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: