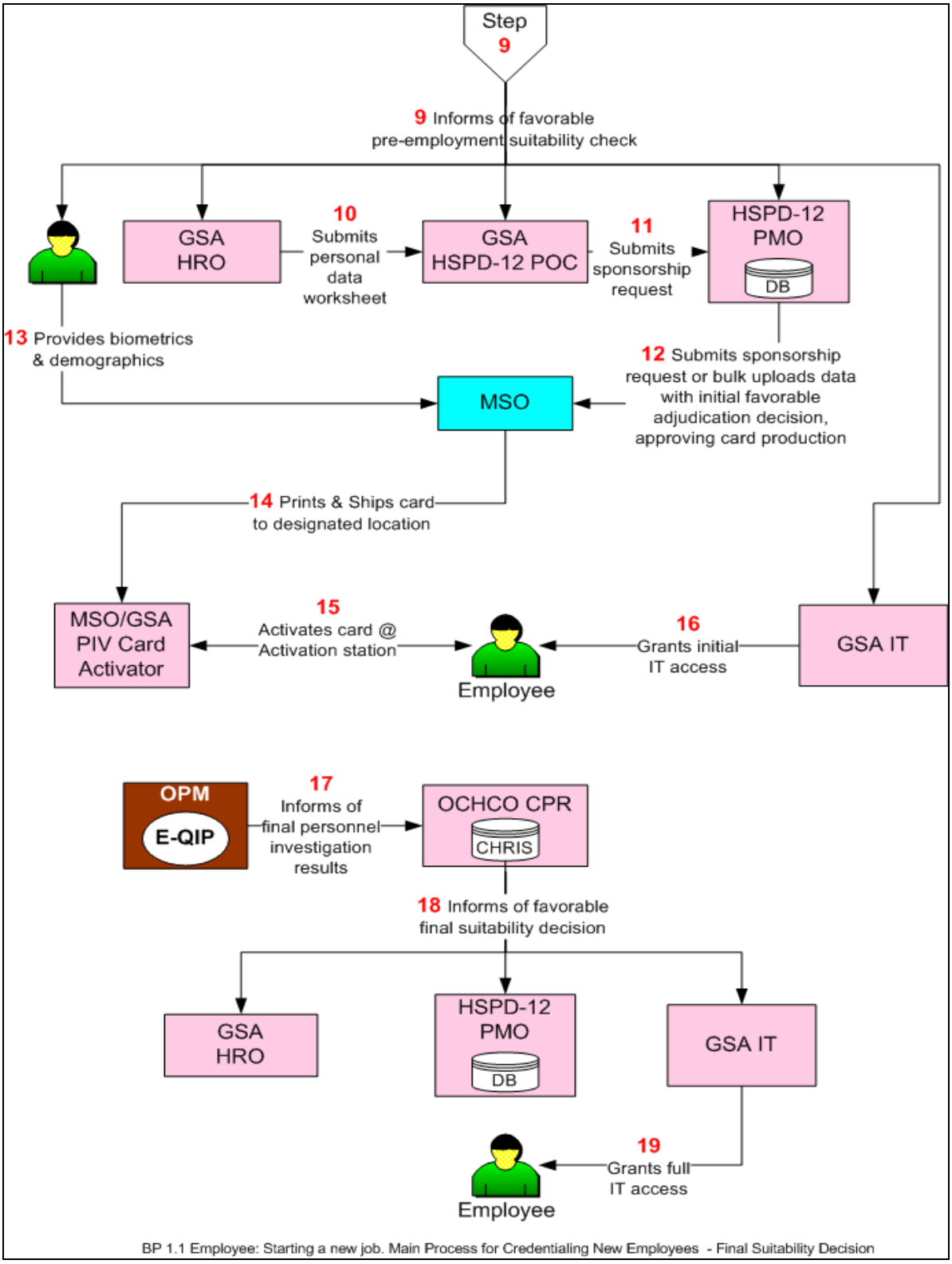


Figure 3-2. BP 1.1 Employee: starting a new job—main process (Part 2 of 2)



a. Step-by-step process for new employees.

(1) Step 1: Employee provides requested basic personal information.

(a.) Accepts job offer.

(b.) Provides basic personal information to the HRO, including name, SSN, phone number, e-mail address, and date and place of birth.

(2) Step 2a: HRO selects personnel investigation and sets up e-QIP request.

(a.) Refer to the position description for the risk level. (See ch. 2-4.)

(b.) Refer to the position description for the personnel investigation needed. (See ch. 2-4.)

(c.) Set up investigation request in OPM e-QIP system. (See Attachment B for details on setting up e-QIP request.)

(d.) Create e-QIP record for the employee requesting appropriate form. (See ch. 2-4 on which investigations and forms to use.)

(3) Step 2b: HRO sends e-QIP invitation to employee at a predetermined e-mail address.

(4) Step 3a: Employee provides biometrics to a fingerprint service provider.

(a.) Go to a local police station, FPS live-scan station, GSA HR department, or other agency fingerprinting facility to submit fingerprints.

(b.) If fingerprints are taken on paper, use SF87 Fingerprint Card.

(c.) Fingerprint service provider should verify employee's identity by their examining 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 ID.

(5) Step 3b: Fingerprint service provider forwards fingerprints to HRO.

(a.) Forward fingerprints to HRO.

(b.) If paper fingerprint cards are used, employees should not be allowed to return their own fingerprint card to the HRO. HRO should provide employee with a prepaid, preaddressed, sealable envelope that the fingerprint service provider can use to return fingerprint card by mail, overnight express mail, or interoffice mail.

(6) Step 4a: Employee provides background information to OPM's e-QIP. For complete instructions for e-QIP, see http://www.opm.gov/e-qip/.

(a.) Logon to OPM's e-QIP system as per instructions in the e-mail invite.

(b.) Fill out designated personnel investigation form (e.g. SF85, SF85P, or SF86).

(c.) Print and sign all three signature pages.

(7) Step 4b: Employee forwards all signature pages to the HRO.

(8) Step 5: HRO, for low risk, non-sensitive positions only, reviews completed forms and forwards fingerprints and signature forms to OPM.

(a.) Review the submitted forms in e-QIP for accuracy. Contact the candidate to obtain missing forms or information before submission to OPM for processing.

(b.) Tips for reviewing security forms:

i. SF85 cannot have employment or residency gaps for the last 5 years.

ii. Forms must have complete addresses on both SF85 and resume for all employment within the last 5 years.

iii. On OF-306, if applicant answers "yes" to questions, applicant must provide complete and thorough information on the form.

iv. If the applicant makes an error on the form, make sure the applicant corrects the errors in e-QIP.

v. The publication "Requesting OPM Personnel Investigations (IS-15)" at http://www.opm.gov/extra/investigate/IS-15.pdf helps ensure that the investigative forms are complete and accurate and that your requested investigation is not delayed. (See Attachment B for help in completing SF85, SF85P and SF86.)

(c.) Forward fingerprints and signature pages to OPM (for SF85 only), and make low risk personnel investigation request. Fingerprints must be submitted to OPM within 14 days of submitting personnel investigation request to OPM; otherwise, the investigation request will be rejected.

(d.) Incomplete security packages sent to OPM will be returned promptly to HROs for completion and resubmission.

(e.) If fingerprints are deemed "unclassifiable" by FBI , OPM will notify CPR, not the HRO; CPR will work with the HRO to resubmit the new employee's fingerprints.

(f.) HRO must create and maintain a copy of the security package and submit a second copy to CPR by fax or overnight express mail:

i. If by overnight express mail, send copy to:

Personnel Security Requirements Division
Attn: Security Package Enclosed
1800 F. Street, NW., Room G-230
Washington, D.C. 20405

ii. If by fax, send copy to (202) 219-0572.

(9) Step 6a: HRO, for moderate/high risk investigations, forwards fingerprints, signature pages, and other investigative forms to CPR.

(10) Step 6b: CPR, for moderate/high risk or national security positions only, reviews completed forms and forwards fingerprints, signature forms, and other forms to OPM.

(a.) Review personnel investigation information (for SF85P and SF86 only) submitted by new employee for moderate- and high-risk public-trust positions or national security positions.

(b.) Forward fingerprints, signature pages, and other necessary forms to OPM to formally request an investigation.

(11) Step 7: OPM conducts FBI fingerprint and name checks.

(a.) Send fingerprints to FBI for fingerprint check and receive results.

(b.) Start personnel investigation. (For more details on the OPM personnel investigation service, see http://www.opm.gov/e-qip/)

(c.) Request clarifications on the SF85, SF85P, or SF86 forms information. If OPM requests more information and clarifications on the submitted forms, they will notify the HRO and/or OCHCO CPR, who in turn will gather this information from the applicant.

(12) Step 8: OPM sends FBI fingerprint check results to CPR.

(a.) Inform CPR of FBI fingerprint check results.

(b.) Using employee-provided information and results of various checks, make initial suitability decision.

(13) Step 9: CPR informs GSA HSPD-12 PMO of initial suitability results. Forward initial suitability results to HRO, employee, HSPD-12 POC, GSA HSPD-12 PMO (HSPD-12Security@gsa.gov), and GSA IT security (ITSecurity@gsa.gov).

(14) Step 10: HRO requests PIV card for new employee.

(a.) If the results are favorable, fill out Personal Data Worksheet request for a new employee to get PIV card. (See Attachment A for link to GSA HSPD-12 Personal Data Worksheet.)

(b.) Send request to HSPD-12 POC.

(15) Step 11: HSPD-12 POC submits sponsorship request through GSA HSPD-12 PMO. Submit the sponsorship request to MSO through PMO using the Personal Data Worksheet (paper or electronic format).

(16) Step 12: HSPD-12 PMO requests fingerprints and PIV card from MSO.

(a.) Sponsor employee to MSO. For more than one employee, bulk upload the data, using MSO's provided tools.

i. Logon to MSO system as "Sponsor." (Use web browser to access URL https://gsa.identitymsp.com/AssuredIdentityPortal.)

ii. Enroll employee by providing requested information.

(b.) Request PIV card when enrolling.

(c.) Provide CPR's initial suitability results to MSO.

i. Logon to MSO system as "Adjudicator." (Use web browser to access URL https://gsa.identitymsp.com/AssuredIdentityPortal.) For more than one employee, bulk upload the data, using MSO's provided tools.

ii. Record initial favorable adjudication decision, thereby approving card production.

(d.) MSO sends e-mail notification to employee of enrollment time and place.

(17) Step 13: MSO and employee provide biometrics and demographics.

(a.) Employee. Go to designated MSO enrollment location at scheduled date and time.

(b.) Employee. Provide one government-issued photo ID and one other acceptable form of identification acceptable for use with Form I-9, OMB No. 1115-0136, "Employment Eligibility Verification." (See Attachment F.)

(c.) MSO. Verify employee's identity using I-9 credentials.

i. The MSO enrollment officer must meet the employee in person and verify the employee's identity source documents. The MSO enrollment officer verifies the employee's identification by evaluating the documents.

ii. Identity source documents should be inspected visually and may be verified electronically as being unaltered and authentic. If electronic means are unavailable, the MSO enrollment officer will use other means to verify the identity source documents.

iii. For each identity source document, the MSO enrollment officer must record the following information: title, issuing authority, document number, and expiration date.

iv. Personal information collected for identification purposes must be handled consistent with the Privacy Act of 1974 (5 U.S.C. 552a).

(d.) MSO. Capture employee photo, fingerprints, and additional personal data as needed.

(e.) MSO. Enrollment officer (PIV registrar) digitally signs enrollment transaction.

(18) Step 14: MSO prints and ships PIV card to MSO/GSA activation location.

(a.) Print and ship PIV card to MSO/GSA activation location.

(b.) Send notification to employee and the HRO (optional) of estimated availability of PIV card at selected location.

(19) Step 15: PIV card activator and employee activate PIV card.

(a.) Employee. Go to designated MSO/GSA activation point when PIV card is available.

(b.) PIV card activator. Verify employee's identity and provide unactivated PIV card.

(c.) Employee. Use MSO/GSA Activation Station to activate PIV card.

i. Activation Station activates PIV card and loads on-board PKI certificates.

ii. Employee sets PIN for PIV card.

(20) Step 16: GSA IT provides initial IT access. IT Security provides initial IT access to employee. (See ch. 6 for more details on initial and full IT access.)

(21) Step 17: OPM informs OCHCO CPR of final personnel investigation results.

(22) Step 18: CPR notifies other parties of final favorable adjudication results.

(a.) Based on final results of OPM investigation, CPR makes final suitability decision.

(b.) If OPM indicates the investigation has actionable issues, CPR follows up on these issues and uses OF79 to report back to OPM.

(c.) If CPR cannot make a favorable decision, it will refer the investigation to the Regional Administrator (RA) and/or Head of Services and Staff Office (HSSO).

(d.) If the decision is favorable, CPR will forward the final suitability results to the HRO and employee by e-mail.

(e.) Forward final suitability results to HRO and GSA HSPD-12 PMO (HSPD-12Security@gsa.gov).

(f.) Forward final suitability results to GSA IT Security (ITSecurity@gsa.gov).

(23) Step 19: GSA IT provides full IT access. GSA IT security provides full IT access to employee if final suitability results are favorable. (See ch. 6 for more details on initial and full IT access.) Otherwise, IT Security revokes initial access.

b. Procedures for credentialing employees with prior investigation.

(1) HSPD-12 implementation guidelines specify that Federal agencies shall not readjudicate employees with previous personnel investigations, provided the following requirements are met:

(a.) Employees have less than a 2-year break in service.

(b.) Employees have undergone the required minimum NACI or other approved personnel investigation or national security clearance investigation at the person's former agency and were adjudicated favorably.

(2) In order to process an employee with previous personnel investigation, HRO provides OCHCO CPR with form SF75, Request for Preliminary Employment Data. HRO also ensures that the applicant completes the proper security questionnaire form (SF85/SF85P/SF86, whichever is applicable). In addition, HRO notifies OCHCO CPR of the following (by e-mail, in a secure manner in accordance GSA IT security policy, or fax):

(a.) Name, SSN, date of birth, place of birth, and current agency of transfer employee

(b.) GSA Position Sensitivity Level

(c.) GSA organization/region/office symbol

(d.) Enter-on-duty date, if possible

(e.) Copy of security questionnaire (fax)

(3) Form SF75, security questionnaire, and employee information transferred in a secure manner do not need to be provided in a particular order, but all information must be provided to CPR before CPR is able to verify prior investigation.

(4) CPR will contact OPM, Defense Security Service, or other appropriate investigating agency to determine the current level of security clearance/personnel investigation.

(5) If the minimum security standard is verified, CPR will normally approve the security clearance or personnel investigation. In some cases, additional investigation or waiver of investigation may be required. If the individual does not meet security requirements, CPR will notify the HRO or requesting official, as appropriate, to request submission of security package to process the appropriate personnel investigation for the individual before enter-on-duty or beginning work.

(6) A transferring employee with a lower investigation from their previous agency than required for their GSA position may still be eligible to receive a PIV card but would need to work with the HRO to complete any additional forms to meet the position requirements.

c. Procedures for unfavorable adjudication results.

(1) Routinely, CPR does not consider a case for adjudication until OPM completes the investigation. CPR may consider a partial investigation that has serious issues. CPR adjudicates the results using the criteria in 5 CFR Part 731.202 and GSA Order ADM P 9732.1C, Appendix B, "Suitability Determination."

(2) If CPR cannot make a favorable suitability determination, the office refers the investigation to the appropriate HSSO or RA. The HSSOs or RAs may delegate to other officials the authority to review the information and to request additional investigation by GSA to resolve issues. The HSSOs or RAs may also permit these officials to make the suitability determinations under the Code of Federal Regulations (CFR) and to take disciplinary or other personnel action that may be warranted under the circumstances. The HSSO, RA, or designee makes the suitability determinations using GSA Order 9732.1C, Appendix B, "Suitability Determination," or guidance.

(3) HSSOs or RAs are responsible for ensuring due process in all cases, and their decision constitutes the suitability determination of record for GSA.

(4) Getting assistance. Officials must coordinate their determinations through their servicing human resources offices. The professionals in these offices are familiar with 5 CFR 315.804 through 806, 731, 752, and 1200, and they can answer any questions. They can provide advice in applying suitability criteria, taking appropriate administrative actions, following due process procedures, and notifying persons of their appeal rights to the Merit Systems Protection Board (MSPB). The GSA security office is also available to provide assistance.

d. Procedures for current employees holding non-MSO PIV cards.

(1) All existing employees with the minimum of a completed and adjudicated NACI on record will not require additional background checks. For all existing GSA employees with no NACI or other suitable investigation on record, a NACI at a minimum must be in process by October 27, 2008.

(2) Exact procedures, instructions, and deployment plan/schedule for credentialing current employees holding non-MSO PIV cards will be developed at a later stage, pending finalization of the HSPD-12 MSO transition plan and deployment schedule, including bulk-upload data plan.

3. Changing jobs within GSA.

a. In the event an employee changes jobs and/or locations within GSA, the HRO for the new position is responsible for reevaluating the risk level of the employee's status.

b. If the risk level of the new status is higher, then the employee needs a new personnel investigation appropriate for the higher risk. In this case, the HRO should follow the procedures for an employee joining a new job. (See par. 2.)

c. Regardless, if an employee has already received a PIV card based on a favorable initial or final suitability decision, then the employee should retain the PIV card. If the result of a new investigation is unfavorable, then the employee's PIV card can be revoked at that time.

d. A change in employment status (i.e., new job or move from region to region) with no break in service shall not be grounds for removal of access to an IT system during the adjudication process when that access is needed to accomplish assigned duties.

4. Leaving a job at GSA (BP 1.3).

a. When an employee leaves GSA, the employee's supervising manager is responsible for revoking all IT access privileges and all GSA-issued credentials, including the PIV card. If the employee is changing to another job at GSA, follow the procedures in par. 3, above.

b. The employee's supervisor must perform the following steps:

(1) Receive all of employee's GSA credentials, including the current PIV card.

