Privacy Impact Assessment Template

FHFA INFRASTRUCTURE GENERAL SUPPORT SYSTEM (GSS)

March 15, 2023
Date

Tasha L. Cooper
Senior Agency Official for Privacy
(202) 649-3091
tasha.cooper@fhfa.gov

Guidance for Completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how Personally Identifiable Information (PII) is collected, stored, maintained, and shared. A PIA must be completed when FHFA: 1) develops or procures an Information Technology (IT) system or project that collects, maintains, or disseminates PII that can be used to identify a specific individual; or 2) initiates a new electronic collection of PII for 10 or more members of the public, which includes any information in an identifiable form permitting the physical or online contacting of a specific individual.

System Owners are primarily responsible for completing the PIA with assistance from IT developers, IT security officers, and the Privacy Office.

OVERVIEW SECTION

- Provide a thorough, complete, and clear overview of the System and give the reader the appropriate context to understand the responses. Some questions to consider include:

    - What is the purpose of the System?
    - What will be the primary uses of the System?
    - How will this support the Division's/Office's/Program's mission?

- This section fulfills the E-Government Act's requirement for an introduction to members of the public who may be reading the PIA. PIAs may 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, geographical, or financial information, with no link to a name or other identifier, such as, home address, social security number, account number, home, mobile or facsimile telephone number, or personal e-mail address.

- Examples of sources of the information include information that comes from an individual applying for a loan or mortgage, or other forms that an individual completes. A question to consider:

    - Where does the data originate? (e.g., FHFA, Office of Personnel Management, Regulated Entities, other Financial Institutions, or third parties). 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, or a private organization).

- If the System collects information from 10 or more members of the public, ensure that FHFA has received prior approval from OMB to do so or determine whether OMB's approval is needed to collect the information in accordance with the Paperwork Reduction Act. If you are unsure of this last requirement, contact the Office of General Counsel for assistance.

SECTION 2.0 USES OF THE INFORMATION

- Identify the primary uses of the information and how the information supports FHFA's or the Office's/Division's/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 to a limited number of staff who use the data for their specific program use.

SECTION 3.0 RETENTION

- **The Privacy Act requires an agency to address the retention and disposal of information about individuals. This retention information is published in the Privacy Act System of Record Notice (SORN).**

- The retention periods for data/records that FHFA manages are contained in either the National Archives and Records Administration (NARA) General Records Schedule (GRS) or FHFA's Records Schedule. For the data being created/ maintained in the System, these records schedules are the authoritative sources for this information. For assistance, contact FHFA's Records Management Office.

- 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 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." 5 U.S.C. 552a(e)(1).

- 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 unique identifier (e.g. social security number) it is a Privacy Act System and will need a SORN published in the Federal Register. The System may already have a Privacy Act SORN. If you do not have a published SORN, or are unsure whether one exists, contact FHFA's Privacy Office.

- If a name or other unique 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 still 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.

- Any employee who knowingly and willfully maintains a System 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.

SECTION 5.0 SHARING AND DISCLOSURE

- If you do not know whether or not Systems share data, contact either the business owner of the data, or the IT specialist who knows what interfaces exist 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 GAO, or FHFA's Office of Inspector General. "Other" may also include database administrators or IT Security Officers. Also include organizations listed in the Privacy Act SORN under the "Routine Use" section when a Privacy Act SORN is required. The more comprehensive the list, the better it is.

- You must first review the 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 restrictions on the use and disclosure of information that are set forth in a SORN.

SECTION 6.0 ACCESS AND SECURITY

- Access to data by a user (i.e. employee or contractor personnel) within FHFA is determined on a "need-to-know" basis. This means to authorized employees or contractor personnel who have a need for the information to perform their duties may be granted access to the information. Factors to consider in making this determination include the user's job requirements including supervisory responsibilities.

- The criteria, procedures, controls, and responsibilities regarding access must be documented in order to comply with the intent of the Federal Information Security Management Act of 2002 for standards and guidelines on security and privacy.

- 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 greater access – i.e. to all of the data – depending upon the System and/or application. However, restrict access when users do 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. Contact the Contracting Officer or

Contracting Officer's Representative to determine whether the contract contains the Privacy Act clause and the requirements thereunder.

- The Security Assessment and Authorization (SA&A) process requires a System security plan that identifies the technical controls associated with identification and authentication of users. Certain laws and regulations require monitoring of Systems to ensure that only authorized users can access the System for authorized reasons. In doing so, consider what controls are in place to ensure that only those authorized to monitor the System can in fact monitor use of the System. For example, business rules, internal instructions, and posting Privacy Warning Notices address access controls and violations for unauthorized monitoring. System Owners are responsible for ensuring that 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 to access a System is either explicitly enabled or restricted. System Owners are responsible for ensuring that no unauthorized access is occurring.

- The IT Security Plan describes the practice of audit trails. An audit trail maintains a record of System activity and user activity including invalid logon attempts, access to data and monitoring. The SA&A process requires a System security plan outlining the implementation of the technical controls associated with identification and authentication.

- Every System/application/process that uses data must have controls in place 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.

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

PIA FORM

Overview

Provide an overview of the System and address the following:

- 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 Owner(s)			
Name	**E-mail**	**Division/Office**	**Office or Mobile Phone Number**
Thomas Leach	thomas.leach@fhfa.gov	Office of the Chief Operating Officer (OCOO)/Office of Technology and Information Management (OTIM)	202-649-3640

System Overview: Briefly describe the purpose of the program, System, or technology, and the information in the System, and how it relates to the agency's mission.

The FHFA Infrastructure General Support System (GSS) supports FHFA's mission by providing fault-tolerant network, Voice over Internet Protocol (VOIP) and Internet connectivity, end-user computing equipment, collaboration tools, application systems and services, and perimeter/endpoint security solutions. The GSS encompasses on-premises, cloud technologies, and processes that support and protect FHFA information resources.

GSS components include cloud-based Federal Risk and Authorization Management Program (FedRAMP) providers of Infrastructure-As-A-Service (IAAS), Software-As-A-Service (SAAS), Platform-As-A-Service (PAAS) and Security-As-A-Service (SecAAS) where the Office of Technology of Information Management (OTIM) is the system owner, the service is enterprise wide, and the information types are already or traditionally stored on the FHFA network.

The GSS is extended for mobile users with Apple iPhones and 802.11i Wi-Fi Protected Access (WPA) Points using Advanced Encryption Standards (AES) Encryption at Constitution Center, Freddie Mac and Freddie Mae, and the FHLBank sites. Remote network access to Agency resources is provided through an encrypted, always-on Palo Alto GlobalProtect Virtual Private Network (VPN) connection across public networks and through a Citrix Virtual Desktop Infrastructure (VDI) solution that provides access to local information resources using a web browser from non-FHFA devices.

The information received, stored, and transported using the GSS includes an expansive data set used by FHFA to achieve its various mission and statutory requirements. This information includes examination-related data, regulatory and financial information provided by Government-Sponsored Enterprises (GSEs), commercial market data, data provided by other federal agencies, internal administrative data, analytical data, statistical products data, and other types of data required for meeting operational and mission requirements. This data also includes Personally Identifiable Information ("PII") of employees, contractors, individual holders of mortgages issued by the GSEs, and others. The PII ranges from low sensitivity, such as the type of contact information (e.g., name, email, address, and phone number), to sensitive information, such as Social Security number and financial information.

The GSS PIA covers all these components and types of information that exist on or traverse those systems, and applications forming part of FHFA's infrastructure that are identified in the attached addendum. The addendum to this PIA will be updated as in-scope systems and applications are added to the GSS and each system or application is evaluated to determine if a PIA is required and whether the processing of PII by that system or application aligns with the processing of PII described in this PIA. The addendum will also be updated when any significant changes are made in how PII is managed for an applicable system or application.

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, or technology being developed. The questions address all information collected, with more emphasis provided on the collection of PII,

such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information is being collected, used, disseminated, or maintained in the System?	Regulatory and financial information provided by Government-Sponsored Enterprises (GSEs), commercial market data, data provided by other federal agencies, internal administrative data, analytical data, statistical products data, and other types of data required for meeting operational and mission requirements. This data at times contains PII of employees, contractors, individual mortgage holders held by the GSEs, and others. This could range from PII of low sensitivity such as contact information (e.g., name, business and personal email, personal address, and business and personal phone numbers) to sensitive information such as Social Security numbers and financial information. Information specific to the GSS includes, but is not limited to the following: • Employee or contractor name; • FHFA username; • Business email address; • Duty station location; • Business telephone numbers; • Internet Protocol (IP) address; • Network audit history (login, logout times, internet usage logs); • Password (stored as a hash value); • PIN (stored as a hash value). Information stored on the GSS but specific to systems that are components of the GSS and which are covered under a separate PIA includes but is not limited to: • Individual names, • Addresses (business or personal), • Phone numbers (business or personal), • E-Mail addresses (business or personal), • Social Security number, • Individual financial data, • Demographic information, • Income information, • Employment information, • Information from GSEs collected for supervisory or conservatorship, • Information collected to support market analysis, research, and policy.

1.2	What or who are the sources of the information in the System?	The data specific to the GSS are primarily derived from current and former FHFA network users, including employees, interns, and contractors. Sources are FHFA hardware, software and system components that generate information reflecting activity on the FHFA network. Sources of the data stored on the GSS but specific to systems that are components of the GSS and which are covered under a separate PIA are the GSEs, commercial data providers, individuals who voluntarily provide comment/correspondence, other federal agencies.

#	Question	Response
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The GSS-specific data is collected, used, disseminated, and maintained to enable effective, reliable, and secure operation of the FHFA network in support of FHFA's business mission. The data stored by the GSS but specific to systems that are components of the GSS and which are covered under a separate PIA is used by FHFA business offices to complete mission and statutory requirements such as examination, research, and policy.
1.4	How is the information provided to FHFA?	GSS-specific data is collected via communications with FHFA users as part of the on-boarding processes, including identity verification and fingerprinting as part of background investigation adjudication. Active FHFA network users can generate additional information that is reflective of their network activity includes, but is not limited to, information such as security logs of access to applications, Internet use, VOIP call logs. The GSS also receives and stores data that is

		specific to systems that are components of the GSS and which are covered under a separate PIA. Such data includes information from external entities, for example, the Dept. of Interior (DOI) as part of the Human Resources Information System (HRIS), Office of Personnel Management (OPM) eDelivery system, receiving this information via site-to-site virtual private network (VPN) connections, or Connect:Direct connections. These additional, external sources of information and the privacy risks associated with them are described in PIAs issued by the federal agencies that own the described systems. GSS stored information is provided from the GSEs through Secure File Transfer Protocol (SFTP), GSE data collection portal (NExtranet), and commercial data providers via subscriptions allowing data downloads.
1.5	Given the amount and type of information collected, what are the risks to an individual's privacy that are associated with collection of the data? Explain in detail how the loss, or compromise of the information will/can affect an individual's privacy.	There are risks associated with the loss or compromise of the information collected and maintained that is specific to the GSS. Elements, including name, business location, telephone numbers and account information are not normally publicly available, but do not pose a higher risk of subsequent identity theft or personal harm to the individual if released. If PII is lost, stolen, or compromised, an individual could experience unlawful acts such as identity theft or fraud.
1.6	Are Social Security numbers are being collected or used in the system?	SSNs are not specifically collected and stored by the GSS. Rather, they are collected and stored in specific applications which have separate PIAs, as required
1.7	If SSNs are collected or used in the system, 1) describe in detail the business justification for collecting or using SSNs; 2) the consequences if SSNs are not collected or used, and 3) how the SSNs will be protected while in use, in transit and in storage.	SSNs are not collected and stored specifically by the GSS. The specific applications/systems that rely on GSS for storage have separate PIAs, as required, and privacy risks associated with the collection of SSNs by those systems are addressed in those separate PIAs.

