



Privacy Impact Assessment Form

**PERSONAL IDENTITY VERIFICATION IDENTITY
MANAGEMENT SYSTEM (HSPD-12)**
(SYSTEM NAME)

This document is only used when the Chief Privacy Officer determines that the system contains personally identifiable information and a more in depth assessment is required.

Complete and sign this form and forward to the Chief Privacy Officer.

David A. Lee
Federal Housing Finance Agency
1700 G Street NW
Washington, DC 20552
(202) 414-3804
David.Lee@fhfa.gov

Guidance for Completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how information in identifiable form is handled. PIAs are to be completed when FHFA: 1) develops or procures IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public; or 2) initiates a new electronic collection of information in an identifiable form for 10 or more members of the public. System owners and developers are responsible for completing the. The guidance below has been provided to help the system owners and developers complete the PIA.

Overview

- This section should provide a thorough and clear overview of the system and give the reader the appropriate context to understand the system owner's responses in the PIA. What is the purpose of the IT system? What will be the primary uses of the system? How will this support the program's mission?
- This section fulfills the E-Government Act's requirement for an introduction for members of the public who may be reading the PIA. PIAs will be made publicly available (unless a determination is made to not make the PIA available because publication would raise security concerns and/or reveal classified or sensitive information).

Section 1.0 Characterization of the Information

- Identify if the system contains information about individuals, versus statistical, geographic, or financial, with no link to a name or other identifier, such as name, home address, social security number, account number, home telephone and fax numbers, or personal e-mail address.
- Examples of sources of the information include information that comes from individuals applying for loans, mortgages, and forms individuals completed. Where does the data originate? (e.g., the FHA, Office of Personnel Management, and Financial Institutions). A third party is usually a non-Federal person or entity, which may be a source of data/information (e.g., a bank, an internet service provider, an organization).
- If the system collects information from 10 or more members of the public, ensure that the agency has received OMB's approval to do so or determine whether OMB's approval is needed to collect the information in accordance with the Paperwork Reduction Act of 1980.

Section 2.0 Uses of the Information

- Identify the primary uses of the information and how the information supports the program's mission.
- Identify the controls that are in place to ensure the information will be used for the manner for which it was collected. For example, access to the information will be restricted a limited number of program staff who use the data for their specific program use.

Section 3.0 Retention

- The Privacy Act requires agencies to address the retention and disposal of information about individuals. (The retention information is published in the Privacy Act system of records notice).

- The retention periods of data/records that the agency manages are contained in either the NARA General Records Schedule or agency Records Schedule. For the data being created/maintained in the system, the records schedules are the authoritative sources for this information.
- Disposing of the data at the end of the retention period is the last state of life cycle management. Records subject to the Privacy Act have special disposal procedures (e.g. shredding of paper documents).

Section 4.0 Notice, Access, Redress and Correction

- The Privacy Act at 5 U.S.C. 552a(e)(1) requires that "each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."
- Data can be retrieved in a number of ways, but there is usually a personal identifier associated with a record. If the system retrieves information by an individual's name or other personal identifier it is a Privacy Act system and may need a system of records notice (SORN published in the Federal Register. The system may already have a Privacy Act SORN that applies to it. If you do not have a published SORN, contact the Privacy Act Officer. The Privacy Act requires that amendments to an existing system must also be addressed in a Federal Register notice. Any employee who knowingly and willfully maintains a systems of records without meeting the Privacy Act notice requirements (5 U.S.C. 552a(e)(4)) is guilty of a misdemeanor and may be fined up to \$5,000.
- If a name or other personal identifier is not used to retrieve information, it is possible that the system is not a Privacy Act system. However, even though information may not fall under the Privacy Act's protection and requirements, certain information may be protected from disclosure under the Freedom of Information Act.
- The agency has developed and published an agency specific Privacy Act Rule in the Federal Register (12 CFR Part 1204) that explains how individuals can gain access to information about themselves and correct errors if appropriate.
- The Privacy Act of 1974 requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. These requirements are statutory and need to be addressed. If the data does not meet any one of these four components, then fairness in making any determination is compromised.

Section 5.0 Sharing and Disclosure

- If it is unknown to you whether or not systems share data, you can either contact the business owner of the data, or you can contact the IT specialist who knows what other interface goes on between the systems/applications. As an example, if your system/application shares data with another system/application, ask yourself whether you have access to the data in the interfaced system/application. If so, then your answer is yes and an explanation is needed.
- Also consider "other" users who may not be obvious as those listed, such as the GAO or the Inspector General. "Other" may also include database administrators or IT Security Officers. Also include organizations listed in the Privacy Act system of records notice

under the “Routine Use” section when a Privacy Act system of records notice is required. The more comprehensive the list, the better it is.