(2) Inform GSA security.

(3) Inform GSA HSPD-12 PMO.

(4) Mail the PIV card to RCO for destruction.

(5) Request IT access revocation from GSA IT.

c. The RCO must take the following steps:

(1) Destroy card.

(2) Inform HSPD-12 PMO.

(3) Request card and PKI certificates revocation from MSO.

CHAPTER 4. CREDENTIALING PROCEDURES FOR CONTRACTORS

1. Roles in contractor process. Fig. 4-1 summarizes the roles involved in credentialing contractors.

a. Contractor. The contractor is an individual who is contractually employed by GSA through their own or another vendor company. However, there are other individuals who are not GSA employees and are subject to the same requirements as contractors, e.g., volunteers. These individuals will also be referred to as "contractors" in the procedures described in this section.

(1) Contractors must provide all information and biometric data needed for personnel investigations and credentialing requests.

(2) In order to receive a PIV card, contractors must present themselves at a designated MSO enrollment center at the scheduled time; at that time, the contractor must provide two identity source documents in original form. The documents must be on the list of acceptable documents included in I-9, OMB No.1115-0136, "Employment Eligibility Verification." (See Attachment F.) One of the documents must be a valid (not expired) picture ID issued by a State government or the Federal Government.

(3) After receiving a favorable initial suitability decision, contractors must present themselves at the designated MSO activation point in order to receive their PIV card and activate it; they may be required to verify their identity upon request.

(4) The contractor fulfills the FIPS 201 Applicant role.

b. PIV card requesting official. The requesting official makes all personnel investigation and credentialing requests for all contractors on contracts they are designated to support. In order to better implement privacy controls, the requesting official must be specifically designated to act in this capacity in writing by the CO for each contract and be provided training on handling PII. Often the requesting official is the COTR or Contracting Officer's Representative (COR) for the contract, but this role may be fulfilled by a project manager, PBS building manager, or local HSPD-12 POC as appropriate.

(1) The requesting official is responsible for requesting personnel investigations and identity credentials for a contractor and is responsible for reviewing all contractor-provided information that they receive.

(2) Personnel investigation requests can be made directly by the requesting official or by providing the equivalent information to an HSPD-12 POC for submission by them, depending on established regional procedures.

(3) MSO-related requests for fingerprinting and issuing a PIV card are requested by the requesting official and sent to the HSPD-12 POC for submission to the MSO.

(4) The requesting official will be notified of all adjudication results.

(5) The requesting official is responsible for requesting any additional GSA credentials, IT access rights, and/or other permissions necessary for the contractor to perform their duties.

(6) When a contractor leaves a contract for any reason, the requesting official is responsible for revoking their IT access and retrieving all GSA-issued credentials, from either the contractor or their company, and forwarding the credentials to the RCO for disposal.

(7) The requesting official fulfills the FIPS 201 PIV Sponsor role.

c. HSPD-12 POC. The HSPD-12 POCs are a designated group of specialists who are fully familiar with FIPS 201, HSPD-12, and privacy requirements and are trained by the MSO and FPS (where applicable) to use their IT request tracking systems. They may also act as requesting officials if so designated in writing by the CO for a particular contract.

(1) The HSPD-12 POC is responsible for assisting the requesting officials in making requests and monitoring the results.

(2) The HSPD-12 POC can submit all forms and documentation for a personnel investigation to FPS on behalf of a requesting official, including CIW, SF85P, signature forms, fingerprint cards, correspondence, and other documents where applicable.

(3) The HSPD-12 POC is responsible for making the PIV card sponsorship request to MSO based on a request from the requesting official.

(4) During card renewal, replacement, and re-issuance processes, the HSPD-12 POC is responsible for making card maintenance requests to MSO.

(5) The HSPD-12 POC will communicate closely with the contract requesting official, advising and assisting them on HSPD-12 procedures, choice of risk level for each position, and appropriate personnel investigation. POCs can also check the FPS FIST system and MSO credentialing request system for status information.

(6) The HSPD-12 POC fulfills the FIPS 201 PIV Sponsor role.

d. Fingerprint service provider.

(1) The fingerprint service provider can be any of the following:

(a.) FPS or GSA live-scan fingerprints station

(b.) Police station

(c.) GSA OCHO office

(d.) Any other entity entitled to provide fingerprint services

(2) The fingerprint service provider should be trained and certified to identify I-9 form credentials correctly and perform fingerprint services as regulated by government procedures.

e. FPS DHS ICE Federal Protective Service Contractor Suitability and Adjudication Division. The FPS Contractor Suitability and Adjudication Division staff have the overall responsibility for processing and monitoring personnel investigations for contractors as well as ensuring that investigative requirements are consistent with DHS Management Directives and GSA/FPS standards.

(1) FPS provides personnel investigations and adjudication for contractors under the terms and conditions of separate MOAs for PBS or non-PBS contractors.

(2) FPS reports adjudication results to the contractor, their company, the requesting official, HSPD-12 POC, HSPD-12 PMO, and GSA IT (ITsecurity@gsa.gov).

(3) FPS fulfills the FIPS 201 PIV Registrar role for GSA contractors.

f. MSO.

(1) MSO is responsible for all project, acquisition, and financial management, necessary to provide end-to-end service for the production of PIV-2 compliant credentials to GSA employees and contractors.

(2) MSO is responsible for:

(a.) Providing credentialing centers for the enrollment of contractors and activation of PIV cards.

(b.) During enrollment, taking and storing a contractor's biometrics (fingerprints and photo) after verifying the identity of the contractor.

(c.) After enrollment, sending a contractor's fingerprints to OPM and FBI for processing if needed for a personnel investigation.

(d.) Printing PIV cards, and securely shipping them to the requested activation point.

(e.) At an MSO activation point, verifying the identity of the contractor, issuing a PIV card, and supervising the activation of the PIV card by the contractor

(f.) MSO fulfills the FIPS 201 roles of the PIV Registrar, Issuer and PIV Digital Signatory; its PKI provider is the FIPS 201 PIV Authentication Certification Authority.

g. PMO.

(1) PMO is responsible for overall coordination of GSA's HSPD-12 process implementation.

(2) PMO receives the contractor adjudication results, forwards them to GSA IT security as needed, and acts as the MSO Adjudicator recording with the MSO a favorable initial suitability decision, thereby enabling the printing and activation of a contractor's PIV card.

(3) PMO has a help desk that can be reached at HSPD12PMO@gsa.gov.

(4) PMO fulfills the MSO Adjudicator role.

h. CPR.

(1) CPR is the primary GSA office responsible for direction, guidance, and interpretation of HSPD-12 personnel investigation requirements for all GSA employees and contractors.

(2) CPR publishes the instructions for processing personnel investigations and credential requests for employees and contractors. (from GSA Order ADM P 9732.1C Suitability and Personnel Security)

i. OPM. OPM performs the personnel investigations requested by FPS.

j. FBI. FBI performs the fingerprint and name checks requested by FPS.

k. MSO security officer. The MSO security officer is a GSA-designated executive responsible for the overall security of the MSO shared solution.

(1) The MSO security officer will be able to view system security reports, investigate, and resolve system security-related issues identified by the MSO shared solution system. For example, when duplicate fingerprints are detected and the scope spans more the one agency, the MSO security officer will investigate the reports and work with other GSA security officials to resolve the duplicate fingerprint issue.

(2) The MSO security officer will also be the point of contact to the OIG and will respond to requests from agencies for follow-up action on instances of unauthorized use or abuse. The MSO security officer will coordinate all necessary investigative and follow-up actions with the OIG, law enforcement, and appropriate agency HRM.

l. PIV card activator.

(1) The individual responsible for processing card activations at the Activation Station.

(2) The activator verifies that the applicant is the person to whom the credential is to be issued and guides the applicant through the activation process.

(3) A MSO activation point is an activation station located at an MSO enrollment center and operated by an MSO registrar. A GSA activation point is an activation station operated by a non-MSO GSA employee. At this point, GSA only has MSO activation points but may have GSA activation points in the future. If the PIV card is sent to an MSO activation point, then the PIV card activator role is performed by an MSO employee or contractor; if the PIV card is sent to a GSA activation point, then the PIV card activator role is performed by a GSA RCO.

m. Regional Credentialing Officer (RCO).

(1) Act as PIV card activator for GSA's own PIV card activation points.

(2) Receive and dispose of old PIV cards.

(3) Provide temporary badges to qualified GSA employees and contractors. (See ch. 2-3(b) for details.)

n. GSA IT security

(1) GSA IT personnel and IT security staff are responsible for granting initial IT access to contractors who have been granted access by the authorizing official or have received a favorable initial suitability decision; initial IT access usually includes receiving a GSA e-mail account, a network logon account, and access to appropriate shared disk space.

(2) Upon having been granted access by the authorizing official or receiving a favorable final suitability decision, GSA IT will grant the contractor full IT access; full access includes access to all other GSA applications and data required for the contractor's specific duties not already provided as part of their initial IT access.

o. Separation of roles.

(1) The roles of contractor, requesting official, FPS, and MSO are mutually exclusive. No individual shall hold more than one of these roles in the identity proofing and registration process.

(2) HSPD-12 POCs can act as the requesting official for any contract for which they have been designated in writing by the CO.

(3) MSO and PIV card activator roles may be assumed by one individual or entity, as well as any other roles combination that does not violate the above clause.

Figure 4-1. Summary of roles and responsibilities for GSA HSPD-12 contractor process

Role	**Responsibility**	**Training Plan**	**FIPS 201 Role**	**MSO Role**
Contractor	Provide information & biometrics	None	Applicant	Applicant
Requesting Official	Request personnel investigations & GSA credentials	Requesting officials must have training on handling date PII data.	PIV Sponsor	None
HSPD-12 POC	Assist Requesting Officials by forwarding and/or monitoring personnel investigation and MSO requests.	POCs must complete MSO Sponsor training, FPS FIST training, and be fully familiar with the FIPS 201 and HSPD-12 requirements.	None	MSO Sponsor
Fingerprint Service Provider	Record fingerprints to be used in personnel investigations	None	None	None
FPS	Request personnel investigations from OPM & make suitability decisions for GSA contractors	None	PIV Registrar	None
MSO	Provide enrollment, PIV Card production, and activation	None	PIV Registar, Issuer, PIV Digital Signatory	None
PMO	Coordinate overall HSPD-12 process; forward adjudication results to MSO, IT Security.	MSO Adjudicator training	None	MSO Adjudicator
OPM/FBI	Perform personnel investigations and other background checks.	None	None	None
PIV Card Activator	Activates PIV card.	MSO Activator training	PIV Digital Signatory	MSO Activator
GSA IT	Creates Windows and email account, grants relevant system access depending on risk level.	None	None	None

MSO Security Officer	Handles MSO-related security problems.	MSO Security Officer training	None	MSO Security Officer
CPR	Overall responsibility for personnel security requirements at GSA	None	None	None

---

2. Joining a new GSA contract (BP 2.1). Fig. 4-2 illustrates the process for credentialing a contractor at GSA.

Figure 4-2. BP 2.1 Contractor: Joining a new contract—main process (part 1 of 2)

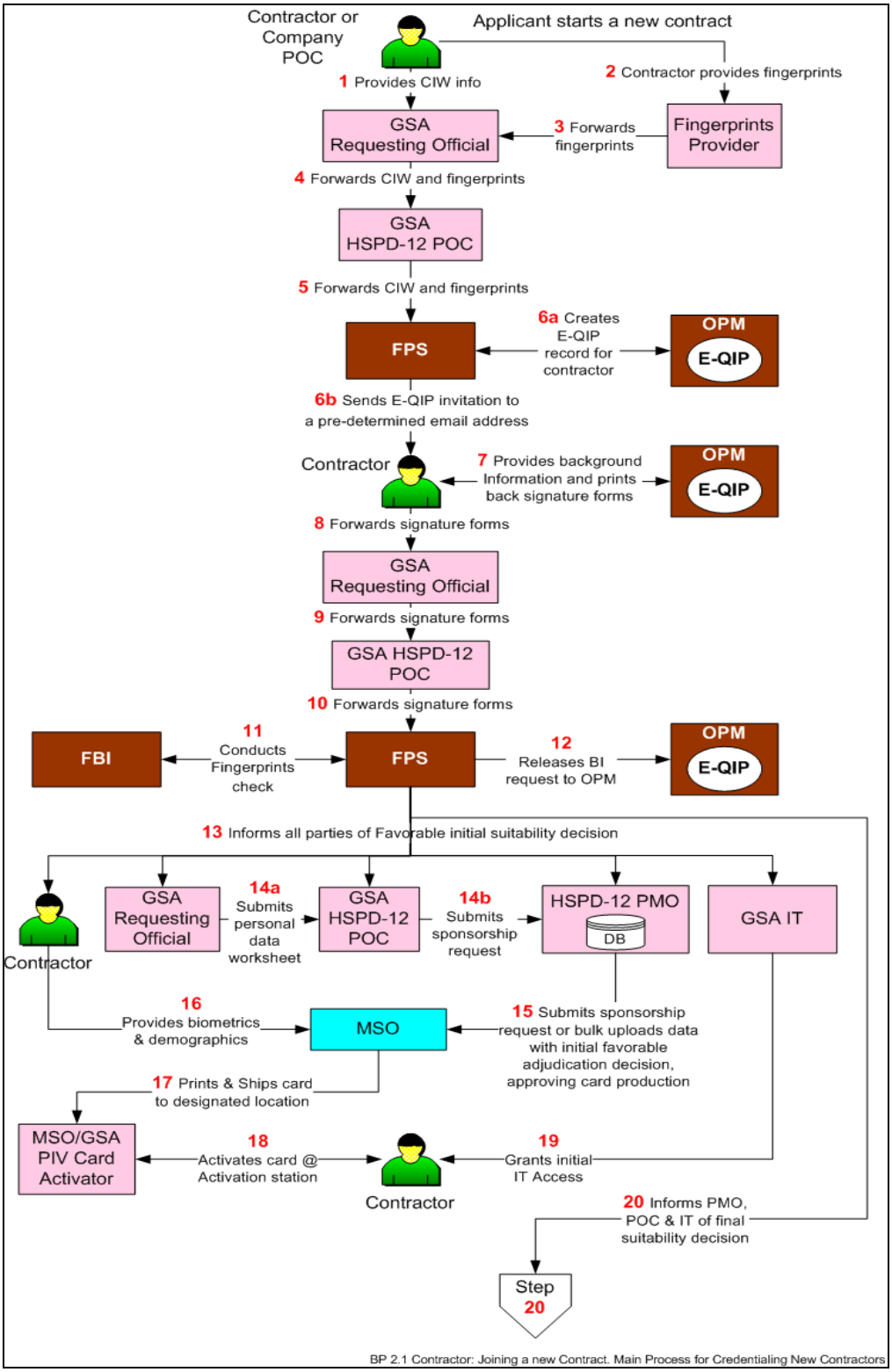
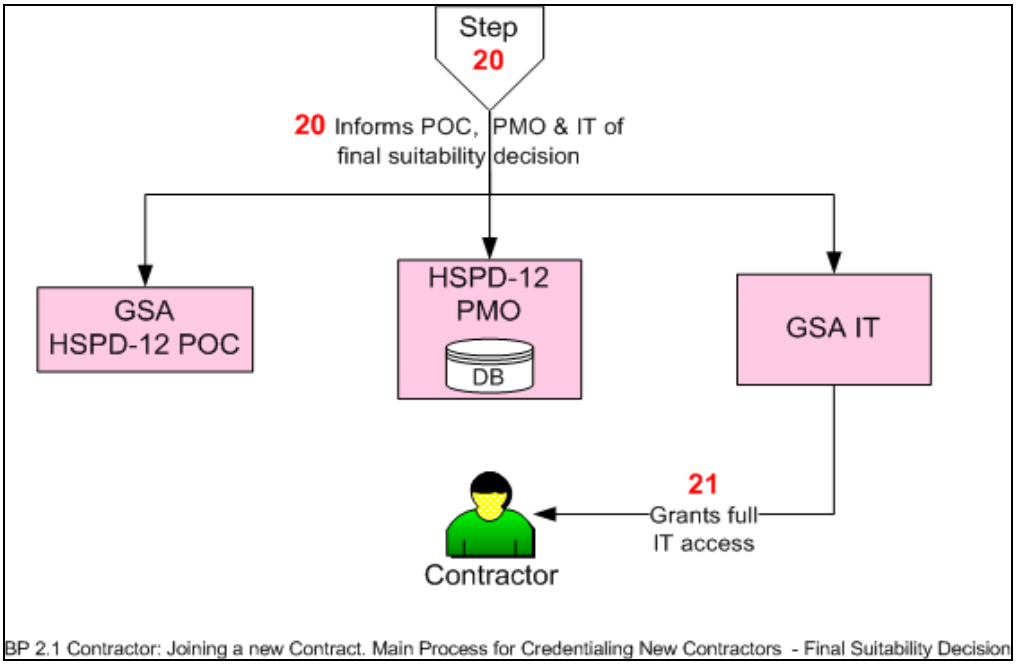


Figure 4.2. BP 2.1 Contractor: Joining a new contract—main process (part 2 of 2)



a. Step-by-step process for new contractors.

(1) General note: incomplete Contractor Information Worksheet and/or other forms: If FPS finds that the Contractor Information Worksheet (CIW) and/or other forms are not correct, FPS e-mails the contractor, contractor company, POC and requesting official to request them to correct the information. Either the requesting official or POC may forward the corrected CIW and/or information to FPS. FPS cannot begin their suitability determination process until the personnel investigation forms are satisfactorily completed and all signature pages are received by FPS.

(2) Step 1: Contractor provides CIW information.

(a.) When contractors are assigned to a new contract, they provide CIW information. In certain cases, the contractor's company PM/POC might provide all or part of this information.

(b.) Contractors without an e-mail address of their own should use their contractor company's e-mail address.

(3) Step 2: Contractor provides biometrics to a fingerprint service provider.

(a.) Go to a local police station, FPS, or GSA live-scan station, GSA HR department, or other agency fingerprinting facility to submit fingerprints.

(b.) If fingerprints are taken on paper, use FD258 Fingerprint Card.

(c.) Fingerprint service provider should verify contractor's identity by examining 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 ID.

(4) Step 3: Fingerprint service provider forwards fingerprints to requesting official.

(a.) Forward fingerprints to requesting official.

(b.) If paper fingerprint cards are used, contractors should not be allowed to return their own fingerprint card to the requesting official. Requesting official should provide contractor with a prepaid, preaddressed, sealable envelope that the fingerprint service provider can use to return fingerprint card by mail, overnight express mail, or interoffice mail.

(5) Step 4: Requesting official fills out and forwards CIW and fingerprints.

(a.) Requesting official must perform the following steps before filling out the CIW:

i. Assess job risk level. (See ch. 2-4.)

ii. Select the type of personnel investigation needed. (See ch. 2-4-d.)

iii. Select the types of GSA credentials needed. (See ch. 2-3.)

iv. Decide whether IT access is needed. (See ch. 6.) Note that contractors needing routine access to GSA-occupied space for more than 6 months or contractors needing access to GSA IT systems need to have a PIV card.

(b.) Fill out CIW. (See Attachment A for link to the form.)

(c.) If e-QIP is not used for personnel investigation, the personnel investigation forms described in step 7 should be submitted with the CIW.

(d.) Forward CIW and fingerprints (and personnel investigation forms if e-QIP is not used) to HSPD-12 POC.

(6) Step 5: HSPD-12 POC reviews submitted forms and forwards to FPS.

(a.) HSPD-12 POC reviews the CIW and, if needed, provides guidance to requesting official.

(b.) Upon review of all documents, POC forwards the whole package securely by e-mail, fax, or overnight express mail in a sealed envelope to the appropriate FPS office as follows:

i. For non-PBS contractor, requests go to FPS HQ. (See Attachment G for addresses.)

ii. For PBS contractor requests go to regional FPS offices. (See Attachment G for addresses.)

iii. For full FPS instructions, see the HSPD-12 Implementation site on the GSA InSite. (See GSA InSite > Information Technology > HSPD-12 Implementation > Policy and Guidance Resources.)

(7) Step 6A: FPS sets up new suitability decision request.

(a.) Receive new CIW and set up new request in their IT systems.

(b.) Open new personnel investigation request with OPM in e-QIP system.

(8) Step 6B: FPS sends e-QIP invite (if used).

(a.) Send e-QIP invitation to contractor.

(b.) Send notifications to HSPD-12 POC, requesting official, contractor, and contractor company

(9) Step 7: Contractor fills out personnel investigation forms.

(a.) Note: If e-QIP is not used, the personnel investigation forms should be submitted at step 4 with the CIW.

(b.) Fill out personnel investigation forms. For complete instructions for e-QIP, see http://www.opm.gov/e-qip/.

i. Logon to OPM's e-QIP system as per instructions in e-mail invite.

ii. Fill out personnel investigation form (usually SF85P or SF86).

iii. Print and sign all three signature pages.

(10) Step 8: Contractor forwards signature forms. Forward signature pages to requesting official.

(11) Step 9: Requesting official forwards signature forms. Forward signature pages to HSPD-12 POC.

(12) Step 10: HSPD-12 POC forwards signature forms to FPS. Forward signature pages to FPS.

(13) Step 11: FPS conducts FBI fingerprint and other suitability checks. See paragraph c for procedures for contractors with a prior investigation. See paragraph e for procedures for unfavorable adjudication results. For more details on the FPS personnel investigation service, see the HSPD-12 Implementation site on the GSA InSite: GSA InSite > Information Technology > HSPD-12 Implementation > Policy and Guidance Resources.

(a.) Send fingerprints to FBI for fingerprint check and receive results.

(b.) Conduct other checks on contractor's background.

(c.) Using contractor-provided information and results of various checks, make initial suitability decision.

(14) Step 12: FPS releases personnel investigation request to OPM. Submit personnel investigation request to OPM.

(15) Step 13: FPS informs all parties of initial suitability results.

(a.) Forward initial suitability decision results to requesting official, HSPD-12 POC, contractor, and contractor company.

(b.) Forward initial suitability results to GSA HSPD-12 PMO (HSPD-12Security@gsa.gov).

(c.) Forward initial suitability results to GSA IT security (ITSecurity@gsa.gov).

(16) Step 14A: Requesting official submits GSA HSPD-12 Personal Data Worksheet to POC. Submit Personal Data Worksheet to the HSPD-12 POC with all relevant information to be used for the MSO enrollment. (See Attachment A for link to the form.)

(17) Step 14B: HSPD-12 POC submits sponsorship request to GSA HSPD-12 PMO. Submit sponsorship request to PMO using the Personal Data Worksheet (paper or electronic format).

(18) Step 15: HSPD-12 PMO requests PIV card from MSO.

(a.) Enroll contractor at MSO.

i. Logon to MSO system as "Sponsor." (Use web browser to access URL https://gsa.identitymsp.com/AssuredIdentityPortal)

ii. Enroll contractor by providing requested information. For more than one contractor, bulk upload the data, using MSO's provided tools.

(b.) Request PIV card when doing enrollment.

(c.) Provide FPS initial suitability results to MSO.

i. Log onto MSO system as "Adjudicator." (Use web browser to access URL https://gsa.identitymsp.com/AssuredIdentityPortal.) For more than one contractor bulk upload the data, using MSO's provided tools.

ii. Record initial favorable adjudication decision, thereby approving card production.

(d.) Choose enrollment location. MSO sends e-mail notification to contractor of enrollment request.

(19) Step 16: MSO and contractor provide biometrics and demographics.

(a.) Contractor. Logon to the MSO scheduling Web site and select appointment location, date and time. (Use web browser to access URL https://www.schedulemsp.com/tc/login.do?url=10001)

(b.) Contractor. Go to designated MSO enrollment center at scheduled date and time.

(c.) Contractor. Provide one government issued photo ID and one other acceptable form of identification acceptable for use with Form I-9, OMB No. 1115-0136, "Employment Eligibility Verification." (See Attachment F.)

(d.) MSO. Verify contractor's identity using I-9 credentials.

i. The MSO enrollment officer must meet the contractor in person and verify the contractor's identity source documents. The MSO enrollment officer verifies the contractor's identification by evaluating the documents.

ii. Identity source documents should be inspected visually and may be verified electronically as being unaltered and authentic. If electronic means are unavailable, the MSO enrollment officer will use other means to verify the identity source documents.

iii. For each identity source document, the MSO enrollment officer must record the following information: title, issuing authority, document number, expiration date.

iv. Personal information collected for identification purposes must be handled consistent with the Privacy Act of 1974 (5 U.S.C. 552a).

(e.) MSO. Capture contractor photo, fingerprints, and additional personal data as needed.

(f.) MSO enrollment officer (PIV Registrar) digitally signs enrollment transaction.

(20) Step 17: MSO prints and ships PIV card to MSO/GSA activation location.

(a.) Print and ship PIV card to MSO activation location.

(b.) Send notification to contractor and HSPD-12 POC of estimated availability of PIV card at designated location.

(21) Step 18: PIV card activator and contractor activate PIV card.

(a.) Contractor. Go to designated MSO or GSA activation point when notified that PIV card is available.

(b.) PIV card activator. Verify contractor's identity and provide unactivated PIV card.

(c.) Contractor. Use PIV card Activation Station to activate PIV card. Activation Station activates PIV card and loads on-board PKI certificates. Contractor sets PIN for PIV card.

(22) Step 19: GSA IT grants initial IT access. GSA IT security provides initial IT access to contractor, if needed. (See ch. 6.)

(23) Step 20: FPS makes final suitability decision.

(a.) Receive OPM investigation results and make final suitability decision.

(b.) Inform requesting official, HSPD-12 POC, contractor, and contractor company of final suitability results.

(c.) Inform HSPD-12 PMO (HSPD-12Security@gsa.gov) and GSA IT security (ITSecurity@gsa.gov) of results.

(24) Step 21: GSA IT grants full IT access. Provide full IT access to contractor if final suitability results are favorable and if IT access is needed. (See ch. 6.)

b. Procedures for national security clearances for contractors.

(1) The personnel investigation procedures for Federal contractors for National Security Information (NSI) level are different than for Federal employees. Contractor clearances are processed by DISCO.

(2) Contractors who need a Confidential, Secret, or Top Secret clearance will need to obtain their clearances from their employing contract company. The company will have an internal security officer who deals directly with DISCO to obtain the correct personnel investigation forms and clearance request.

(3) Once DISCO has completed the NSI personnel investigation case, the contract company will provide a Visit Authorization Request (VAR) letter that informs the Federal agency what kind of personnel investigation was completed, the date of completion, the level of clearance, and the duration of the clearance.

(4) Federal agencies do not process the personnel investigations for contractors at the Confidential, Secret or Top Secret levels.

c. Procedures for contractors with prior investigation.

(1) HSPD-12 implementing guidelines specify that Federal agencies shall not readjudicate contractors with previous personnel investigations, provided the following requirements are met:

(a.) FPS can verify with OPM and/or the agency that performed the adjudication the following conditions:.

i. The prior investigation was completed.

ii. The investigation results were favorable.

iii. The granting agency has not received any significant derogatory information that was not previously adjudicated.

(b.) The contractor has had less than a 2-year break in service since the end of the previous contract.

(c.) The prior investigation is at the same or higher level as the personnel investigation that would be requested for the new contract.

(2) In order to process a contractor with previous personnel investigation, the requesting official shall provide FPS with a completed SF85P and CIW, indicating in Section 1 of the form that there was a prior investigation and the date of the investigation, and indicating in Section 6 (Comments/Notes) the name of the agency that performed the adjudication.

(3) FPS will notify the adjudicating agency and request verification of the successful adjudication.

(4) If the previous agency adjudication information is not available or cannot be verified, the applicant should submit the personnel investigation forms to FPS who will forward them to OPM. OPM disseminates case files or information from previous investigations upon receipt of the completed personnel investigation questionnaire form (i.e., SF85P). The applicant's signature of consent will allow OPM to release the investigation file to the requesting agency.

d. Procedures for contractors on multiple GSA contracts.

(1) In certain cases, a contractor may be staffed onto more than one GSA contract. When a contractor joins a new contract, the COTR for the new contract is responsible for evaluating the risk level of the contractor’s new work and verifying with CPR and the COTR for the old contract that the risk level and credentials for the old work are sufficient for the new work.

(2) If the risk level of the new work is higher, then the contractor needs a new personnel investigation appropriate for the higher risk. The COTR for the new contract should follow the procedures for a contractor joining a new contract described in ch. 4-2.

(3) If the risk level of the new work is the same or lower than the old one, the contractor does not have to be readjudicated.

(4) However, if any information on the face of the PIV card has changed, especially the expiration date of the card or the organizational affiliation, then the new COTR needs to request a new PIV card and return the old PIV card to the old COTR for deactivation. The new COTR should follow the procedures described in ch. 5-3 for PIV card replacement.

(5) Likewise, the new COTR is responsible for evaluating the employee's current access to GSA IT systems. The new COTR should inform IT security of adjustments to the employee's IT access in accordance with their new job responsibilities.

e. Procedures for unfavorable adjudication results.

(1) FPS Contractor Suitability (CS) Adjudication staff will contact the contractor directly to address any suitability issues that have developed in the preliminary review and checks. Written notification will be mailed out using certified mail or express mail with return receipt.

(2) If the contractor fails to submit security documents or respond completely to inquiries made by the FPS CS Adjudication staff within 15 calendar days, the applicant will no longer be considered for an "Enter-On-Duty" determination and the GSA requesting official, contractor, and contracting company will be notified of this decision in writing.

(3) Contractor employment suitability determinations are made in accordance with OPM's guidance in "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12" issued on July 31, 2008.

(4) In cases where the initial result for a contractor employment suitability determination is unfavorable, DHS/FPS will afford the contractor an opportunity to address the issues raised by the investigation. DHS/FPS will notify the GSA requesting official of the initial unfavorable determination in order for the requesting official to take appropriate action to protect GSA employees, property, and interests.

(5) DHS/FPS will provide a written proposal notification to the contractor providing the specific reasons for proposing to deny the contractor's participation in the contract due to the unfavorable suitability determination. DHS/FPS will allow the contractor 30 days to respond in writing to the proposal. After 30 days, or after receiving the contractor's response, DHS/FPS will make the final determination and respond in writing to the requesting official and the contractor on the final determination.

(6) In the case of a final unfavorable determination, DHS/FPS notifies the requesting official who is responsible for ensuring that the contractor company removes the contractor from the GSA contract and for revoking all GSA credentials and access to GSA IT systems and facilities.

(7) For further information, see FPS implementation plans for PBS and non-PBS contractors. (For PBS: FPS Contractor Suitability & Adjudication Program, Security & Law Enforcement Division, HSPD-12 Implementation, July 31, 2006. For non-PBS: FPS Implementation Plan for GSA Non-PBS Contractors, Contractor Suitability & Adjudication Program, Security & Law Enforcement Division, HSPD-12 Implementation, February 20, 2007.)

f. Procedures for current contractors holding non-MSO PIV cards.

(1) Existing contractors with a completed and adjudicated NACI (minimum) on record will not require additional background checks. For all existing GSA contractors with no NACI or other suitable investigation on record, a NACI (minimum) will be in process by October 27, 2008.

(2) Exact procedures, instructions, and deployment plan/schedule for credentialing current contractors holding non-MSO PIV cards will be developed at a later stage, pending finalization of the HSPD-12 MSO Transition Plan and Deployment Schedule, including bulk-upload data plan.

3. Changing GSA contracts.

a. In case the contractor changes contracts, status, and/or locations within GSA for any reason, or any other event of similar type causes a change to the information on the face of the card, the contract's requesting official is responsible for reevaluating the risk level of the contractor's position.

b. If the risk level of the new position is higher, then the contractor needs a new personnel investigation appropriate for the higher risk. In this case, the requesting official should follow the procedures for a contractor joining a new job/contract as described in par. 2.

c. However, if the contractor's new position and/or responsibilities do not affect their risk level or the information on the face of the card, there is no need to replace the card with a new one.

d. Likewise, if the risk level of the new position is the same or lower than the old one, the contractor does not have to be reinvestigated.

e. If the contractor has been issued a PIV card, having received a favorable initial or final suitability decision, they can retain that PIV card whether or not they need an additional investigation. If the result of any subsequent investigation is unfavorable, the contractor's PIV card will be revoked at that time.

f. If a contractor is changing contracts and/or contract company without any break in service, the contractor can retain their PIV card since it does not hold any company specific information. If the contractor is changing to a new contractor company, the new contractor company must assume the prior contract company's responsibility for returning the contractor's PIV card to GSA upon completion of GSA contracted services.

4. Leaving a GSA contract.

a. When a contractor leaves a GSA contract to work elsewhere, the requesting official is responsible for revoking all IT access privileges and all GSA-issued credentials including the

PIV card. If the contractor is joining another contract at GSA, follow the procedures in par. 3, above.

b. The requesting official must perform the following steps:

(1) Receive all of the contractor's GSA credentials including their current PIV card.

(2) Inform GSA security.

(3) Inform GSA HSPD-12 PMO.

(4) Mail the PIV card to RCO for destruction.

(5) Request IT access revocation from IT.

c. The RCO must take the following steps:

(1) Destroy the card.

(2) Inform HSPD-12 PMO.

(3) Request card and PKI certificates deactivation from MSO.

5. Help for HSPD-12 related questions.

a. The primary person to contact for questions about the HSPD-12 process, specific personnel investigation requests, or credentialing requests is the local HSPD-12 POC. (See par. 1c.) HSPD-12 POCs are trained on the concepts and details of the HSPD-12 process.

b. For questions that the POCs are unable or unavailable to answer, the next point of contact is the GSA HSPD-12 PMO. They will either answer the questions directly or refer the question to other staff at CPR who can answer the questions.

c. For questions regarding accessing and using MSO hardware and software, contact the USAccess (MSO) Help Desk.

d. Here are the current contact points for HSPD-12 related questions:

(1) HSPD-12 POCs. See list on GSA InSite Web site at http://insite.gsa.gov/ Information Technology tab, under HSPD-12 Implementation.

(2) HSPD-12 PMO. Email: HSPD12PMO@gsa.gov

(3) USAccess (MSO) Help Desk. Phone: 1-866-493-8391

CHAPTER 5. PIV CARD MAINTENANCE AND RENEWAL

1. Types of situations in which a PIV card may be reissued.

a. There are three types of situations in which a PIV card may be reissued:

(1) PIV card renewal. The current PIV card is expiring and a new card needs to be issued.

(2) PIV card replacement. The current PIV card is available, but a new card needs to be issued because the current one is damaged, unreadable, broken, or unusable or the information on the front or stored on the card has changed.

(3) PIV card re-issuance: The current PIV card is not available because it has been lost, stolen, or destroyed, and a new card needs to be issued.

b. The event triggering a card renewal is quite explicit—the arrival of the card's expiration date. On the other hand, the exact reasons for a card replacement as opposed to a card re-issuance can vary, and the important criterion to consider is whether the current card is available or not. Use the card replacement procedure described in par. 2, below, when the current card is available to be turned in. If the current card is not available because it was lost, destroyed, etc., follow the procedures in par. 3 for card re-issuance. But in this case, there is a risk that the card could be misused unless it is subsequently found or recovered.

c. Procedures for each situation are described in the following paragraphs. Additionally, Par. 5 covers the procedures for resetting the PIN on a PIV card.

2. PIV card renewal.

a. If an employee/contractor's PIV card has expired or is within six weeks of expiration, the original PIV card must be replaced by having a new PIV card issued and the original PIV card deactivated. Reinvestigation is not required, per OMB Guidance M-05-24. (OMB memoranda can be found the OMB website www.OMB.gov or directly through: http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf.)

b. If the expiring PIV card was not issued by the MSO, then the biometrics (i.e., fingerprints and photo) of the employee/contractor are not on file with the MSO, and the employee/contractor will have to be enrolled with the MSO before a replacement card can be issued. This is done by following the procedures for sponsoring a new employee or contractor at the MSO in order to request fingerprinting and a new PIV card. (See ch. 3-2. or ch. 4-2.)

c. Two main principles should be followed when renewing a card:

(1) Employee/contractor should not be left without a card during the process.

(2) Employee/contractor should not be in possession of more than one card during the process.

d. Card renewal process. Fig. 5-2 illustrates the card renewal-card expiration process.

(1) Step 1a/b: Employee/contractor notifies supervisor/requesting official.

(a.) Inform employee's supervisor or contractor's requesting official within 60 days of the expiration date of the PIV card and request a renewal using the PIV card request form.

i. If the current PIV card has expired, return the current PIV card to the employee's supervisor or contractor's requesting official, and request a temporary badge.

ii. If the current PIV card has not expired, it can continue to be used until its expiration but then must be returned to the supervisor/requesting official.

(b.) Contractors should also inform their contractor company manager.

(2) Step 2a/b: Supervisor/requesting official sends renewal request to HSPD-12 POC. The supervisor/requesting official should sign the request form and forward it to the HSPD-12 POC.

(3) Step 3: HSPD-12 POC requests new PIV card.

(a.) Verify the individual's personal information so that if there is any change that affects the information on the face of the card or stored on the card, the appropriate changes can be made.

(b.) Request a renewed PIV card to be issued by MSO. If the original PIV card was not issued by MSO, follow the procedures for arranging for the employee or contractor to provide biometrics and personal information data. (See ch. 3-2 or ch. 4-2.)

(4) Step 4: MSO prints and ships the PIV card to MSO/GSA activation point.

(a.) If record of employee/contractor is valid in the database, print and ship the card to the MSO/GSA Activation Station location selected by the HSPD-12 POC.

(b.) Revoke old PIV card and all card-specific digital PKI certificates (e.g., revoke the card authentication certificate but not the individual's signing and encryption certificates).

(5) Step 5: Employee/contractor and PIV card activator return old card and activate new card.

(a.) Employee/contractor. Appear at MSO/GSA activation point with old PIV card.

(b.) PIV card activator. Verify employee/contractor's identity, receive old PIV card, and issue new, unactivated PIV card. PIV card activator should not release new PIV card without receiving old PIV card first.

(c.) Employee/contractor. Activate new PIV card and load with PKI digital certificates, etc.

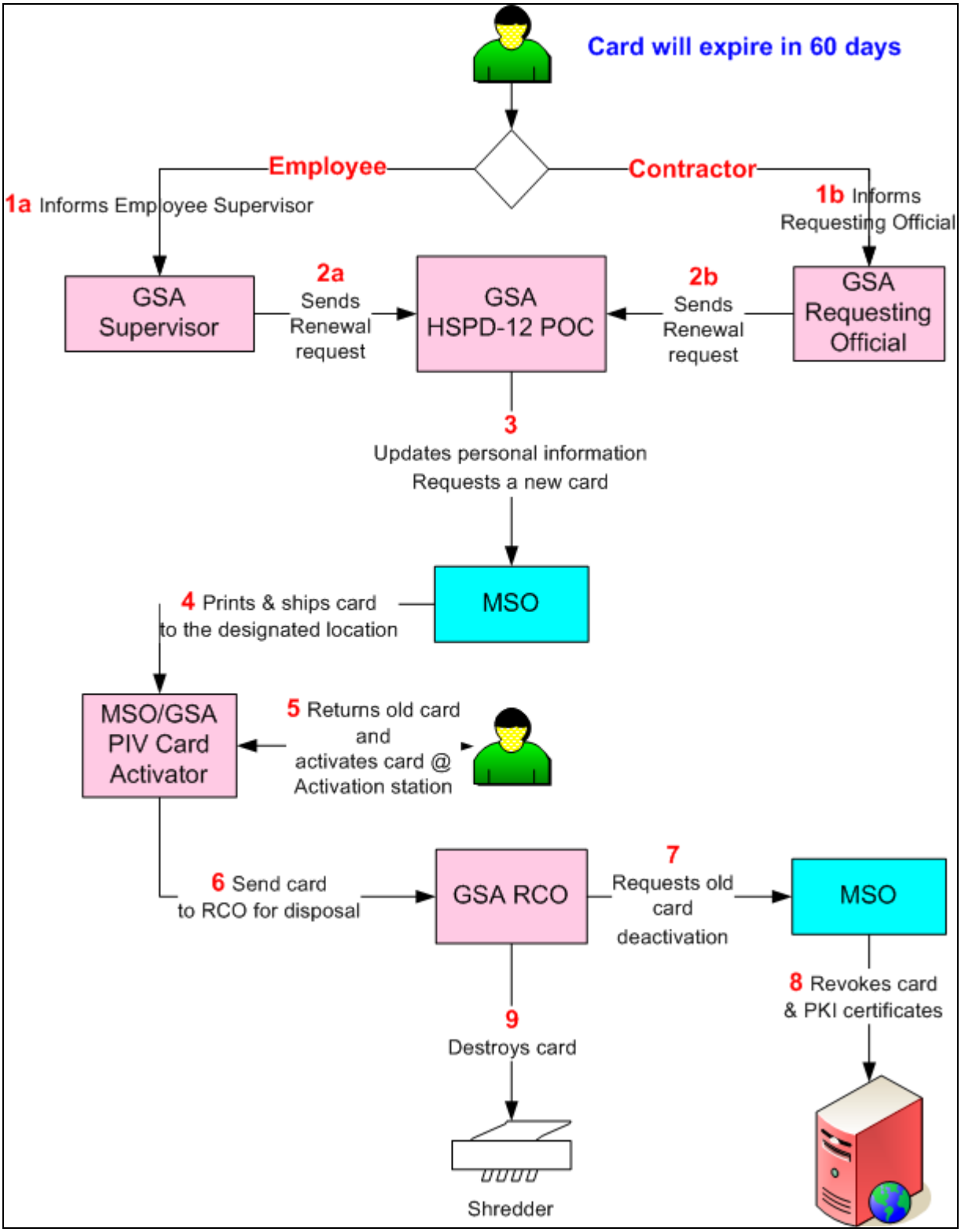
(6) Step 6: PIV card activator sends PIV card to Regional Credential Officer for disposal. If the PIV card activator is not a RCO, then send PIV card to RCO for disposal.

(7) Step 7: RCO requests old card deactivation by MSO.

(8) Step 8: MSO revokes old card and PKI certificates.

(9) Step 9: RCO destroys PIV card.

Figure 5-2. PIV card renewal process (BP 3.1 Card renewal-card expiration)



3. <u>PIV card replacement.</u>

a. If an employee/contractor's PIV card is physically available but unusable because it has been damaged, broken, unreadable, etc., or if the information on the face of the PIV card has changed, then the original PIV card must be replaced by having a new PIV card issued and the original PIV card deactivated.

b. If the original PIV card was not issued by the MSO, then the biometrics (i.e., fingerprints and photo) of the employee/contractor are not on file with the MSO, and the employee/contractor will have to be enrolled with the MSO before a replacement card can be issued. This is done by following the procedures for sponsoring a new employee or contractor at the MSO in order to request fingerprinting and a new PIV card. (See ch. 3-2 and ch. 4-2.) However, no new background check or adjudication is required.

c. Two main principles should be followed when replacing a card:

(1) Employee/contractor should not be left without a card during the process.

(2) Employee/contractor should not be in possession of more than one card during the process.

d. In order to obtain a replacement PIV card, follow the steps and procedures for card renewal described in par. 2.

4. PIV card re-issuance.

a. If an employee/contractor's PIV card is physically unavailable because it has been lost, destroyed, or stolen, a new PIV card must be issued.

b. In this case, it is important that the original PIV card is deactivated and all credentials revoked as soon as notification is received.

c. If the original PIV card was not issued by the MSO, then the biometrics (i.e., fingerprints and photo) of the employee or contractor are not on file with the MSO, and the employee/contractor will have to be enrolled with the MSO before a replacement card can be issued. This is done by following the procedures for sponsoring a new employee or contractor at the MSO in order to request fingerprinting and a new PIV card. (See ch.3-2 for employees and ch. 4-2 for contractors.) However, no new background check or adjudication is required.

d. Card re-issuance process. Fig. 5-4 illustrates the card re-issuance process.

(1) Step 1: Employee/contractor notifies HSPD-12 POC immediately of lost/stolen card.

(a.) Notify HSPD-12 POC that the PIV card has been lost, stolen, etc.

(b.) Inform employee's supervisor or contractor's requesting official, and request a new card using PIV Card Request form.

(c.) Contractors should inform their contractor company manager.

(2) Step 2: HSPD-12 POC notifies others of lost PIV card. Notify HSPD-12 PMO, MSO, GSA security, and GSA IT security that the PIV card has been lost.

(3) Step 3: MSO revokes lost PIV card. Revoke PIV card and all card-specific digital PKI certificates (e.g., revoke the card authentication certificate but not the individual's signing and encryption certificates).

(4) Step 4: Employee/contractor notifies HSPD-12 supervisor/requesting official of lost/stolen card.

(a.) Inform employee's supervisor or contractor's requesting official, and request a new card using PIV Card Request form.

(5) Step 5: Supervisor/requesting official sends renewal request to HSPD-12 POC. The supervisor/requesting official should sign the request form and forward it to the HSPD-12 POC.

(6) Step 6: HSPD-12 POC requests a new PIV card.

(a.) Verify the individual's personal information, so that if there is any change that affects the information on the face of the card or stored on the PIV card, the appropriate changes can be made.

(b.) Request a new PIV card to be issued by MSO. If the original PIV card was not issued by MSO, follow the procedures for arranging for the employee or contractor to provide their biometrics and personal information data. (See ch. 3-2. or ch. 4-2.)

(7) Step 7: MSO prints and ship PIV card to MSO/GSA activation point.

(a.) If record of employee/contractor is valid in the database, print and ship the card to the MSO/GSA Activation Station location selected by the HSPD-12 POC.

(b.) If not already done, revoke old PIV card and all card-specific digital PKI certificates (e.g., revoke the card authentication certificate but not the individual's signing and encryption certificates).

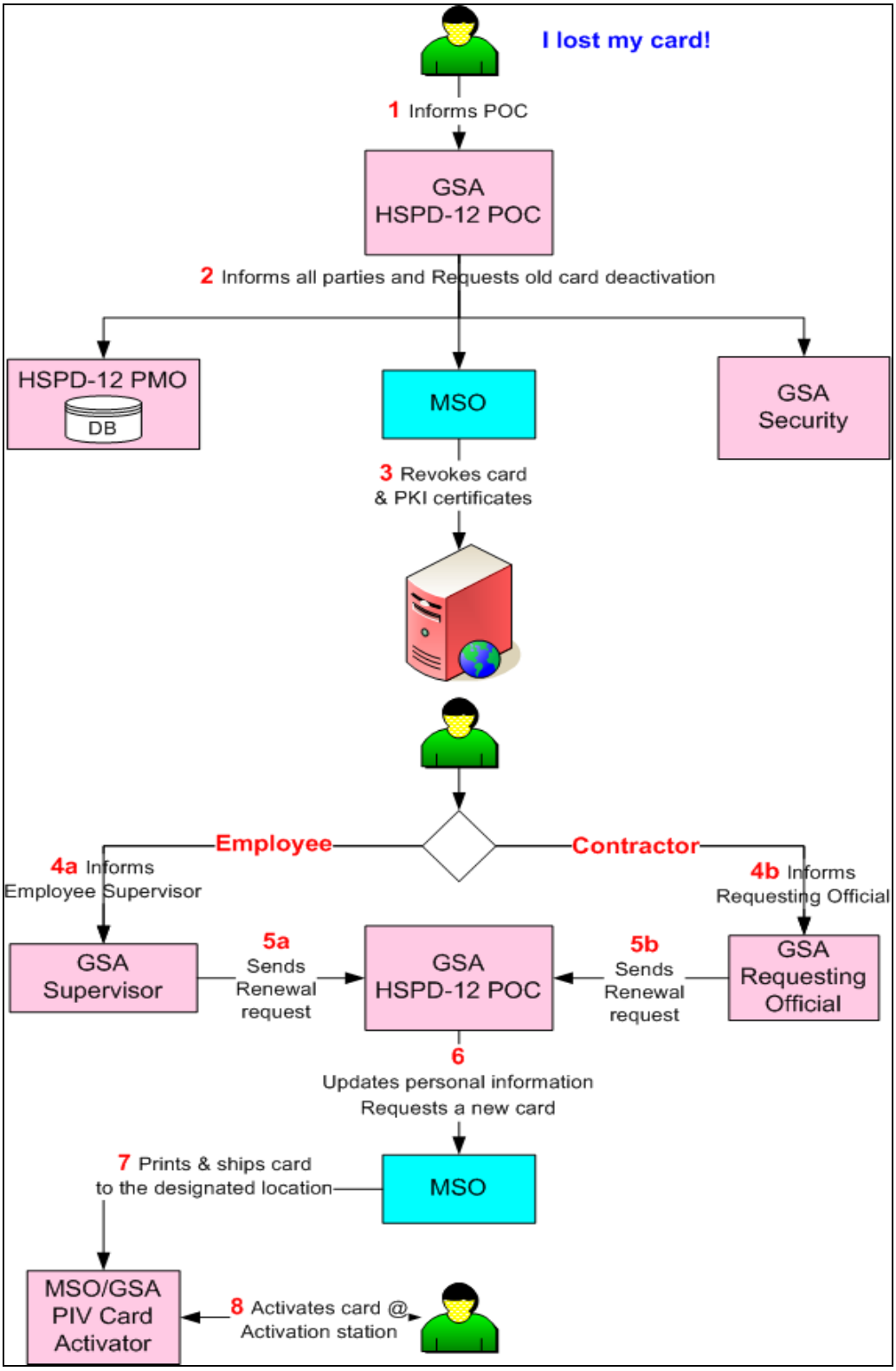
(8) Step 8: Employee/contractor and PIV card activator activate new card.

(a.) Employee/contractor. Appear at MSO/GSA activation point

(b.) PIV card activator. Verify employee/contractor's identity and issue new unactivated PIV card.

(c.) Employee/contractor. Activate new PIV card and load with PKI digital certificates, etc.

Figure 5-4. PIV card re-issuance process (BP 3.3 Card re-issuance)



5. Reset PIN on PIV card. If an employee/contractor needs to reset the PIN on their PIV card, they should schedule an activation appointment. At the Activation Station, the employee/contractor should tell the PIV card activator that they wish to reset the PIN on their PIV card. The employee/contractor then follows the instructions provided by the PIV card activator for resetting a PIV card PIN.

CHAPTER 6. PROVIDING LOGICAL ACCESS TO GSA IT SYSTEMS AND NETWORKS

1. General requirements.

a. GSA employees and contractors requiring access to GSA IT systems and networks must have personnel investigations and other checks appropriate to the level of sensitivity and risk of those IT systems and their contents. Higher impact systems and more sensitive information contents require a personnel investigation appropriate for a higher risk category. (See ch. 2-4 for guidelines on assessing risk levels and the appropriate personnel investigations for each risk level.) The policies and procedures in this SOP apply to GSA employees and contractors who require routine access to GSA IT systems and networks, regardless of the physical location from which an employee or contractor accesses the GSA IT system or network.

b. Access to GSA IT systems and networks is granted in two phases: initial and full. "Initial" access for employees and contractors typically includes access to a workstation, e-mail, the Internet, and low-impact systems needed for their work. "Full" access typically includes access to any moderate or high-impact systems needed for the individual's work that had been excluded from their initial access. Guidelines for setting initial and full access are provided in par. 2 below.

c. Employees and contractors are granted access in two steps (unless access is granted by the authorizing official after verifying an existing required personnel investigation):

(1) Initial access is granted after the completion of a favorable FBI National Criminal History Check and the submission of the appropriate personnel investigation.

(2) Full access is granted only after the completion of the appropriate personnel investigation with favorable results.

d. Temporary contractors (those requiring routine access for 6 months or less) must generally follow the same requirements as employees and long-term contractors.

2. Initial vs. full IT access.

a. Initial and full access shall be defined by the authorizing official (i.e., DAA) commensurate with the individual's job function and for the risk and magnitude of harm that can be done.

b. The following paragraphs provide general guidelines for defining initial and full access. However, each organization, division, or team may have different access requirements based on job descriptions and roles and should use these guidelines to define access accordingly. Access requirements should be documented and approved by the authorizing official.

c. Initial access for an employee or contractor should generally include network access and personal IT applications (e.g., desktop applications, network access, Lotus Notes access – personal and shared mailboxes), shared, and home directory access. It should also include access to low-impact applications as defined by FIPS 199. Access to moderate- impact applications that contain privacy act information should be restricted until full access is granted after the appropriate personnel investigation is completed with favorable results. Likewise, system administrator access should not be given at the Organization Unit (OU), domain, or enterprise level until full access is granted.

d. Initial access to other moderate-impact systems, including those that contain financial information or other sensitive information (i.e., building drawings, etc.), should be limited until full access is granted. If access to these systems is determined to be business critical before the full personnel investigation is complete, then additional compensating controls should be implemented. Additional compensating controls include, but are not limited to, additional logging and review of system logs, stricter access controls (i.e., read-only access), restricted ability to download information to portable media, etc.

e. Upon notification of a favorable full adjudication of the completed personnel investigation, full access to GSA IT systems will be granted commensurate with the individual's job position and duties, unless access is granted by the authorizing official after verifying an existing required personnel investigation.

3. Granting access to IT systems by authorizing officials upon personnel investigation verification. The authorizing official can grant initial or full IT system access after verifying an employee's or contractor's Access National Agency Check and Inquiries (ANACI), National Agency Check with Law and Credit (NACLC), or Single Scope Background Investigation (SSBI). The authorizing official may choose not to grant access to employees or contractors with Access National Agency Check and Inquiries (ANACI), National Agency Check with Law and Credit (NACLC), or Single Scope Background Investigation (SSBI) or other acceptable level of investigation or clearance, but instead require the same GSA personnel security investigations that are required for access to GSA facilities. The COTR or manager verifies with the authorizing official's IT Security representative (normally the ISSM/ISSO) that a memo from the authorizing official has been issued to grant IT system access for employees and contractors with a verified ANACI, NACLC, SSBI, or other acceptable level of investigation or clearance. If the memo from the authorizing official is in place, the COTR or manager works with GSA Personnel Security Requirements Division (OCHCO/CPR) or DHS Federal Protective Service (FPS) to verify the ANACI, NACLC, or SSBI or other acceptable level of investigation or clearance.

4. Initial IT access waiver requests for contractors.

a. According to a GSA Chief Information Officer memo titled "HSPD-12 Waiver Request Process for Contractors" to GSA heads of services and staff offices on March 10, 2008, GSA may need to grant IT access to contractors before their National Crime History Check (NCHC) (commonly referred to as the fingerprint check) results are returned to maintain GSA business operations. The waiver requests should be used judiciously and not place unnecessary risks to GSA assets.

b. The procedures for submitting a waiver request begins when the contracting officer (CO) or contracting officer technical representative (COTR) submits an accurate and complete background investigation (BI package, per U.S. Department of Homeland Security FPS requirements. The CO/COTR then obtains written confirmation that the BI package was accepted by FPS. If written confirmation cannot be obtained, the CO/COTR contacts ITsecurity@gsa.gov.

c. If GSA has not received notification of the results of the fingerprint check 15 business days after the package has been accepted by FPS, the CO/COTR or their designee(s) may send a waiver request for initial IT access to the general support system. The waiver request should be sent via e-mail to the Office of Senior Agency Information Security Officer (OSAISO) at ITsecurity@gsa.gov with the subject line "Waiver Request" and must include the written confirmation that FPS accepted the BI package.

d. If a waiver is requested for a GSA application, the request must be forwarded to the appropriate authorizing official (AO) for approval. If access to the GSA application is available only through the general support system, the contractor must first get approval to access the general support system through OCIO.

e. Waivers for GSA applications should be used in very limited circumstances. If a waiver is approved and GSA is subsequently informed of an "unfavorable" result, the GSA Office of the CIO will immediately terminate all access to GSA IT resources. The waiver process for initial IT access does not impact policies and procedures for physical access to GSA-controlled facilities.

5. Change in employment status. A change in employment status (i.e., contractor to government, government to contractor, region to region, etc.) with no break in service shall not be grounds for removal from an IT system during the adjudication process when access to IT systems is needed to accomplish assigned duties.

CHAPTER 7. PROVIDING PHYSICAL ACCESS TO GSA-CONTROLLED FACILITIES

1. General requirements.

a. GSA-controlled facilities are defined as occupied buildings housing Federal operations under space assignment by GSA. GSA-controlled facilities are leased or owned by GSA, and they may be "partially occupied" or "fully occupied" by Federal agencies. GSA-controlled space is any space in a GSA-controlled facility.

b. GSA-occupied space is defined as space in a GSA-controlled facility assigned to GSA employees and/or contractors.

c. Access to a GSA-controlled facility is based on the facility's established procedures as set by the Building Security Committee (BSC).

d. All GSA employees and contractors who need routine access to GSA-controlled facilitates must follow the policies and procedures set out in ch. 2 of this document when construction for the space has been completed and accepted by the government. The following are exceptions:

(1) The facility is under construction prior to occupancy and is not considered to be "substantially complete." (See par.2, below.)

(2) The facility is involved in a repair and alteration (R&A) project where the work areas are partitioned and/or fully separated from occupied areas, with isolated access for construction contractors and other workers. (See par. 2, below.)

e. GSA contractors do not need personnel investigations and credentials apart from those required by this issuance to work in any GSA-controlled facility except where required by a tenant agency. If a tenant agency has personnel investigation requirements in addition to those provided by GSA, the funding for these investigations will be borne by the requesting agency.

f. GSA policy for non-GSA Federal agency employees and contractors that need routine access to a GSA-controlled facility depends on several factors:

(1) If the facility is federally owned, then tenant agency contractors are subject to the same policies and requirements as defined by OMB.

(2) If the facility is leased, then the background check requirements depend on the Department of Justice (DOJ) risk level of the facility:

(a.) DOJ Level IV facility. Background checks are required of all lessor employees and contractors who require routine access to GSA-controlled lease space.

(b.) DOJ Level III facility solely occupied by the Federal Government. Background checks conforming to the same standards required in GSA-controlled Federal office buildings are required for all leased facilities that are solely occupied by the Federal Government.

(c.) DOJ Level III facility with a GSA child-care center on site. Tenant agency contractors are subject to the policies and requirements defined for GSA contractors.

(d.) All Other DOJ Level III facilities. Background checks are not required.

(e.) DOJ Level I and II facility with a GSA child-care center on site. Tenant agency contractors are subject to the policies and requirements defined for GSA contractors.

(f.) All other DOJ Level I and II facilities. Background checks are not required, but tenant agencies can request a BI on a reimbursable basis.

g. Employees and contractors of tenant agencies who work in space that has been formally delegated by GSA to that agency are not subject to this issuance.

2. Access control on construction sites.

a. A construction project becomes a GSA-controlled facility and subject to the procedures in this issuance upon substantial completion. For repair and alteration projects, work areas that are fully separated from occupied areas with isolated access are classified as construction projects until substantial completion. Therefore, building areas under construction, prior to occupancy, would not fall under this standard, and employees and contractors are not

required to comply with the HSPD-12 program. However, once the construction site is substantially completed, contractors, including all architects and engineers, construction management, consultants, and subcontractors, requiring routine access for more than 6 months in areas of a GSA-controlled facility without separate and isolated access are required to comply with the HSPD-12 program. This regulation affects all construction contract projects awarded after October 27, 2006. Contracts awarded before October 27, 2006 have until April 1, 2009 to implement HSPD-12 standards as applicable.

b. Prior to the commencement of new construction, or of a repair and alteration project, PBS policy regarding personnel investigations on contractors should be reviewed with representatives of the tenant agency, particularly tenant agencies engaged in law enforcement, and the judiciary. Should a tenant agency require personnel investigations on contractors working on a construction project prior to substantial completion, then the funding for these investigations must be provided by the requesting agency. Upon substantial completion, if a tenant agency requires a higher level personnel investigation than the NACI, the funding for these investigations must be borne by the requesting agency.

CHAPTER 8. GSA HSPD-12 PIV HANDBOOK REVISION PROCESS

1. Source of Handbook changes and frequency of revisions. The GSA HSPD-12 PIV Handbook will be reviewed and updated as needed to reflect changes to the GSA HSPD-12 credentialing procedures. Major changes to the Handbook will be addressed every 3 months, and minor changes to the Handbook will be addressed as they are identified. Changes to the Handbook are initiated when a member of the GSA Stakeholders Group identifies a need to revise the Handbook. In addition, the GSA HSPD-12 PMO may also identify potential changes to the Handbook by monitoring for changes to policies and collecting feedback from GSA HSPD-12 applicants and role-holders that may impact the GSA HSPD-12 process. The GSA HSPD-12 PMO will manage the Handbook revision process.

2. Type of Handbook changes. The GSA HSPD-12 PMO identifies whether the proposed revision will result in a major or minor change to the Handbook in the proposed Handbook summary, and the Stakeholder Group verifies the designation of the Handbook type of change. The Handbook is then revised by following the process for either major or minor changes. Following are definitions and examples of major and minor Handbook changes:

a. Major Handbook changes. Major Handbook changes are significant changes to the HSPD-12 role-holder responsibility or procedural requirements in the GSA HSPD-12 PIV Handbook. Major changes require input from an ad hoc Process Working Group selected by the Stakeholder Group, review by the Stakeholder Group and GSA Regions, and an updated Instructional Letter and approval signatures and comments from clearance officers. Examples of major Handbook changes include:

(1) Adding or eliminating a role-holder position or a role-holder's responsibilities, such as forwarding applicant forms to a designated point of contact.

(2) Streamlining process steps as a result of new or enhanced IT systems.

(3) Changes to GSA's requirements to provide physical or logical access.

b. Minor Handbook changes. Minor Handbook changes are changes to the Handbook that do not significantly affect the HSPD-12 role-holder responsibility or procedural requirements in the GSA HSPD-12 PIV Handbook. Minor changes do not require input from an ad hoc Working Group selected by the Stakeholder Group, review by the GSA Regions, or an updated Instructional Letter or approval signatures and comments from clearance officers. A minor Handbook change may significantly affect GSA, but it does not substantially impact the GSA credentialing procedures and does not require extensive coordination and input from GSA HSPD-12 stakeholders. Examples of minor Handbook changes include:

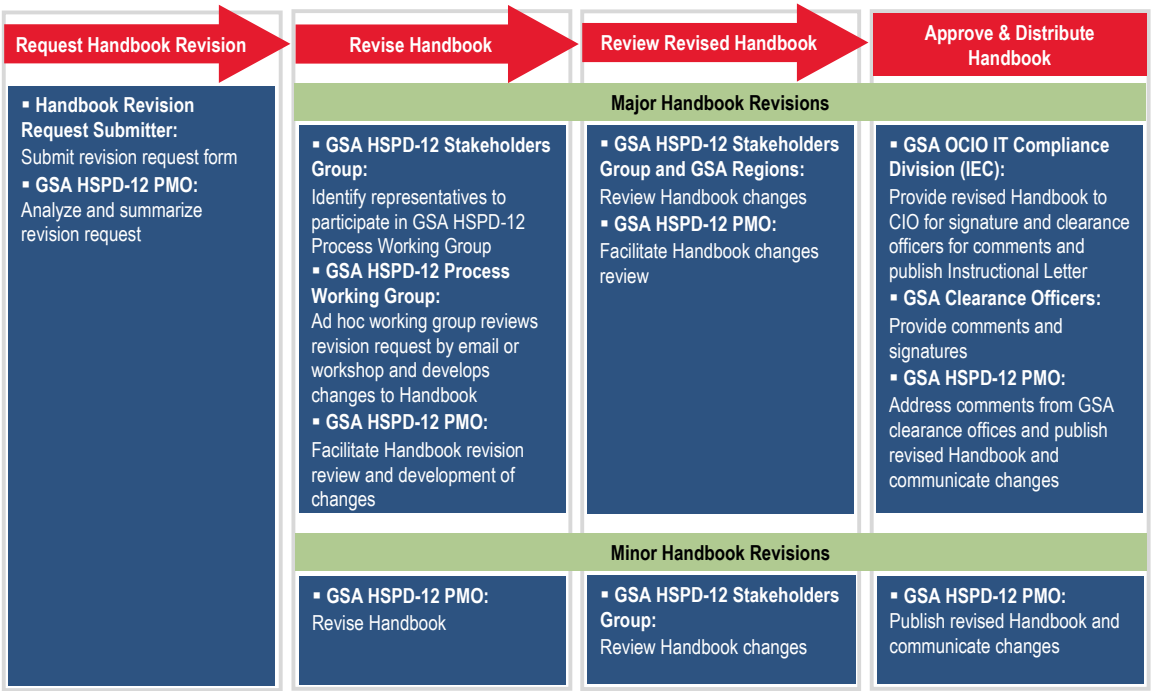
(1) Changes in PIV card attributes

(2) Changes to GSA types of personnel investigations, risk levels for suitability, computer systems, and national security positions, or forms for employees and contractors

(3) Updating a form used in the process

3. Handbook Revision process description. Fig. 8-3 illustrates the Handbook revision process. Attachment H describes the process in more detail.

Figure 8-3. Handbook revision process overview



a. Phase I: Request Handbook revision. The Handbook revision process begins when a member of the GSA stakeholders group submits a revision request to the GSA HSPD-12

PMO. The revision request form (GSA 3687) can be found on the GSA Forms Library at http://www.gsa.gov/Portal/gsa/ep/formslibrary.do?formType=ALL. The GSA HSPD-12 PMO analyzes the request and completes a brief summary of the proposed change. The summary identifies whether the proposed revision will result in a major or minor Handbook change and includes an analysis of issues, offices, or role-holders impacted and identifies other dependencies that are affected by the proposed revision. The GSA HSPD-12 PMO may also identify potential changes to the Handbook.

b. Phase II: Revise Handbook.

(1) If the change is minor, the GSA HSPD-12 PMO develops the changes to the Handbook, the Stakeholder Group reviews the changes, and the GSA HSPD-12 PMO posts the revised Handbook on the HSPD-12 Web pages on GSA InSite at http://insite.gsa.gov/hspd12implementation under Program Management Documents and communicates the changes.

(2) If the changes are major, the Handbook revision process involves more reviews. As the next step, the Stakeholder Group identifies representatives from their offices to serve on a Process Working Group to review the change summary and develop the changes to the Handbook. The Process Working Group is composed of subject matter experts from the offices represented in the GSA Stakeholders Group. An individual may serve on both the GSA Stakeholders Group and GSA Process Working Group. The Process Working Group decides whether a workshop is required to change the Handbook or whether it can be done by e-mail. The GSA HSPD-12 PMO holds a kickoff conference call with the Process Working Group, facilitates the workshop, and identifies any areas of disagreement among the GSA HSPD-12 Process Working Group that require resolution by the working group before the GSA HSPD-12 Stakeholder Group's review.

c. Phase III: Review revised Handbook. The GSA HSPD-12 Stakeholder Group members review the revised Handbook individually and provide feedback by e-mail to the GSA HSPD-12 PMO. The GSA HSPD-12 Stakeholder Group members gather feedback from members of the national and regional offices they represent. The GSA HSPD-12 PMO identifies any areas of disagreement among the GSA HSPD-12 Stakeholder Group that require resolution by the stakeholders before finalizing the draft Handbook. Similarly, the PMO then provides the Handbook to the RCOs for their input to coordinate input from their regions.

d. Phase IV: Approve and distribute Handbook. The GSA HSPD-12 PMO reviews the final draft of the revised Handbook with the GSA OCIO IT Compliance Division (IEC) to determine whether the revisions to the Handbook are major or minor. If the changes to the Handbook are major, the GSA HSPD-12 PMO provides the final draft of the Handbook to the IEC to issue a new Instructional Letter and gather approval signatures and comments from clearance officers. The GSA HSPD-12 PMO responds by e-mail to any comments from clearance officers and copies the IEC on each response. If the comments from the clearance officers lead to a revision to the Handbook, then the GSA HSPD-12 PMO provides the revised Handbook to the IEC to obtain the CIO's signature on a new Instructional Letter. Afterwards, or if the changes to the Handbook are minor, the GSA HSPD-12 PMO posts the revised Handbook on GSA InSite, distributes it to the appropriate individuals, and communicates the change to users and stakeholders.

ATTACHMENT A: LIST OF HSPD-12 RELATED FORMS

Form	Form Description	Date Form Created or Last Updated
CIW	Contractor Information Worksheet (pdf format)	05/2007
SF75	Request for Preliminary Employment Data	08/1998
SF85	Questionnaire for Non-Sensitive Positions	09/1995
SF85P	Questionnaire for Public Trust Positions	09/1995
SF85PS	Supplemental Questionnaire for Selected Positions	09/1995
SF86	Questionnaire for National Security Positions	09/1995
SF86A	Continuation Sheet for SF86, SF85, and SF85-P	09/1995
OF306	Declaration for Federal Employment	01/2001
DHS 176T	Statement of Personal History for Contract and Childcare Personnel)	10/2004
GSA3648	Public Trust Position	08/1998
GSA1380	National Security Position	03/1999
GSA3665	Authorization to Obtain Credit Report	05/1998
SF87	Fingerprint Chart, used for GSA Employees	04/2005
FD-258	Fingerprint Chart, used for GSA contractors	10/2005
PDW	GSA HSPD-12 Personal Data Worksheet	12/2007

The above and other forms, guidelines, and helpful HSPD-12 related information can be found at the following Web sites on the GSA InSite:

GSA Forms Library

http://www.gsa.gov/Portal/gsa/ep/formslibrary.do?pageTypeId=8199&channelPage=%2Fep%2Fchannel%2FgsaOverview.jsp&channelId=-13253

GSA HSPD-12 PMO

http://insite.gsa.gov/Insite/gsa/ep/channelView.do?pageTypeId=8624&channelPage=%2Fep%2Fchannel%2FgsaOverview.jsp&channelId=-11189

GSA HSPD-12 Policy and Guidance Resources

http://insite.gsa.gov/Insite/gsa/ep/contentView.do?programId=10346&channelId=-11189&ooid=12460&contentId=12464&pageTypeId=8624&contentType=GSA_BASIC&programPage=%2Fep%2Fprogram%2FgsaBasic.jsp&P=MVS

ATTACHMENT B: GSA-SPECIFIC INFORMATION FOR SF85

1. HROs are required to complete the following blocks on SF85, Questionnaire for Non-Sensitive Positions:

- Top of SF85 in block named "Codes" place an "R"
- Block "A" –Type of Investigation—place an "02B" for NACI
- Block "B" – Extra Coverage—place a "3"
- Block "C" – Nature of Action (optional)
- Block "D" – Date of Action (optional)
- Block "E" - Location
- Block "F" – Fill in position title
- Block "G" – Local HRO Submitting Office Number (SON)
- Block "H" – SOI (Security Office Identifier) will always be "GS00" in order to return results to CPR
- Block "I" – OPAC-ALC Number—see below
- "47-00-0016" for Staff Offices/FSS
- "47-00-0017" for PBS/FTS only
- Block "J" – Accounting Data and or/Agency Case Number – Pegasys # generated by the requesting office
- Block "K" – Requesting Official, Signature, Phone, and Date. Requesting Officials can only be the HR specialists identified to OPM with the SON request.

2. The HRO is responsible for inserting the Pegasys Document Number (PDN) Number in Block J of the SF85. Otherwise the process could be delayed.

3. There is an OPM fee for processing security investigations. The organization's Pegasys number must be listed on the cover sheet in the funding section in order for it to be processed.

4. HRO must use the SON and only those specialists in HRO that were approved on the SON listing can contact OPM.

5. If forms are not electronically input using OPM's e-QIP system, then the local HRO submits their completed security packages by Fed-Ex to:

OPM-FIPC
1137 Branchton Road
Boyers, PA 16018
Telephone: (724) 794-5612

6. If OPM requests additional information, OPM will contact the requesting official listed on the SF85 in Block K.

7. OPM provides a 3-day respond time for the requesting official listed on the SF85 to respond via e-mail or by fax to (724) 458-6019 to the OPM inquiry.

8. When the requested official listed on the SF85 sends requested documents/information to OPM, the official must identify the applicant's name and the HRO's SON.

9. If the information is not submitted 3 days after OPM has contacted the requesting official, OPM will return the security package to the SON location and the process will start anew upon resubmission of the personnel investigation request to OPM.

10. HRO will input the data for low risk investigations into the Consolidated Human Resources Information System Personnel Security Tracking System (CHRIS PSTS). (Step-by-step instructions for entering information in to CHRIS PSTS is found in Attachment E.)

11. See Attachments A and B for links to SF85, 85P and SF86, and GSA specific instructions on filling out SF85.

12. HRO will make a copy of all low risk investigation packages and send it by mail or fax to CPR at the following address:

General Services Administration
Personnel Security Requirements Division (CPR)
Attn: Security Package Enclosed
1800 F Street, NW, Room G-230
Washington, DC 20405

13. HRO Officers are required to always list the Security Office Identifier (SOI) as "GS00" for security investigation results to be sent directly to the Personnel Security Requirements Division.

ATTACHMENT C: MSO ROLES DESCRIPTIONS

Sponsor The individual who substantiates the need for a PIV credential to be issued to the applicant. The sponsor is also the individual responsible for entering the applicant's sponsorship required data elements and for remaining aware of applicant status and associated continuing need for holding a PIV credential. The sponsor is responsible for managing the employment status of the card holder in the managed service system through a Web interface when a PIV cardholder retires, terminates, or for another reason no longer requires a PIV card.

Adjudicator The individual authorized to record the adjudication result for an applicant. The adjudicator enters or updates the status of adjudication result for an applicant through a Web-enabled interface in the managed service system.

Registrar	The individual responsible for identity proofing the applicant. The registrar confirms that the individual present at time of enrollment is sponsored, inspects two I-9 identity-source documents in original form and scans the documents into the system, takes the applicant's biometrics and photo in accordance with FIPS 201 specifications, live tests and validates the primary and secondary biometric minutia template, and digitally signs and saves the enrollment record.
Activator	The individual responsible for processing card activations. The activator verifies that the applicant is the person to whom the credential is to be issued and guides the applicant through the activation process.
Lead Agency Role Administrator	The agency designated individual responsible for managing the agency role administrators at the agency level (this is a 1:N relationship). This role allows the delegation of role administration down to the subagency level. The scope of the lead agency role administrator is bound to the agency as established in the managed service system. The lead agency role administrator will verify that the appropriate separation of duties policies are followed and will verify that all training certification requirements have been met prior to delegating role administration.
Agency Role Administrator	An agency- or subagency-level individual designated by the lead agency role administrator. The agency role administrator is responsible for managing the agency or subagency's roles (such as sponsor, adjudicator, activator, and agency security officer). The scope of the agency role administrator is bound to the agency as established in the managed service system. The agency role administrator will verify that the appropriate separation of duties policies are followed and will verify that all training certification requirements have been met prior to granting role privileges in the HSPD-12 system.
Agency Security Officer	The individual who is authorized to perform security functions. The agency security officer is an agency-designated individual responsible for managing the card and cardholder security functions in the shared solution. The scope of the agency security officer is bound to the scope of the agency the person is with. The agency security will be able to suspend and terminate a person's card, is authorized to physically collect revoked cards, and will be able to view agency specific security reports and investigate and resolve agency security related issues and incidents identified by the shared solution system.
MSO Role Administrator	The GSA-designated executive responsible for assigning the initial agency primary roles in the managed service system. The MSO role administrator creates the initial accounts for the agency role administrator, sponsor, registrar (if applicable), and adjudicator per the role management policies described in this document. After the initial creation of the HSPD-12 accounts only the registrar and agency role administrator accounts will continue to be managed by the MSO role administrator. The agency role administrator will be responsible for managing the other HSPD-12 roles (sponsor, adjudicator, and activator).

MSO On-Boarding Official The GSA-designated executive responsible for sponsoring and recording the adjudication results for the applicants that will fill the initial agency primary roles in the managed service system. The MSO on-boarding official enters the information required for sponsoring and adjudicating the agency role administrator, sponsor, registrar (if applicable), and adjudicator per the policies described in this document. After the initial sponsorship and recording of adjudication results by the MSO on-boarding official, the agency-designated sponsors and adjudicators will take over the responsibility for entering the information for all remaining agency applicants.

MSO Security Officer The MSO security officer is a GSA-designated executive responsible for the overall security of the shared solution. The MSO security officer will be able to view system security reports and investigate and resolve system security-related issues identified by the shared solution system. For example, when duplicate fingerprints are detected and the scope spans more the one agency, the MSO security officer will investigate the reports and work with the agency security officials to resolve the duplicate fingerprint set issue.

The MSO security officer will also be the point of contact to the Office of the Inspector General (OIG) and will respond to requests from agencies for follow-up action on instances of unauthorized use or abuse. The MSO security officer will coordinate all necessary investigative and follow-up actions with the OIG, law enforcement, and appropriate agency Office of Human Resources Management (HRM).

SSP System Administrator The system administrator role is a shared-solution-designated person. This role is required to support system operations, administration, maintenance, troubleshooting, and MSO role account administration.

ATTACHMENT D: FIPS 201 ROLES DESCRIPTIONS

Applicant The individual to whom a PIV credential needs to be issued.

PIV Sponsor 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.

PIV Registrar The entity responsible for identity proofing 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.

PIV Issuer 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.

PIV Digital Signatory The entity that digitally signs the PIV biometrics and Cardholder Unique Identifier (CHUID). This role only applies for PIV-II.

PIV Authentication Certification Authority (CA)	The CA that signs and issues the PIV Authentication Certificate. This role only applies to PIV-II.

ATTACHMENT E: STEP-BY-STEP PROCESS FOR ENTERING DATA INTO CHRIS-PSTS

Step 1

Before you can initiate a case in *CHRIS PSTS* for an applicant or contractor, you will need to create a *CHRIS* person record. If the person is a current or former agency employee, a *CHRIS* record should already exist for the person. In this case, skip to *Step 1* in the **Initiating Cases** section to begin the process of initiating a case in the system.

After logging into *CHRIS* and selecting the GSA HR Office responsibility that has been assigned to you, select **Applicant** to begin the process of creating a *CHRIS* record for an applicant (if the person is not an agency employee).

Step 2

The **CHRIS Create and Maintain Applicant** form opens. In the *Find Person* window, click on the New button to begin the process of entering information into the **CHRIS Create and Maintain Applicant** form.

Step 3

You will need to change the effective date that will display on this form. To do so, click on the **Alter Effective Date** icon that displays on the tool bar at the top of the form.

Step 4

In the **Alter Effective Date** box that opens, enter a date that is at least 2 months earlier than today's date. You can enter the date manually in the required DD-MMM-YYYY format or you can click on the LOV button and use the calendar to locate and select the appropriate date.

Step 5

Click on the OK button to close the **Alter Effective Date** field. The date entered now displays at the top of in the **CHRIS Create and Maintain Applicant** form and in the **Effective Dates – From** field located at the bottom of the form.

Step 6

In the **Last, First and Middle** fields, enter the appropriate values. **Note:** Only the first letter in the last and first names should be capitalized. **DO NOT** enter titles such as Mr., Ms. Miss, Dr., and etcetera. When there is a need to enter a hyphenated last name, it should be entered without spaces before and after the hyphen (**Example:** Smith-Jones).

Step 7

In the **Gender** field, click on the Down Arrow key and select the appropriate value from the list.

Step 8

In the **Action** field, click on the Down Arrow key, select **Create Applicant**. Values auto-populate into the **Person Types** and **Identification** fields.

Step 9

In the **Social Security** field, enter the appropriate value. **Note:** Be sure to place a hyphen where appropriate.

Step 10

In the **Birth Date** field, enter the appropriate value. **Note:** The value entered should be in the DD-MMM-YYYY format. After pressing the Enter key on your keyboard, the appropriate value auto-populates into the **Age** field.

Step 11

Click on the Save icon located on the toolbar at the top of the screen. Once the record has been saved in *CHRIS*, a confirmation message will display in the bottom left-side of the window.

Step 12

To begin the process of entering the applicant's address, click on the Address button.

Step 13

Click into the **Address Line 1** field to open up the form for entry. Replace the existing value in this field with values that represent the first line of the subject's address. Enter the appropriate values into the remaining fields. **DO NOT** enter values in all capital letters. **Note:** The **only** special characters that can used in any of the fields in this for are #, /, and -. **DO NOT** use special characters such as e.g., @, &, *, and etcetera.

Step 14

After you have entered values into the fields in the form, click on the OK button to close the form.

Step 15

Click on the Save icon located on the toolbar at the top of the screen. Once the record has been saved in *CHRIS*, a confirmation message will display in the bottom left-side of the window. Close the form by clicking on the X located in the top right corner of the *CHRIS* Create and Maintain Applicant **form.**

Initiating Cases

After you have created the *CHRIS* Person record, you can begin the process of initiating a case in *CHRIS PSTS*.

Step 1

From the Certification menu, select Certification

Step 2

In the **Find Person** window, enter the subject's last name into the **Full Name** field and press the Enter key on your keyboard.

Step 3

Highlight the appropriate value in the list and then press the OK button.

Step 4

If appropriate, a **Note** field will display with a message indicating that an active case does not currently exist for the person selected. Click on the OK button. **Note:** If a case exists for the person, *CHRIS* will automatically open up the case file. If a value displays in the **End Date** field, you will be able to click on the New icon (located on the toolbar at the top of the screen, to initiate a new case.

Step 5

The CHRIS Security Tracking System **form opens, the** Subject **tab displays, and values are auto-populated into the fields displayed in the Header section.** Note: **The Header section will always display when the case file is open.** Note: **If the subject is a current agency employee, information about the subject's current position will display in the** Initial Subject Information **section. If anything has changed about the subject's current position since this**

case was initially created, all changes will display in the appropriate fields in the Updated Subject Information **section.**

Step 6

In the **Place of Birth** area, enter the appropriate values into the **City**, **State**, and **Country** fields. To see a list of values available for the **State** and **Country** fields, click on the Down Arrow button that displays after clicking into either field. Otherwise, enter the appropriate 2 character values for either field (e.g., CA, US).

Step 7

Click into the box on the right of **US Citizen** to indicate that the person is a US citizen.

Step 8

If the person is a current agency contractor, enter the appropriate values into the fields listed in the **Initial Subject Information** section. Click into a field and then on the LOV --- button to select from a list of values available for the field. **Note:** If the person is a current agency employee, values will auto-populate into these fields. The information that displays in each field (if appropriate) is related to the person's current position.

Step 9

Click on the **Initiation** tab to begin the process of recording information about the position the person is being investigated for.

Step 10

Click into the white box to the right of **SES Position** to indicate that the person is being investigated for a SES position. **Note:** If a previous case has been processed in the system for this person, a value will display in the **Last Investigation** field.

Step 11

In the **Offered Date** field, enter the date the subject was offered the position. **Note:** The value entered into this field must be fin the required DD-MMM-YYYY format.

Step 12

In the **Position** field, enter the title of the position the person is being investigated for.

Step 13

Click into the **Series** field and enter a value the represents the occupational series of the position the person is being investigated for.

Step 14

Enter values into the remaining fields in the **Target** section. Click into a field and then on the LOV button to select from a list of values available for the field.

Step 15

In the **Duty Station** field, enter the name of the city where the position is located and then press the Enter key on your keyboard. Select the appropriate value from the list that displays.

Step 16

In the **Public Trust Risk Level** area, click in to the **Target** field to see a list of values available for the field. The value that will display in this field will represent the public trust risk level of the position the person is being investigated for. **Note:** If the position is a National Security position, click instead into the **National Security** field (in the **Sensitivity Level** area) to see a list of values to select from.

Step 17

If available, enter values into the fields listed in the **Cleared** area. If a previous case has been processed in the system for this person, values will already display in these fields.

Step 18

If available, enter values into the fields listed in the **Last Break in Fed/Federal Contractor Service** area.

Step 19

If available, enter values into the fields listed in the **SF312** area.

Step 20

To save your entries, click on the Save icon located on the toolbar at the top of the screen. Once the record has been saved in *CHRIS*, a confirmation message will display in the bottom left-side of the window.

Reviewing Investigation Forms

The fields listed under the **Forms** tab can be used to store information about the forms review process.

Step 1

After clicking on the **Forms** tab, click on the Down Arrow button to see a list of values to select from.

Step 2

To place the case on hold because additional/clarifying information is needed about the investigation forms submitted by the person, select **On Hold** from the list available for the **Forms Status** field.

Step 3

Enter the appropriate value into each of the fields in the **Additional Info Requested** section. Click into a field and then on the LOV button to select from a list of values available for the field. **Note:** Date field values must be entered in the DD-MMM-YYYY format.

Step 4

To save your entries, click on the Save icon located on the toolbar at the top of the screen. Once the record has been saved in *CHRIS*, a confirmation message will display in the bottom left-side of the window.

Step 5

When the requested information has been received, click into the white box to the right of the **Add'l Info Received** field (located in the **Information Received** area) and enter the appropriate value into the **Receipt Date** field. **Note:** Date field values must be entered in the DD-MMM-YYYY format.

Step 6

To terminate the case, enter appropriate values into the fields listed in the **Case Closed** area. **Caution:** Entering values into these fields will close the case. No further information can be entered into this case file.

Step 7

To approve the investigation forms submitted by the person, select **Approved** from the list available for the **Forms Status** field. Enter the appropriate values into the **Forms Approved Date** and **Signature Date** fields. **Note:** Date field values must be entered in the DD-MMM-YYYY format.

Step 8

To save your entries, click on the Save icon located on the toolbar at the top of the screen. Once the record has been saved in CHRIS, a confirmation message will display in the bottom left-side of the window.

Requesting Investigations

The fields listed under the **Investigation Request** tab can be used to record information about the type of investigation to be requested.

Note: After clicking on the **Investigation Request** tab, a series of fields will display. Some of the fields are already auto-populated with information. If a previous case has been processed in the system for this person, a value will display in the **Current Certification** field (located at the top of form). The system will display the suggested investigation based on information you have already entered into the case.

Step 1

In the **Accounting Data** field (located in the **Investigation Information** area), enter a value that represents the accounting code associated to the payment of the investigation to be requested.

Step 2

In the **Location** area, click on the Down Arrow button in the **OPF** and **Security Folder** fields to see a list of values to select from.

Step 3

In the next area, enter the appropriate values into the **Position Code** and **OPAC-ALC** fields. After clicking into either field, click on the Down Arrow button to see a list of values to select from.

Step 4

In the **Request Investigation** area, click on the LOV button to select from a list of values available for the field.

Step 5

Click into the white box located to the right of **Requested** to indicate that the investigation has been requested. **Note:** If this case is for a required reinvestigation, click instead into the white box to the right of **Reinvestigation**. Values auto-populate into the **Requester**, **Requested Date**,

and **Phone** fields. **Note:** Values auto-populated into any Date fields in the system can be overridden. However, they must be overridden prior to initiating the Save feature.

Step 6

A value will auto-populate into the **Default** field (in the Cost area) based on the value entered into the **To Request** field (in the **Request Investigation** area). To select additional costs (if appropriate), click into the first row in the **Extra Coverage** area and then on the LOV button to select from a list of values available. If a value is selected, the value in the **Total** field will automatically update.

To save your entries, click on the Save icon located on the toolbar at the top of the screen. Once the record has been saved in CHRIS, a confirmation message will display in the bottom left-side of the window.

ATTACHMENT F: OMB FORM I-9, 1115-0136, EMPLOYMENT ELIGIBILITY VERIFICATION

Figure F-1. List of Acceptable Documents

LISTS OF ACCEPTABLE DOCUMENTS

LIST A Documents that Establish Both Identity and Employment Eligibility	OR	LIST B Documents that Establish Identity	AND	LIST C Documents that Establish Employment Eligibility
1. U.S. Passport (unexpired or expired)		1. Driver's license or ID card issued by a state or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address		1. U.S. Social Security card issued by the Social Security Administration *(other than a card stating it is not valid for employment)*
2. Permanent Resident Card or Alien Registration Receipt Card (Form I-551)		2. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address		2. Certification of Birth Abroad issued by the Department of State *(Form FS-545 or Form DS-1350)*
3. An unexpired foreign passport with a temporary I-551 stamp		3. School ID card with a photograph		3. Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal
4. An unexpired Employment Authorization Document that contains a photograph (Form I-766, I-688, I-688A, I-688B)		4. Voter's registration card		4. Native American tribal document
		5. U.S. Military card or draft record		5. U.S. Citizen ID Card *(Form I-197)*
5. An unexpired foreign passport with an unexpired Arrival-Departure Record, Form I-94, bearing the same name as the passport and containing an endorsement of the alien's nonimmigrant status, if that status authorizes the alien to work for the employer		6. Military dependent's ID card		6. ID Card for use of Resident Citizen in the United States *(Form I-179)*
		7. U.S. Coast Guard Merchant Mariner Card		
		8. Native American tribal document		7. Unexpired employment authorization document issued by DHS *(other than those listed under List A)*
		9. Driver's license issued by a Canadian government authority		
		For persons under age 18 who are unable to present a document listed above:		
		10. School record or report card		
		11. Clinic, doctor or hospital record		
		12. Day-care or nursery school record		

Illustrations of many of these documents appear in Part 8 of the Handbook for Employers (M-274)

Form I-9 (Rev. 06/05/07) N Page 2

ATTACHMENT G: FPS HQ AND REGIONAL OFFICES

Mailing address for Contractor Personnel investigation packages to FPS/Contract Suitability Adjudication Staff – Regional Offices. All security contractor personnel investigation packages will need to be mailed to their respective FPS Regional Office listed below:

Region	Regional CSA PoC	Phone	FAX	Street	Suite, Room	City	ST	Zip + 4
Hq	Evelyn Flores	(202) 732-0215	(202) 732-0210	800 N CAPITOL ST NW	500	Washington	DC	20536-1000
Hq	Elaine Stewart	(202) 732-0213	(202) 732-0210	800 N CAPITOL ST NW	500	Washington	DC	20536-1000
1	Thomas McGoff	(617) 565-5772	(617) 565-5784	10 Causeway Street	935	Boston	MA	02222-1001
2	George L. Ware	(212) 264-0729	(212) 264-9803	26 Federal Plaza	17-130	New York	NY	10278-0004
3	Sheree Reed	(215) 521-2164	(215) 521-2169	701 Market St	4200	Philadelphia	PA	19106-1538
4	Todd Ware	(404) 331-4383	(404) 331-4383	77 FORSYTH ST	700	Atlanta	GA	30303-0000
5	Doris Meaux	(312) 353-4833	(312) 353-0257	230 S. Dearborn St.	3540	Chicago	IL	60604-1505
*6	Robert E Ostrander	(816) 426-2168	(816) 426-2160	601 E 12TH ST	1712	Kansas City	MO	64106-2818
7	Nancy L. Anthis	(817) 334-5283	(817) 334-5282	529 W. Felix Street		Fort Worth	TX	76115-3400
8	Arcadio "Mike" Prado	(303) 236-7813x326	(303) 236-6413	W 6TH Ave&Kipling St		Lakewood	CO	80225-0000
9	May S. Joe	(213) 894-2614	(213) 894-3767	300 N Los Angeles St.	2207	Los Angeles	CA	90012-3322
10	Janis Davis	(253) 815-4709	(253) 815-4754	32125 - 32nd Avenue S.	2nd Fl	Auburn	WA	98001-9345
11	Douglas Avery	(202) 619-9388	(202) 690-3909	3rd & M St SE	220	Washington	DC	20370-0001

Special Note: FPS/R6 personnel investigations will be processed out of the FPS/R8 office, effective ***August 21, 2006*** *until further notice.*

ATTACHMENT H: GSA HSPD-12 PIV HANDBOOK REVISION PROCESS DETAILED DESCRIPTION

Figure H-1. Handbook revision process detailed description. (Part 1 of 2)

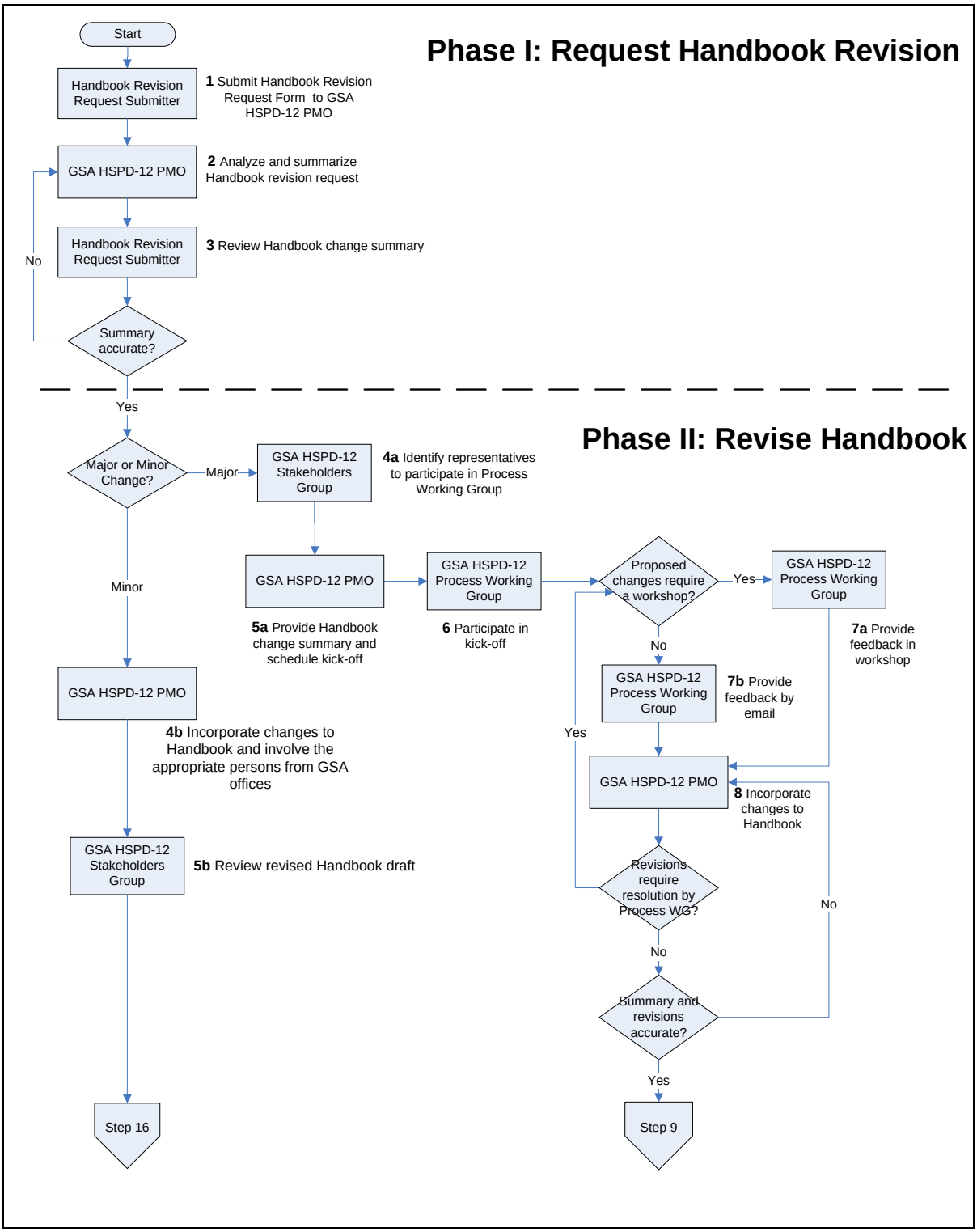
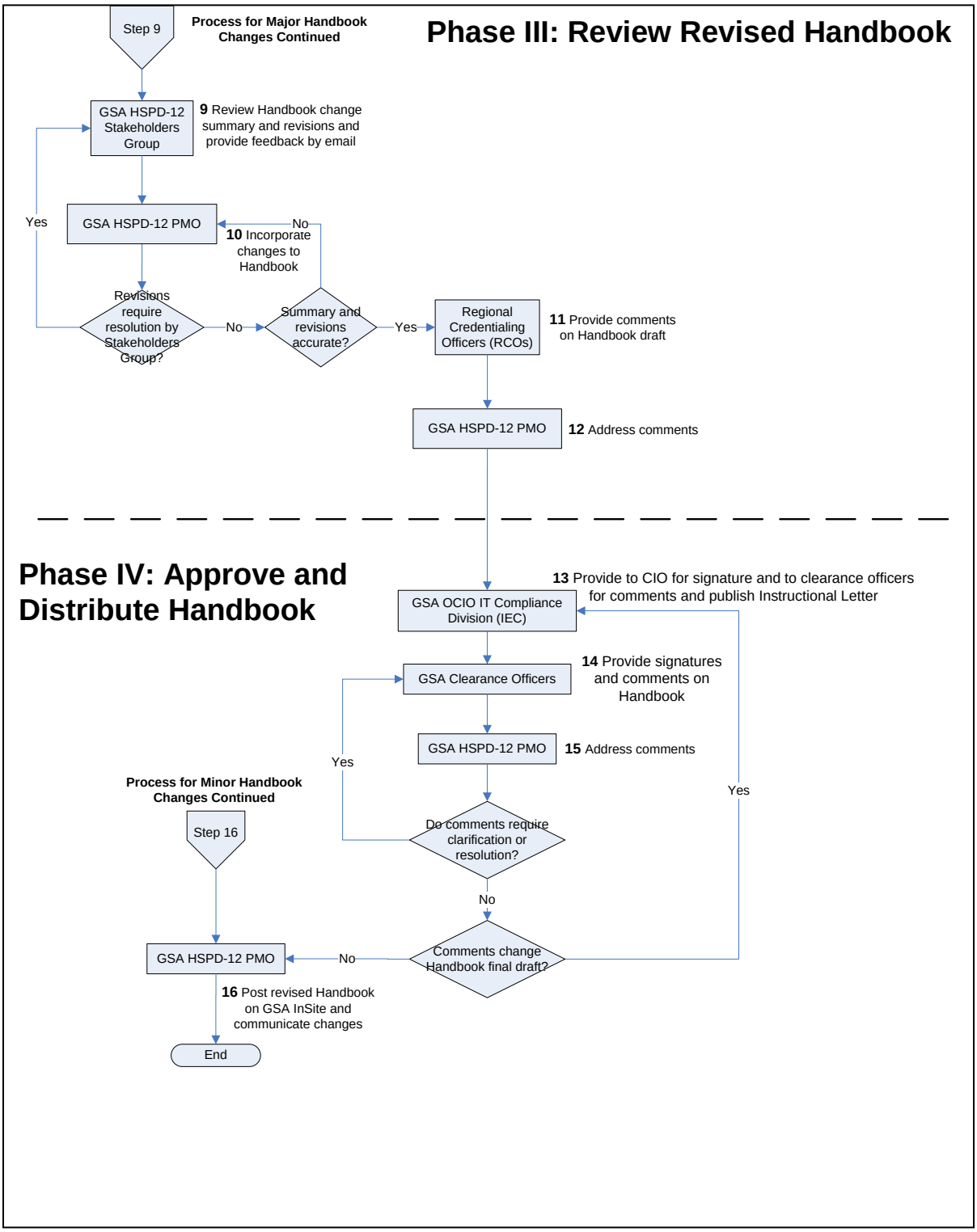


Figure H-1. Handbook revision process detailed description. (Part 2 of 2)



Step-By-Step Process to Revise Handbook

1. Phase I: Request Handbook revision.

   a. Step 1: Revision request submitter submits Handbook revision request form to GSA HSPD-12 PMO.

      (1) A GSA HSPD-12 Stakeholders Group member completes the Handbook Revision Request Form and provides it to the GSA HSPD-12 PMO to identify the Handbook revision request submitter, proposed Handbook revision, reason for revision, new or modified revision request, and level of impact to Handbook. The revision request form (GSA 3687) can be found on the GSA Forms Library at http://www.gsa.gov/Portal/gsa/ep/formslibrary.do?formType=ALL.

      (2) The GSA HSPD-12 PMO will continuously monitor additions and changes to policies that may impact the GSA HSPD-12 process. If GSA HSPD-12 PMO identifies a potential change to the Handbook, the revision process begins at Step 2 when the GSA HSPD-12 PMO completes a brief summary of the proposed change (about 1 page).

   b. Step 2: GSA HSPD-12 PMO analyzes and summarizes Handbook revision request.

      (1) The GSA HSPD-12 PMO completes a brief summary of the proposed change from the Handbook revision request form submitted by a member of the GSA HSPD-12 Stakeholders Group or a change identified by the GSA HSPD-12 PMO.

      (2) The brief summary of the proposed change differs from the Handbook revision request form by identifying whether the change is major or minor and includes an analysis of issues, offices or role-holders impacted, and other dependencies that are affected by the proposed revision.

   c. Step 3: Change request submitter reviews Handbook change summary.

      (1) The GSA HSPD-12 PMO provides the brief summary of the proposed change to the member of the GSA HSPD-12 Stakeholders Group who submitted the revision request to verify its accuracy.

      (2) If needed, the GSA HSPD-12 PMO makes any corrections to the brief summary of the proposed change for accuracy.

      (3) The GSA HSPD-12 PMO proceeds to Step 4a for major changes or Step 4b for minor changes.

2. Phase II: Revise Handbook

   a. Step 4a: GSA HSPD-12 Stakeholders Group identifies representatives to participate in Process Working Group. Every 3 months, the GSA HSPD-12 PMO provides the change summaries completed to date to the GSA HSPD-12 Stakeholders Group to identify the representatives from their offices to serve on the GSA HSPD-12 Process Working Group. (The Process Working Group will later review the change summary and develop the changes to the Handbook.)

   b. Step 4b: GSA HSPD-12 PMO incorporates changes to Handbook and involved appropriate persons from GSA offices. The GSA HSPD-12 PMO incorporates the minor

changes to the Handbook and involves the appropriate persons from GSA offices to complete the revisions.

c. Step 5a. GSA HSPD-12 PMO provides Handbook change summary and schedule kick-off. The GSA HSPD-12 PMO provides the brief summary of the proposed change to the GSA HSPD-12 Process Working Group by e-mail for their review and schedules a kick-off conference call.

d. Step 5b: GSA HSPD-12 Stakeholders Group reviews revised Handbook.

(1) The GSA HSPD-12 Stakeholders Group reviews the revised Handbook individually and provides feedback by e-mail to the GSA HSPD-12 PMO.

(2) After the GSA HSPD-12 PMO addresses any comments from the Stakeholders, the next step is Step 16 when the GSA HSPD-12 PMO posts the revised Handbook on the HSPD-12 Web pages on GSA InSite at http://insite.gsa.gov/hspd12implementation under Program Management Documents and communicates the changes.

e. Step 6: GSA HSPD-12 Process Working Group participates in kick-off. The GSA HSPD-12 PMO holds a kick-off conference call with the GSA HSPD-12 Process Working Group to review the objectives of the Working Group, define the ground rules, and determine whether a workshop is needed to identify whether the Handbook will be revised based on the proposed change and how the Handbook will be revised. A workshop will be held if a majority of the GSA HSPD-12 Process Working Group members determine it is needed.

f. Step 7a: GSA HSPD-12 Process Working Group provides feedback in workshop. If the GSA HSPD-12 Process Working Group determines that a workshop is needed, the GSA HSPD-12 PMO schedules and facilitates a workshop with the GSA HSPD-12 Process Working Group to identify how the Handbook will be revised.

g. Step 7b: GSA HSPD-12 Process Working Group provides feedback by e-mail. If the GSA HSPD-12 Process Working Group determines that a workshop is not needed, the GSA HSPD-12 Process Working Group reviews the Handbook change summary individually and provides feedback by email to the GSA HSPD-12 PMO.

h. Step 8: GSA HSPD-12 PMO incorporates changes to Handbook.

(1) The GSA HSPD-12 PMO incorporates and highlights the changes to the Handbook that were identified from the GSA HSPD-12 Process Working Group.

(2) The GSA HSPD-12 PMO identifies any areas of disagreement among the GSA HSPD-12 Process Working Group that require resolution by the Working Group.

(3) The GSA HSPD-12 PMO provides the revised Handbook to the GSA HSPD-12 Process Working Group to verify the accuracy of the changes.

(4) If needed, the GSA HSPD-12 PMO makes any corrections to the revisions to the Handbook for accuracy before providing the revised Handbook to the GSA HSPD-12 Stakeholders Group for their review.

3. Phase III: Review revised Handbook.

a. Step 9: GSA HSPD-12 Stakeholders Group reviews Handbook change summary and revisions and provides feedback by e-mail.

(1) The GSA HSPD-12 PMO provides the brief summary of the proposed change and the revised Handbook to the GSA HSPD-12 Stakeholders Group for their review.

(2) The GSA HSPD-12 PMO provides an overview of the proposed changes to the Handbook to GSA HSPD-12 Stakeholders Group at the next scheduled Stakeholder Meeting and answers any questions about the proposed changes.

(3) The GSA HSPD-12 Stakeholders Group reviews the revised Handbook individually and provides feedback by e-mail to the GSA HSPD-12 PMO.

(4) The GSA HSPD-12 Stakeholders Group members gather feedback from members of the national and regional offices they represent.

b. Step 10: GSA HSPD-12 PMO incorporates changes to Handbook.

(1) The GSA HSPD-12 PMO incorporates and highlights the changes to the Handbook that were identified from the GSA HSPD-12 Stakeholders Group.

(2) The GSA HSPD-12 PMO identifies any areas of disagreement among the GSA HSPD-12 Stakeholders Group members that require resolution by the Stakeholders.

(3) The GSA HSPD-12 PMO provides the revised Handbook to the GSA HSPD-12 Stakeholders Group to verify the accuracy of the changes.

(4) If needed, the GSA HSPD-12 PMO makes any corrections to the revisions to the Handbook for accuracy before finalizing the draft and providing it to the GSA OCIO IT Compliance Division (IEC).

c. Step 11: GSA HSPD-12 RCOs provide comments on Handbook draft.

(1) The GSA HSPD-12 RCOs review the revised Handbook individually and provide feedback by e-mail to the GSA HSPD-12 PMO.

(2) The GSA HSPD-12 RCOs gather feedback from the regions offices they represent.

d. Step 12. GSA HSPD-12 PMO addresses comments. The GSA HSPD-12 PMO responds by e-mail to any comments from the RCOs.

4. Phase IV: Approve and distribute Handbook.

a. Step 13: GSA OCIO IT Compliance Division (IEC) provides Handbook to CIO for signature and clearance officers for comments and publishes Instructional Letter.

(1) The GSA HSPD-12 PMO provides the final draft of the revised Handbook to the IEC by e-mail. The e-mail message includes:

(a.) Attachment of the final draft of the revised Handbook.

(b.) The number of the last corresponding instructional letter.

(2) The IEC develops an Instructional Letter and provides it and the final draft of the revised Handbook to the CIO for signature. The CIO's signature on the Instructional Letter makes the final draft of the revised Handbook official.