Section 2.0 Uses of the Information

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

#	Question	Response
2.1	How will the information be used and for what purpose?	The GSS specific information collected is required to create and maintain secure network accounts for FHFA employees, contractors and NExtranet users, and to allow these users to utilize FHFA network resources such as email, word processing, instant messaging, VOIP, etc. The GSS stored information that is specific to systems that are components of the GSS and which are covered under a separate PIA is used by FHFA business offices to achieve FHFA's strategic mission, goals, and statutory requirements including examinations, supervision, and policy.
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.	Access to the GSS-specific information and separately the GSS-stored information that is specific to systems that are components of the GSS and which are covered under separate PIAs are managed to a principle of least privilege where access is granted to data, resources, and applications as needed. Access is granted through Active Directory security groups based on group membership to only those resources for which the user has a legitimate business need.

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 the information retained?	FHFA manages permanent and temporary electronic records in accordance with FHFA's *Comprehensive Records Schedule* (CRS).
3.2	Has a retention schedule been approved by FHFA's Records Management Office and NARA? If yes, provide the corresponding GRS or FHFA specific Records Schedule number.	Yes. Records are managed in accordance with the NARA-approved FHFA's CRS as assigned to each system, and the applicable CRS for each system is identified in addendum attached to this PIA.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	Risk: Disposition (reviews, approvals, and deletions) may not be carried out as required in the normal course of business due to external circumstances such as litigation holds. Mitigation: Instituted annual reviews of disabled accounts to update status as necessary.

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? If so, provide the SORN name and number. If one has not, and one is required, provide the name of the SORN and the expected publication date in the Federal Register.	Due to the variety of types, sources, and uses of the data specifically collected by GSS, multiple of the SORNs available at: https://www.fhfa.gov/AboutUs/FOIAPrivacy/Pages/Privacy.aspx may apply to the GSS data collections, including but not limited to FHFA-5, Photographic, Video, Voice, and Similar Files, FHFA-7, Mail, Contact, Telephone, and Other Lists, FHFA-19, Computer Systems Activity and Access Records System, and FHFA-20, Telecommunications System. The data generally collected by the GSS for the systems within the GSS authorization boundary that specifically use that data and are covered by a separate PIA may rely on other SORNs, as detailed in those individual PIAs.
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice	N/A. Information is obtained from the FHFA Active Directory and from the wireless and telecommunications carriers associated with the

	was provided?	agency managed mobile, voice, and network devices and is not directly collected from individuals.
4.3	Do individuals have the opportunity and/or right to decline to provide information? What are the consequences if an individual declines to provide the information?	N/A. Information is obtained from the FHFA Active Directory and from the wireless carriers associated with the agency managed mobile devices. Information is not directly collected from individuals.
4.4	What are the procedures that allow individuals to gain access to their information?	Individuals may submit a Privacy Act request to FHFA's Privacy Act Officer pursuant to 12 CFR §1204.3(b)
4.5	What are the procedures for correcting inaccurate or erroneous information?	Individuals may submit a request to amend or correct records to FHFA's Privacy Act Officer pursuant to 12 CFR § 1204.3(d)

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?	FHFA's Office of Technology and Information Management (OTIM) manages the GSS-specific information. Access to the GSS-specific data or the data that is generally collected by the GSS for the systems that are components of the GSS, specifically use that data, and are covered under a separate PIA, is limited to those individuals with an operational need, such as IT administrators and engineers. In addition, access is provided to external entities such as Agency contracted law firms and federal law enforcement agencies as required.
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.	FHFA utilizes Federal Shared Service providers to provide government-wide services such as background investigations, HSPD-12 management, payroll, travel services, financial management, etc. The privacy risks associated with those systems are addressed in the PIAs conducted by the federal agencies who own them and can be found at https://www.fhfa.gov/AboutUs/FOIAPrivacy/Pages/Privacy.aspx. Sharing with authorized contractors is achieved through non-disclosure agreements with authorized contractors as a requirement for the grant of access

		via a secure portal and multi-factor authentication. The information is retained within the control of the GSS. For data that is generally collected by the GSS for the systems that are components of the GSS, that specifically use that data, all privacy risks associated with that data, including risks related to external sharing of PII, are addressed under separate PIAs for each such system.
5.3	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? Describe such use. If not, describe the legal authority that permits PII to be shared outside of FHFA.	Yes, the external sharing of this information is compatible with the original purpose for this information collection and is further authorized by 12 U.S.C. 4511(b)(2), 12 U.S.C. 4513(a)(2)(B), and 44 U.S.C. 3101. Please also see the authorities cited in the SORNs applicable to the specific collections and use of data by the GSS, which may include FHFA-5, Photographic, Video, Voice, and Similar Files, FHFA-7, Mail, Contact, Telephone, and Other Lists, FHFA-19, Computer Systems Activity and Access Records System, FHFA-20, Telecommunications System, and potentially other SORNs made public available at https://www.fhfa.gov/AboutUs/FOIAPrivacy/Pages/Privacy.aspx. For data that is generally collected by the GSS for the systems that are components of the GSS and that specifically use that data, please see the SORN(s) identified in the separate PIAs for those systems.
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	For GSS PII that is shared with federal shared service providers as a part of a federal shared service, such sharing is subject to the Federal Information Security Modernization Act of 2014 (FISMA) and the Privacy Act. The risks to the individual include both the loss of control of PII and the release of potentially sensitive data. These risks are mitigated by limiting any external sharing to that which is required and providing access to data through a secure access only portal, or by validating an external organizations security controls meet FISMA requirements before allowing transfer of PII data.

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? Are these procedures documented in writing?	The GSS System Security and Privacy Plan (SSPP) describes how the GSS implements all applicable NIST SP 800-53 Revision 5 controls including those related to Account Management. All users with access to FHFA's GSS are required to consent to the FHFA Rules of Behavior upon initial logon, and annually thereafter.
6.2	Will non-FHFA personnel (e.g. contractor personnel, regulated entity personnel) have access to the System and information contained therein? If yes, how will they gain access to the System? How will the agency control their access and use of information? Are there procedures documented in writing?	OTIM engineers and external federal organizations with access to GSS specific and stored information may consist of FHFA employees and contractor personnel. All users undergo personnel screening prior to gaining access to FHFA's network and are required to complete security and privacy awareness training within two weeks of their start date. Active Directory (AD) groups are used to apply permissions to all users based on the concept of least privilege. The Account Management Guidelines describes the procedures for using AD groups to restrict access to information based on a user's business need.
6.3	Describe the type and frequency of training that is provided to users either generally or specifically that is relevant to the program or System?	FHFA requires IT Security and Privacy Awareness training as well as Records Management training within two weeks of their start date and annually thereafter. Additionally, specialized security training is required annually for users with elevated privileges.
6.4	Describe the technical/administrative safeguards in place to protect the data?	The GSS SSPP describes the controls in place to protect the confidentiality, integrity and availability of data stored, processed, and transmitted by the GSS. This data includes, but is not limited to: - Multi-factor authentication for all privileged and non-privileged users; - Hard disk encryption on all FHFA workstations; - Layer-7 Intrusion Prevention System (IPS) and web-proxy; - Secure email filtering; - Einstein 3A protections; - Always-on encrypted Virtual Private Network (VPN); - Centralized audit logging and incident detection. The GSS undergoes annual control testing to verify the sufficiency of technical and administrative safeguards.
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	FHFA operates a centralized security information and event management (SIEM) solution that captures events from FHFA devices and information systems and generates alerts for FHFA cybersecurity personnel to investigate based on

		established criteria.
6.6	Has a SA&A been completed for the System or Systems supporting the program? If so, provide the date the last SA&A was completed. If not, and one is required, provided the expected completion date of the SA&A.	The GSS is in the ongoing authorization phase of the Risk Management Framework and undergoes annual security control assessments. The last SA&A was completed on September 26, 2022.
6.7	Has an Authority to Operate (ATO) been issued for this System? If so, what date was it issued, and for how long was it issued? If not, when do you anticipate such ATO being issued?	The most recent ATO Memo for the GSS was signed on September 26, 2022.

Addendum to the Infrastructure General Support System (GSS) PIA

The following systems, applications, and/or databases are expressly included within, and the related privacy risks described by this PIA:

1. Kiteworks – Records are subject to CRS Item 5.4 – OTIM Program Management, which carries a 7-year retention.