Privacy Impact Assessment
of
Personal Identity Verification Program

Program or application name.

Personal Identity Verification (PIV) Program

System Owner.

Board of Governors of the Federal Reserve System's (Board) Management Division

Contact information:

Title:	Human Resources Manager, Personnel Security
Organization:	Management Division
Address:	20th & C Streets, N.W., Washington, D.C. 20551
Telephone:	202-872-4959

Title:	Manager, Technical Security Unit
Organization:	Management Division
Address:	20th & C Streets, N.W., Washington, D.C. 20551
Telephone:	202-452-3331

Summary description of the program or application.

The PIV program implements a secure and reliable form of identification for the Board's employees and contractors that meet the government-wide standards for identifying Federal Government employees and contractors pursuant to Homeland Security Presidential Directive 12 (HSPD 12), dated August 27, 2004, entitled "Policy for a Common Identification Standard for Federal Employees and Contractors." Pursuant to HSPD 12, the Board is issuing PIV cards to employees and contractors that are based on sound criteria for verifying an individual employee's or contractor's identity; strongly resistant to identity fraud, tampering, counterfeiting and terrorist

exploitation; rapidly authenticated electronically; and issued only by providers whose reliability has been established by an official accreditation process.

In the implementation of the PIV program, Board staff utilize personal information collected directly from individual employees, contractors, or affiliates (Applicants), as well as information collected, maintained or disseminated in the Board's Personnel Security and Electronic Security systems and in electronic systems maintained by the Office of Personnel Management (OPM) and the General Services Administration (GSA) to submit and process a request for a PIV card. Board division administrators, contracting officers, and recruiters, designated as PIV Sponsors, establish the need of an individual Applicant for a PIV card. The PIV Sponsor enters certain personal information collected from Applicants into a GSA system and submits the request for a PIV card. The Board Management Division's office of Personnel Security, designated as the PIV Registrar, substantiates the identity of the Applicant by checking identity source documents, performing identity proofing, and uploading the information into the GSA system. The PIV Registrar also ensures that appropriate information is received from the Applicant, including a completed background investigation questionnaire (OPM Standard Form 85P (or equivalent or higher)), to enable OPM to conduct and complete the proper background check required for HSPD-12. The PIV Registrar also collects physical characteristics, portrait, and fingerprints and uploads the information into the GSA system. The Board's Personnel Security Officer reviews the result of the completed background checks and, if favorable, authorizes the creation of the PIV card. The Management Division's Law Enforcement Unit receives a blank PIV card from GSA and electronically loads the blank PIV card with the fingerprint, portrait, identity information, and a government-wide identifier unique to the Applicant, and delivers the personalized PIV card to the Applicant along with appropriate instructions for protection and use.

1. The information concerning individuals to be collected and/or maintained.

The PIV program collects, maintains or disseminates the following personal information:

a. Applicant's full name;

b. Social security number;
c. Date and place of birth;
d. Employee, contractor or affiliate identification number;
e. PIV cardholder's unique identifier;
f. Applicant's affiliation (for example, employee or contractor);
g. Home address;
h. Home telephone number;
i. PIV card status (for example, active or inactive)
j. Additional information from Applicant's completed background investigation questionnaire;
k. Applicant's fingerprint images and fingerprint minutiae (which is a numeric representation of the fingerprint);
l. Applicant's electronic facial image (together with any additional biometric data of the Applicant that may be collected in the future);
m. Physical characteristics used to validate Applicant's identity (for example, height, weight, eye color, or hair color);
n. Results of the completed OPM background checks, including a check of the Security/Suitability Investigations Index, Defense Clearance and Investigations Index, FBI Name Check, and FBI National Criminal History Fingerprint Check;
o. Results of written inquiries and searches of records covering specific areas of an Applicant's background during the past five years (for example, inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities); and
p. Emergency Response Official designation (that is, whether the Applicant is designated as an emergency responder).

2. Source(s) of each category of information listed in item 1.

Board staff utilize personal information collected directly from individual employees, contractors, or affiliates (Applicants), as well as information collected, maintained or disseminated in the Board's Personnel Security and Electronic Security systems, as well as electronic systems maintained by the Office of Personnel Management (OPM) and the General Services Administration (GSA) to submit and process a request for a PIV card, including:

a. Applicant's completed background investigation questionnaire (OPM SF 85P or its equivalent or higher);
b. identity source documents – at least one of which must be a valid picture ID issued by a state or by the Federal Government, together with any information concerning the source documents used for identification that might include address, birth date, social security number;
c. copies of the Applicant's fingerprints and other relevant materials that may be used to validate an Applicant's identity;
d. Checks of the Security/Suitability Investigations Index, Defense Clearance and Investigations Index, FBI Name Check, and FBI National Criminal History Fingerprint Check; and
e. Written inquiries and searches of records covering specific areas of an Applicant's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).

3. Purpose for which the information is being collected.

The information in PIV is collected pursuant to sections 10 and 11 of the Federal Reserve Act, 12 USC 243 and 248, and Homeland Security Presidential Directive 12, dated August 27, 2004, entitled "Policy for a Common Identification Standard for Federal Employees and Contractors." The information collected for PIV is necessary to permit Board staff to make a determination whether an Applicant is eligible for the issuance of a PIV card. The PIV card will enable employees, contractors and affiliates to gain physical access to the Federal Reserve premises, and is a platform to allow future logical access to the Federal Reserve as well as physical and logical access at other government agencies, systems and facilities.

4. Who will have access to the information.

For the most part, access to data by a user within the Federal Reserve is limited to authorized employees within the Federal Reserve who have a need for the information for official business purposes. The information will also be shared with the OPM for the purpose of conducting the appropriate fingerprint and background checks, the FBI for inclusion in the FBI's fingerprint database, and with GSA for the purpose of submitting and processing a request for a PIV card. In addition, the information in PIV may also be disclosed for enforcement, statutory and regulatory purposes; to

another agency or a Federal Reserve Bank; to a member of Congress; to the Department of Justice, a court, an adjudicative body or administrative tribunal, or a party in litigation; to the Equal Employment Opportunity Commission, the Merit Systems Protection Board, the Office of Government Ethics, or the Office of Special Counsel where necessary to carry out their authorized functions; to contractors, agents, and others; to appropriate agencies, entities, and persons who are reasonably necessary to assist in connection with the Board's efforts to respond to the suspected or confirmed compromise of security or confidentiality and prevent, minimize, or remedy such harm; to appropriate federal, state, local, or foreign agencies where disclosure is reasonably necessary to determine whether an individual intending to visit the Board poses a security risk; or to other agencies, entities, and persons reasonably necessary to assist the Board's efforts to respond to a suspected or confirmed compromise of security or confidentiality to prevent, minimize or remedy such harm.

5. Whether the individual to whom the information pertains has an opportunity to decline to provide the information or to consent to particular uses of the information (other than required or authorized uses).

While Applicants are not required to provide the information requested for the PIV program, their failure to provide any of the requested information will provide the Board of Governors with grounds for denying them access to the Board's premises and any other Federal facility. Since access to the Board's premises or other Federal facility may be a necessary prerequisite to the Applicant's retaining employment or performing a contract, the failure to provide the necessary information may result in the denial or withdrawal of employment or a contract.

6. Procedure(s) for ensuring that the information maintained is accurate, complete, and up-to-date.

The majority of the information collected, maintained and disseminated in the PIV program is provided by the Applicant. The submission and processing of a request for a PIV card requires independent verification of identity source documents by the Board Management Division's office of Personnel Security as well as verification with the Applicant that information submitted to the GSA system is accurate and complete. The issuance of a PIV card also requires independent verification of a state or

federal government-issued photograph identification by the Board Management Division's Law Enforcement Unit prior to the card's issuance to the Applicant.

7. The length of time the information will be retained, and how will it be purged.

Information in PIV is stored in both paper and electronic form. The retention period for these records is currently under review. Until review is completed, these records will not be destroyed.

8. The administrative and technological procedures used to secure the information against unauthorized access.

Paper copies of the information are maintained in a secure manner in locked file cabinets and locked vaults. Access to electronic information stored in the Board's databases as well as to the OPM systems is limited to authorized personnel with password controls who have restricted access to a locked room. Access to electronic information stored in the GSA system is limited to authorized personnel with password controls.

9. Whether a new system of records under the Privacy Act will be created. (If the data is retrieved by name, unique number, or other identifier assigned to an individual, then a Privacy Act system of records may be created.)

The information collected in PIV will be maintained in two separate systems of records created by the Board under the Privacy Act of 1974, 5 U.S.C. 552a, because the information will be capable of retrieval by name, unique number or other identifier assigned to the individual: the Staff Identification Card File, (currently identified as SS-2);[1] and the Personnel Security system, a new Privacy Act system of records (which will be designated as BGFRS-2). In the implementation of the PIV program, information will also be maintained in a Privacy Act system of records maintained by the GSA (GSA

[1] This system is currently being revised and will be republished as the Electronic Security System (BGFRS-34).

Smart Card Program (GSA/CIO-1)), and a system of records maintained by the OPM (OPM/CENTRAL-9).

Reviewed:

(signed) Elaine Boutilier	12/20/2007
Chief Information Officer	Date
(signed) Maureen Hannan	12/20/2007
Chief Privacy Officer	Date