- You must first review appropriate SORN to determine whether any information that may come from an existing SORN allows that information to be exchanged and used for these new purposes or uses. There are statutory restrictions on use and disclosure of information that comes from a SORN.

Section 6.0 Technical Access and Security

- For the most part, access to data by a user within FHFA is determined by the “need-to-know” requirements of the Privacy Act (this means to authorized employees within the agency who have a need for the information to perform their duties). Care should be taken to ensure that only those employees who need the information have access to that information. Other considerations are the user’s profile based on the user’s job requirements and managerial decisions.
- The criteria, procedures, controls and responsibilities regarding access must be documented to comply with the intent of the Federal Information Security Management Act of 2002 for standards and guidelines on security and privacy. What criteria will the manager and system security person use to decide on access to the data, for example?
- The system owner is responsible for ensuring that access to information and data is restricted to authorized personnel. Usually, a user is only given access to certain information that is needed to perform an official function. Care should be given to avoid “open systems” where all information can be viewed by all users. System administrators may be afforded access to all of the data depending upon the system and/or application. However, restrict access when users may not need to have access to all the data.
- When a contract provides for the operation of a system on behalf of FHFA, the Privacy Act requirements must be applied to such a system.
- The IT Security C&A process requires a system security plan that identifies the technical controls associated with identification and authentication of users. Certain laws and regulations require certain monitoring for authorized reasons by authorized employees. What is in place to ensure that only those authorized can monitor use of the system? For example, business rules, internal instructions, posting Privacy Warning Notices address access controls and violations for unauthorized monitoring and access. It is the responsibility of managers of systems to ensure no unauthorized monitoring is occurring.
- The IT Security Plan describes the practice of applying logical access controls. Logical access controls are system-based means by which the ability is explicitly enabled or restricted. It is the responsibility of managers of systems to ensure no unauthorized access is occurring.
- The IT Security Plan describes the practice of audit trails. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data. The C&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication.
- According to OMB Circulars A-123 and A-130, every system/application/process that uses data must have some sort of control to prevent the misuse of the data by those having access to the data. For instance, in computerized systems the Security Information Record

(SIR) is part of the Core Storage Terminal Table. The SIR is the automated tool that identifies and authenticates an individual for the system and is transparent to the user. Describe these in response to this question.

- Are there privacy and security awareness controls such as training materials for personnel? All employees, including contractors, have requirements for protecting information in Privacy Act systems
- Describe the controls in place to protect the information.

SUMMARY INFORMATION

Date submitted for review:

Name of System: Personal Identity Verification Identity Management System (HSPD-12)

System Owner(s):

Name	E-mail	Phone #
Tom Davy	Thomas.Davy@FHFA.gov	202-577-9925

Overview

The overview section provides an overview of the system and addresses the following elements:

- The system name and the division/office that owns the system;
- The purpose of the program, system, or technology and how it relates to the agency's mission; and
- A general description of the information in the system.

System Overview
<p>Homeland Security Presidential Direct 12 (HSPD-12) calls for a mandatory, government-wide standard for secure and reliable forms of ID issued by the federal government to its employees and employees of federal contractors for access to federally-controlled facilities and networks. Based upon this directive, the National Institute for Standards and Technology (NIST) developed Federal Information Processing Standards Publication (FIPS Pub) 201 including a description of the minimum requirements for the Federal personal identification verification (PIV) system.</p> <p>FIPS 201 requires that the PIV cards contain a microchip that contains biometric data to ensure that the cardholder is the authorized user of the card. That biometric data is stored in a microchip on the PIV card itself. The PIV cards also have a color photograph on the face of the card to allow security personnel at physical access entrances to verify that the cardholder is the authorized user of the card. The card is designed to allow both physical and logical access. FHFA is issuing laptop computers that require the PIV and its Personal Identification Number (PIN) to log on to them.</p> <p>The purpose of FHFA's HSPD-12 program is to ensure the safety and security of FHFA facilities, systems, and information; occupants and users; to verify that all persons entering FHFA facilities are authorized to do so; to track and control PIV cards issued to persons entering and exiting FHFA facilities; and to facilitate access to FHFA information technology resources (i.e., computers).</p>

Section 1.0 Characterization of the Information

The following questions define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed. The questions address all information collected, with more emphasis provided on the collection of personally identifiable information (PII), such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information is collected, used, disseminated, or maintained in the system?	Name, date of birth, photograph, grade level, status (employee or contractor), office within FHFA, fingerprints, and FHFA e-mail address. The type of investigation – but not the result and the status of the investigation - i.e. “scheduled, in-progress, or completed” is required information.
1.2	What are the sources of the information in the system?	The FHFA Personnel Security Officer provides to the Continuity Program Manager (CPM): employee’s date of birth, grade level, status (employee or contractor) and investigation type, e.g. BI, SSBI, and status. Some of this information is provided to FHFA by the employee during the hiring process. The employee’s name comes from HR when then they are hired and their e-mail address comes from FHFA IT systems.
1.3	Why is the information being collected, used, disseminated, or maintained?	The information is collected in order to verify the identity of the individual carrying the card. Providing multiple biometrics ensures that the PIV cardholder is the authorized user. The PIV card allows physical access to secure FHFA locations, and to provide the ability to track people who enter and exit secured FHFA facilities. Additionally, PIV cards have the ability to allow logical access to computers.

**FHFA PIA FOR Personal Identity Verification
Identity Management System (HSPD-12)**

#	Question	Response
1.4	How is the information collected?	<p>During the hiring process, the FHFA personnel security office mails a form that the prospective employee fills out. The prospective employee fills out the form and returns it via prepaid self-addressed envelope to FHFA. This form includes the prospective employee's name and date of birth.</p> <p>Upon being hired, the prospective employee reports to the FHFA office where they have their picture taken. That picture is printed on the PIV card. At this time, the employee also creates a digital fingerprint which is part of the batch of information contained on the PIV card.</p>
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	Minimal risk is associated with this data collection. The fingerprints are digitized and turned into an equation and are not readable by the human eye. The DOB and investigation type pose slight risk to individual privacy.

Section 2.0 Uses of the Information

The following questions clearly delineate the use of information and the accuracy of the data being used.

#	Question	Response
2.1	Describe the uses of information.	The primary use of the information is to grant physical access to FHFA buildings and to grant logical access to FHFA computer systems that have been configured to require the PIV/PIN. The PIV cards serve as credentials to ensure that authorized users are allowed access into the buildings. The photograph on the PIV card allows FHFA employees or building security to verify the holder of the card is the authorized user of that PIV card.

#	Question	Response
2.2	Describe any types of controls or safeguards in place to ensure that information is only used in the manner for which it was collected.	<p>FHFA PIV cards expire five years after the date of issue. FHFA maintains an active roster of all PIV cards that have been issued, all cards that have been revoked, and all employees who currently have a temporary card (either because they are waiting for a permanent PIV card or because they are on detail assignment to FHFA). This roster includes date of issue and date of expiration.</p> <p>Additionally, all of the PII embedded on the computer chip on the PIV card, except their name, can only be accessed when the card holder enters the card into a PIV reader and enters their unique PIN.</p> <p>FHFA employees and authorized contractors or subcontractors may access the data only when it is part of their role. All persons with roles in the PIV process undergo training to ensure the protection of personally identifiable information.</p> <p>An audit trail is maintained and updated so that errors in the system may be remedied and any unauthorized access points may be addressed.</p>

Section 3.0 Retention

The following questions outline how long information will be retained after the initial collection.

#	Question	Response
3.1	How long is information retained?	<p>Records relating to persons' access covered by this system are retained in accordance with General Records Schedule 18 Security and Protective Services Records approved by the National Archives and Records Administration. The records are disposed in accordance with our disposal policies.</p> <p>Unless retained for specific, ongoing security</p>

**FHFA PIA FOR Personal Identity Verification
Identity Management System (HSPD-12)**

#	Question	Response
		<p>investigations, records of access are maintained for 2 years and then destroyed. In accordance with HSPD-12, FHFA deactivates PIV cards within one working day of cardholder separation, loss of card, or expiration. PIV cards expire five years after the date of issuance.</p> <p>The information on PIV cards is maintained in accordance with General Records Schedule 11 Space and Maintenance Records. PIV cards are destroyed by cross-cut shredding no later than 90 days after deactivation.</p>
3.2	<p>Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?</p>	<p>Records relating to persons' access covered by this system are retained in accordance with General Records Schedule 18 Security and Protective Services Records approved by the National Archives and Records Administration. The records are disposed in accordance with our disposal policies</p>
3.3	<p>Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.</p>	<p>Risks: Long-term data resides on the FHFA and ORC servers.</p> <ol style="list-style-type: none"> 1. Something happens to the storage media, e.g. information is destroyed. 2. Theft from the FHFA server or from the ORC server <p>Mitigation:</p> <ol style="list-style-type: none"> 1. ORC backs the data up offsite on a weekly basis. FHFA OTIM and others audit ORC for backup and other FISMA compliance items. FHFA backs up it data offsite also and also performs routine FISMA compliance audits. 2.1. Individuals with access to the PII have had security investigations. 2.2. FHFA and ORC personnel with access to the PII are informed of sanctions for improper use of computer systems and PII; sanctions include internal discipline up to firing and potential criminal penalties.

Section 4.0 Notice, Access, Redress and Correction

The following questions are directed at notice to the individual, the individual's right to consent to uses of the information, the individual's right to decline to provide information, and an individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	Has a System of Record Notice (SORN) been created?	Yes. See Federal Register Vol. 71 No. 200. FHFA is in the process of adopting GSA's government wide SORN (GSA/GOVT-7).
4.2	Was notice provided to the individual prior to collection of information?	Yes.
4.3	Do individuals have the opportunity and/or right to decline to provide information?	No. Because HSPD-12 mandates that all Federal employees have a PIV card, employees may not decline to provide this information.
4.4	What are the procedures that allow individuals to gain access to their information?	An employee may request a record with their PII from the FHFA Chief Privacy Officer in accordance with the procedures set forth in 12 CFR part 1204.
4.5	What are the procedures for correcting inaccurate or erroneous information?	<p>Within a short time of starting beginning work at FHFA, the Security Manager will invite the employee to look at the documents that were used to generate the PIV request form to make sure all the information contained on those forms is correct. The individual is given the opportunity to change any incorrect information.</p> <p>If the employee's PII changes (i.e. a name change) they may contact the Continuity Program Manager, who will send the updated information to ORC. The employee will be issued a new PIV card with the updated information. The old PIV card must be returned to the Continuity Program Manager, who will destroy the old PIV card.</p>

Section 5.0 Sharing and Disclosure

The following questions define the content, scope, and authority for information sharing.

#	Question	Response
5.1	With which internal organization(s) is the information shared, what information is shared and for what purpose?	<p>End-users do not have access to the application data; ergo the application data is not shared.</p> <p>There is an administrative (non-application) spread sheet with name, e-mail address, DOB, status, i.e. if they are an employee or contractor, and if they are a Foreign National, Emergency Responder, and/or Law Enforcement official. This administrative spreadsheet is maintained on the S://Continuity drive, which only the Continuity personnel have access to. This spread sheet is e-mailed to ORC as an encrypted/password protected attachment.</p> <p>This spreadsheet is required to transmit the required employee/contractor information in order for ORC to make a PIV card and as it is signed by the HSPD-12 authorizer (CPM), it serves as FHFA authorization for ORC to make a PIV card for the named individuals.</p>
5.2	With which external organization(s) is the information shared, what information is shared, and for what purpose? External organization(s) include Federal, state and local government, and the private sector.	<p>The information is shared with Operational Resource Consultants, Inc. (ORC). ORC is a private contractor, certified by GSA to make PIV cards and store and safeguard PII, that creates the actual cards, takes the digital fingerprint algorithm (but not an actual finger print) and programs the PII into the chip embedded in the PIV card. All of this is done under the supervision of the Continuity Program Manager.</p> <p>FHFA provides a roster of FHFA personnel to OTS. This roster only contains the name of current FHFA employees and contractors. While PIV cards that are enrolled with OTS can be read by the OTS screener, there is no information accessible off of the PIV chip that is not also readable off the physical card itself, i.e. photo, name, agency affiliation, and special</p>

#	Question	Response
		<p>status (i.e. emergency responder), if any.</p> <p>In order for another federal agency to access information from the PIV chip that is not on the physical PIV itself, the owner of the PIV must type in their PIN into a PIV reader.</p> <p>When people “badge in” with their PIV cards, the system badged into maintains their name and photo for a period of time (defined by the system and the number of people badging in, i.e. the more people badge in, the shorter time the information is retained as there is a limit on system memory to maintain this information.) Even if this information was kept forever, it would not be any different than signing a visitor log; the only additional information that might be kept is the photo.</p>
5.3	<p>Is the sharing of PII outside the agency compatible with the original information collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe.</p> <p>If not, please describe under what legal authority the program or system is allowed to share the PII outside of the agency.</p>	<p>Yes. The sharing of PII is compatible with the original SORN. FHFA shares PII with ORC for the purpose of creating the PIV cards, which is essential to carrying out the objectives of HSPD-12. Other agencies can only access information not on the physical PIV card if the card owner types in their personal identification number (PIN).</p> <p>In order for another federal agency to access information from the PIV chip that is not on the physical PIV itself, the owner of the PIV must type in their PIN into a PIV reader.</p> <p>When people “badge in” with their PIV cards, the system badged into maintains their name and photo for a short period of time (defined by the system and the number of people badging in, i.e. the more people badge in, the shorter time the information is retained as there is a limit on system memory to maintain this information. Even if this information was kept forever, it would not be any different to signing</p>

#	Question	Response
		a visitor log as the only additional information that might be kept is the photo.
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	<p>When issuing PIV cards, ORC comes to a FHFA facility and works under the supervision of the Continuity Program Manager.</p> <p>When transmitting PII from FHFA to ORC, the FHFA spread sheet with the PII is e-mailed to ORC as an encrypted/password protected attachment.</p> <p>The primary privacy risk is theft of the administrative spreadsheet by an internal source at FHFA or ORC, i.e. one of the ~ three dozen people between FHFA & ORC with access to the information were to steal it.</p> <p>Mitigation:</p> <ol style="list-style-type: none"> 1. Individuals with access to the PII have had security investigations and may have a clearance. 2. FHFA and ORC personnel with access to this PII are informed of sanctions for improper use of PII; sanctions include internal discipline up to firing and potential criminal penalties. 3. A hacker could steal the PII. Both, FHFA and ORC have multiple safeguards to avoid this from happening, including robust physical and logical security on its systems.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	What procedures are in place to determine which users may access the system and are these procedures documented?	Within FHFA, only employees whose role requires them to have access to the PII in order to administer the HSPD-12 system are allowed access to that information. They must undergo privacy training as part of their role. Outside of this PIA and the SORN, these procedures are not documented.

**FHFA PIA FOR Personal Identity Verification
Identity Management System (HSPD-12)**


#	Question	Response
6.2	Will contractors have access to the system? If yes, how will contractors gain access to the system? How will the agency control their access and use of information?	<p>Yes. ORC is an outside contractor that comes on-site to take digital/biometric fingerprints – that are not recorded on paper or similar media, take the photograph, upload the information onto the chip embedded on the PIV card, and issue the PIV card to FHFA employees.</p> <p>FHFA controls their access and use of the information via contractual relationships that require ORC not to divulge, sell, or in any way distribute the information to another party. Additionally, ORC comes on-site to FHFA facilities and works under the supervision of the Continuity Program Manager.</p> <p>According to the terms of service with ORC, only ORC employees fulfilling authorized roles (e.g., Registrar, Issuer, etc.) may access data pertaining to FHFA credential issuance.</p>
6.3	Describe what privacy training is provided to users either generally or specifically relevant to the program or system?	All FHFA employees are required to participate in annual Information System Security Awareness and Privacy Training
6.4	What technical safeguards are in place to protect the data?	<p>ORC's technical safeguards (including information relating to FHFA information) falls under FISMA controls for technical safeguards at the Moderate level.</p> <p>Within FHFA, the information is contained on secured FHFA servers. Back-up tapes are stored offsite. Only employees whose role requires them access to PII are allowed access to the HSPD-12 system. Access is granted by the Continuity Program Manager, and is not granted on an ad-hoc basis.</p>
6.5	What auditing measures are in place to protect the data?	<p>FHFA OTIM recently completed a review of the HSPD-12 system in October of 2010, and found that that there were no problems with the system. They will perform this review again in Spring 2011</p> <p>ORC's systems (including those pertaining to FHFA) fall under FISMA controls for</p>

**FHFA PIA FOR Personal Identity Verification
Identity Management System (HSPD-12)**

#	Question	Response
		Auditing. ORC systems are audited at least annually by an independent third party auditor and the results of the audit are provided to the GSA OSAISO. In the past, on-site reviews of ORC systems have been conducted by FHFA staff.
6.6	Has a Certification & Accreditation been completed for the system or systems supporting the program?	Yes.

Signatures:

Thomas D. Davy III
System Owner (Printed Name)


System Owner (Signature)

21 April
Date

John L. Connor
System Developer (Printed Name)


System Developer (Signature)


2 May 2011
Date

Ralph Mosios
Chief Information Security Officer
(Printed Name)


Chief Information Security Officer
(Signature)


17 May 2011
Date

R. Kevin Winkler
Chief Information Officer
(Printed Name)


Chief Information Officer
(Signature)

5/20/2011
Date

David A. Lee
Chief Privacy Officer
(Printed Name)


Chief Privacy Officer
(Signature)

5/24/2011
Date