(3) The IEC also provides the revised Handbook to the clearance officers for their comments. A list of the clearance officers can be found on GSA InSite at

http://insite.gsa.gov/wps/portal/gsa_insite/reference_and_resources/directives under Clearance Officers.

b. Step 14: Clearance Officers provide signatures and comments on Handbook. The IEC provides the revised Handbook to the clearance officers to provide their signature of approval and any comments.

c. Step 15: GSA HSPD-12 PMO addresses comments.

(1) The GSA HSPD-12 PMO responds by e-mail to any comments from clearance officers and copies the IEC on each response.

(2) The GSA HSPD-12 PMO may seek clarification from the clearance officers on their comments.

(3) If the comments from the clearance officers lead to a revision to the Handbook, then the GSA HSPD-12 PMO provides the revised Handbook to the IEC to obtain the CIO's signature on a new Instructional Letter.

(4) If no comments are received or the comments do not lead to a revision of the Handbook, then no further action is required by the IEC.

d. Step 16: GSA HSPD-12 PMO posts revised Handbook on GSA InSite and communicates changes. The GSA HSPD-12 PMO posts the revised Handbook on the HSPD-12 Web pages on GSA InSite at http://insite.gsa.gov/hspd12implementation under Program Management Documents, distributes it to the appropriate individuals, and communicates the change to users and stakeholders.

ATTACHMENT I: STATUS OF CHILD CARE CENTERS LEGAL OPINION

July 27, 2006

MEMORANDUM FOR EILEEN STERN
DIRECTOR
OFFICE OF CHILD CARE (PLA)

FROM: LESLY P. WILSON
SENIOR ASSISTANT GENERAL COUNSEL
GENERAL LAW DIVISION (LG)

SUBJECT: Status of Child Care Centers

This memorandum is in response to a request for a legal opinion concerning the status of the child care centers and their employees in our space. You specifically questioned whether the child care centers were "government contractors" especially as it relates to the Presidential Directive HSPD-12. In response to your question it is clear that the child care centers and the employees of the center are not government contractors.

GSA has been Congressionally charged with the regulation and oversight of child care centers by the Trible Amendment. 40 U.S.C. 590. In order to accomplish this responsibility, GSA has

devised a permit document that allows a child care provider to utilize Federal space subject to the child care provider's compliance with certain regulatory conditions. As a convenience, GSA has used a GSA Form 1582, entitled Revocable License for Non-Federal Use of Real Property, and the General and Special Conditions attached thereto, as the vehicle through which the Government permits a Child Care Provider to occupy Government space. No interest in real property is transferred to the child care provider under the license agreement, nor does the license contain or create contractual obligations between GSA and the child care provider. In actuality, this form creates an at-will revocable license that gives GSA the authority to terminate the license to utilize Government space with or without cause, gives GSA the authority to redesignate or reconfigure the Government space to be utilized solely at the discretion of GSA; and gives GSA the authority to have free ingress and egress from the space on a 24-hour basis. A legally enforceable interest in Government utilized space is not created. A contract is not formed.

The Federal Acquisition Regulations (FAR) define the term "contract" in Section 2.101. (48 CFR 2.101). This provision defines "contract" as a mutually binding legal relationship obligating the seller to furnish the supplies or services and the buyer to pay for them. It includes all types of commitments that obligate the Government to an expenditure of appropriated funds. This FAR definition would include any type of relationship where the parties have mutually agreed to take or to forbear to take some action. In this case, GSA has not entered into a mutually agreed upon relationship with the providers. The Special Conditions attached to the License Agreement are not the result of negotiations with the child care providers. These special conditions stipulate the minimum standards for the centers and the providers must agree to abide by these requirements to remain in government space. Consequently, no contract, as the term is defined in the FAR, is created between the GSA and the provider and the providers are not contractors of the Government. As such, they should not be considered contractors under the provisions of Presidential Directive HSPD-12 and required to complete the security background checks imposed on Government contractors by that Directive. Instead, the child care providers should be required to complete the criminal history background checks mandated in the Crime Contract Act of 1990, Pub. L. 101-647, dated November 29, 1990, as amended by Pub. L. 102-190, dated December 5, 1991. These statutes require that each employee of a child care center located in a Federal building or in leased space must undergo a background check that is 1) based on fingerprints taken by a law enforcement officer and on other identifying information, 2) conducted through the FBI's Identification Division and through the State criminal history repositories in each state in which the child care employee has been a resident or has listed in an employment application, and 3) initiated through the personnel program of the applicable employing agency. There is no requirement in these provisions to conduct a full National Agency Check with Written Inquiries (NACI). The NACI is the type of check that will be conducted on government employees or government contractors. Since the employees of the child care provider are neither government employees nor government contractors, there is no requirement in the law or HSPD-12 that would require the child care employees to be subject to the NACI check.

If you have any questions on this matter, please feel free to contact me.

ATTACHMENT J: FEDERAL CHILD CARE CENTER WORKERS FACILITY ACCESS CREDENTIALING

MEMORANDUM FOR HEADS OF DEPARTMENTS AND AGENCIES

FROM: STANLEY KACZMARCZYK
PRINCIPAL DEPUTY ASSOCIATE ADMINISTRATOR FOR GOVERNMENTWIDE POLICY

SUBJECT: FEDERAL CHILD CARE CENTER WORKERS FACILITY ACCESS CREDENTIALING

In order to ensure continuing physical access for child care workers in Federal work places, they will be issued access credentials for regular access to federally-controlled buildings that are compatible with, but both physically and electronically distinct from, the PIV card. These facility access cards (FAC) will enable access to local facilities either through visual inspection and/or electronic processing (via a physical access control system). The following pertains to these FACs:

- Child care workers have limited physical access to Federal facilities (access is limited to specific buildings) and no logical access to Federal IT systems.
- The GSA Office of Identity Solutions will issue the FACs to child care workers on behalf of the Agency Child Care Program Office.
- The Agency Child Care Program Office will provide sponsorship for card issuance and specific building access for all child care workers under its purview.
- Each child care worker will be enrolled for access to the specific buildings that house the child care center at which he/she is employed.
- Upon termination of employment, the Agency Child Care Program Office will ensure the FAC is returned to the appropriate office for revocation and destruction.

These are minimum requirements for issuance of access credentials to Child Care workers in Federal facilities and will be utilized in GSA-controlled and multi-tenant buildings. In other buildings, specific agency hosts may require additional background investigations based on local policy and building security profiles.

Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," requires that Federal Employees and Contractors with routine access to Federal facilities acquire personal identity credentials in accordance with a defined standard. The Standard for these identity credentials was developed by the National Institutes of Standards and Technology (NIST) as Federal Information Processing Standard 201 (FIPS 201), "Personal Identity Verification (PIV) of Federal Employees and Contractors." Tenants of Federal facilities that are neither Federal Employees nor Contractor personnel will not be issued a PIV card unless they undergo the background investigation defined in FIPS 201 section 2. The minimum requirement for a PIV card is the Office of Personnel Management (OPM) National Agency Check with Written Inquiries (NACI).

The General Services Administration (GSA) has been congressionally charged with the regulation and oversight of child care centers by the Trible Amendment, 40 U.S.C. 590. In order to accomplish this responsibility, GSA issues a license agreement that allows a child care provider to utilize Federal space subject to the child care provider's compliance with certain regulatory conditions. One of these conditions is the requirement to complete the criminal history background checks for child care workers mandated in the Crime Control Act of 1990, Pub. L. 101-647, dated November 29, 1990, as amended by Pub. L. 102-190, dated December 5, 1991. These statutes require that each employee of a child care center located in a Federal building or in leased space must undergo a background check that is 1) based on fingerprints taken by a law enforcement officer and on other identifying information, 2) conducted through the FBI's Identification Division and through the State criminal history repositories in each state in which the child care employee has been a resident or has listed in an employment application, and 3) initiated through the personnel program of the applicable employing agency. The GSA Child Care Operations Division has worked with the Office of Homeland Security to ensure that all child care workers in Federal work places have gone through the security check process mandated by the Crime Control Act. However, this criminal history check is not the equivalent of the FIPS 201-mandated minimum NACI because it lacks the written inquiries component. Therefore, child care workers are not eligible for PIV credentials under HSPD-12 and will therefore be issued facility access cards as specified above.

For additional information, please contact Eileen Z. Stern, Director, Child Care Operations Division, 212.264.8321, eileen.stern@gsa.gov; or Judith Spencer, Office of Technology Strategy, 202-208-6576, judith.spencer@gsa.gov.

ATTACHMENT K: DEFINITION OF TERMS

Adjudicator – The individual who adjudicates and attests to the results of the personnel investigation for each agency's applicants for the MSO credentialing system.

Administrator – The individual who identifies, assigns, and manages system roles for each Agency for the MSO credentialing system.

Agency Security Officer – A new MSO role request; the individual who has the ability to immediately revoke a card upon termination or other security event.

Authenticate – The process of establishing confidence of authenticity; in this case, in the validity of a person's identity and the PIV card.

Applicant Access Rights – The process of determining what types of activities or access are permitted for a given physical or logical resource. The process is performed by the registrar. Once the identity of the user has been authenticated, the registrar has the authorization to determine whether the applicant has access to a specific location, system, or service.

Background Investigation (BI) – Type of investigation covering specific areas of a person's background. The personnel investigation consists of a record search, credit search, and a NAC, NACI, or similar OPM investigation. The investigating agency interviews the candidate and selected sources.

Biometric - A measurable, physical characteristic or personal behavioral trait used to recognize

the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

Card Activator – The individual who assists the applicant in activating the PIV card and confirms that the card is "active" and recognized by the HSPD-12 system.

Card Personalization - The modification of a card such that it contains data specific to the cardholder. Methods of personalization include encoding the magnetic stripe or bar code, loading data on the ICC, or printing photo or signature data on the card.

Contracting Officer/Contracting Officer's Technical Representative (CO/COTR) – Federal representative who takes appropriate action to protect GSA employees, property, and interest.

Escorts – Government employees and contractors who have received favorable personnel investigations (NACI at a minimum) and possess valid PIV-II GSA credentials.

Favorable adjudication of personnel investigation – Decision made by the Human Resources Security Office about an applicant's personnel investigation. A favorable adjudication indicates that the applicant is suitable for GSA hiring and is capable of retaining a GSA card.

Federal Identity Management Handbook –Handbook was developed in collaboration with the FICC, IAB, FPKIPA, and OMB. It is offered as an implementation guide for government agency credentialing managers, their leadership, and other stakeholders as they pursue compliance with HSPD-12 and FIPS 201. The handbook provides specific implementation direction on course of action, schedule requirements, acquisition planning, migration planning, lessons learned, and case studies.

Federal Information Processing Standard (FIPS) - A standard for adoption and use by Federal departments and agencies developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability.

Federal Information Processing Standard 201 (FIPS 201) Standard written in response to the HSPD-12 directive and published by the National Institute of Standards and Technology (NIST) on February 25, 2005. FIPS 201 and its associated Special Publications provide a detailed specification for Federal agencies and departments deploying personal identity verification (PIV) cards for their employees and contractors. The FIPS 201 standard can be accessed from the NIST web site at http://csrc.nist.gov/piv-project/index.html.

Full Access - Access to sensitive information such as financial systems and PII data beyond what is granted for Initial Access.

GSA controlled facilities – Occupied buildings housing Federal operations under space assignment by GSA

GSA occupied space – Assigned space occupied by GSA employees or contractors

Homeland Security Presidential Directive-12 (HSPD-12) – Directive ordering the creation of a common Federal standard for secure and reliable identification issued by Federal agencies for their employees and contractors.

I-9, OMB No. 1115-0136, Employment Eligibility Verification – Form presented by the applicant to the PIV registrar to assist the registrar in the identity proofing process.

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

Identity Verification - The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV card or system and associated with the identity being claimed.

Initial Access – Access granted to an individual after a favorable FBI fingerprint check. It is currently defined as access to the network (logon), e-mail, and shared directories. Most employees will only need Initial Access to perform their duties. If the results of the fingerprint check are unfavorable, the individual must wait for the full investigation to be completed and a final determination of suitability before credentialing and access is granted

Involuntary Separation –Separation against the will of and without the consent of the employee, other than separation for cause on charges of misconduct or delinquency. Examples include separation based on the reduction of force, abolishment of position, expiration of term of office, lack of funds, and unacceptable performance (unless due to employee's misconduct).

Logical Access - An individual's ability to access one or more computer system resources such as a workstation, network, application, or database. Different access privileges are provided to different persons depending on their roles and responsibilities in the agency.

National Agency Check (NAC) – Record searches with selected sources covering specific areas of a person's background. Standard NACs are: Security/Personnel Investigation Index (SII), Defense Clearance Investigation Index (DCII), FBI Name Check, FBI National Criminal History Fingerprint check. Optional checks can include: credit, military personnel record, citizenship, BVS, Selective Service (males born after 12/31/59), Central Intelligence Agency, and State Department.

National Agency Check with Written Inquiries (NACI) –Investigation consisting of a NAC and written inquiries covering specific areas of a person's background during the past 5 years. All coverage is obtained through written inquiry and computer linkages. Coverage includes: employment, education (highest degree verified), residence, references, law enforcement, and NACs.

National Security Clearance – Certification issued by the GSA Security Officer or designee that a person can access classified information on a need-to-know basis.

National Security Position – A sensitive position under EO 10450. Usually, persons in national security positions hold security clearances, although some employees can be considered eligible for clearances rather than actively holding the clearances.

National Institute for Standards and Technology (NIST) –A non-regulatory Federal agency within the U.S. Commerce Department's Technology Administration founded in 1901. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST developed the FIPS 201 document as a follow up to the HSPD-12 directive and to provide suggestions for agency implementation.

Non-sensitive position – A position that does not require access to classified information and that has low risk to the national security and public trust.

Office of Personnel Management (OPM) – OPM's main role in the credentialing process is to receive personnel investigations requests from the HR Security office, perform personnel investigations on applicants, and deliver the results of the personnel investigations to the HRO Security Office where the results will be adjudicated.

Personal Identity Verification (PIV) - A physical artifact (e.g., identity card, smart card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

Personally Identifiable Information (PII) –Information about a person that contains some unique identifier including, but not limited to, name or Social Security Number, from which the identity of the person can be determined, and name plus home street and email addresses. In OMB M-06-19, the term "Personally Identifiable Information" means any information about an individual maintained by an agency including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, date and place of birth, mother's maiden name, or biometric records, including any other personal information that is linked or linkable to an individual.

Personnel Investigation - A background investigation through written, electronic, telephone, or personal contract to determine the suitability, eligibility, or qualifications of a person for Federal employment, work on Federal contracts, or for National Security purposes

Physical Access - An individual's ability to access a physical location such as a building, parking lot, office, or other designated physical space. Different access privileges are assigned to different persons depending on their roles and responsibilities in an agency.

PIV credential issuance/issuance process –PIV card distribution from the issuer to the applicant.

Routine access – Requiring regularly scheduled access to a particular building or information system. For example, a contractor who reports to a GSA facility on a daily basis in the performance of ongoing duties requires routine access and must have personnel investigation. An intermittent contractor, for example one who is summoned for a service call as needed, is not required to have personnel investigation and can be issued a daily visitors pass

Security Package –All documents and forms compiled by the HR Specialist submitted with the purpose of obtaining initial and full access.

Sponsor – The individual who enters information about card applicants and attests to the applicant's affiliation with each agency.

Substantially Complete and **Substantial Completion –** Indicator that the work, the common, and other areas of the building, and all other things necessary for the Government's access to the premises and occupancy, possession, use and the enjoyment thereof, as provided in a specified lease, have been completed or obtained, excepting only such minor matters as do not interfere with or materially diminish such access, occupancy, possession, use or enjoyment. (See GSA Form 3517B (REV 11/05).

Temporary Contractor – Contractor requiring routine access to federally controlled facilities for 6 months or less.

Unfavorable adjudication of personnel investigation – Decision made by the Human Resources Security Office about an applicant's personnel investigation. An unfavorable adjudication indicates that the applicant is not suitable for GSA hiring, and the GSA card can be revoked. If an appeal is made by the applicant this determination can be changed.

ATTACHMENT L: ACRONYMS

ALC: Agency Location Code
ANACI: Access National Agency Check Inquiry
BI: Background Investigation
CHCO: Chief Human Capital Office
CHRIS: Consolidated Human Resources Information System
CPR: Personnel Security Requirements Division
CO: Contracting Officer
COTR: Contracting Officer Technical Representative
DAA: Designated Approving Authority
DHS: Department of Homeland Security
DOB: Date of birth
DOJ: Department of Justice
E-QIP: Electronic Questionnaire for Investigation Processing
FBI: Federal Bureau of Investigations
FIPC: Federal Investigations Processing Center
FIPS: Federal Information Processing Standard
FPS: Federal Protective Service
GSA: General Service Administration
HR: Human Resources
HRO: Human Resource Officer
HSPD–12: Homeland Security Presidential Directive – 12
HSSO: Head of Services and Staff Offices
ID: Identification
IT: Information Technology, Information Systems
LBI: Limited Background Investigation
MBI: Minimum Background Investigation
MOA: Memorandum of Agreement
NAC: National Agency Check
NACI: National Agency Check with written Inquiries
NCR: National Capital Region
NIST: National Institute for Standards and Technology
OCIO: Office of the Chief Information Officer
OF: Optional Form
OMB: Office of Management and Budget
OPF: Official Personnel Folder
OPM: Office of Personnel Management
OU: Organization Unit
PBS: Public Building Service
PDN: Pegasys Document Number

POB: Place of birth
PII: Personally Identifiable Information
PKI: Public Key Infrastructure
PIV: Personal Identity Verification
PMO: Program Management Office
PSTS: Personnel Security Tracking System
RA: Regional Administrator
R&A: Repair and Alteration projects
SAC: Special Agency Check
SF: Standard Form
SOI: Security Office Identifier
SON: Submitting Office Number
SSBI: Single Scope Background Investigation
SSN: Social Security Number