Privacy Impact Assessment (PIA) Template

FHFA INFRASTRUCTURE GENERAL SUPPORT SYSTEM
(Name of the Information System or Information Collection)

November 20, 2023
(Date)

System Overview
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 FHFA Infrastructure GSS is comprised of hardware and software solutions deployed on-premises, as well as cloud-based providers of Infrastructure-As-A-Service (IAAS), Software-As-A-Service (SAAS), Platform-As-A-Service (PAAS) and Security-As-A-Service (SecAAS) solutions that support FHFA's computing infrastructure. Included in these providers of cloud-based GSS support services are Amazon Web Services (AWS), which extends FHFA's network through the use of virtual and scalable computing (EC2), storage (EBS, S3), database (RDS, RedShift), web (Beanstalk), and other services, as well as Microsoft Office 365, which provides end user collaboration and communication services through systems and applications that include Microsoft Teams, OneDrive, SharePoint Online and Exchange Online, and mobile device management services through Intune. The FHFA Infrastructure GSS includes mobile devices managed by FHFA and network infrastructure to support office locations at Constitution Center (FHFA's HQ), Freddie Mac, Freddie Mae, and each of the Federal Home Loan Banks. Remote network access to Agency resources is provided through an encrypted, always-on Virtual Private Network (VPN) connection across public networks and through a Virtual Desktop Infrastructure (VDI) solution. The information received, stored, and transported by the FHFA Infrastructure 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 and residential real estate 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, and others. The PII ranges from low sensitivity, such as business contact information (e.g., name, email, address, and phone number), to sensitive information, such as Social Security number and financial information. The FHFA Infrastructure GSS PIA covers all types of information that exist on or traverse the supporting components and systems, which are identified in the attached addendum. The addendum to this PIA will be updated as in-scope systems are added to the GSS, based on 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 System/Collection being procured or 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 types (e.g., name, date of birth, business contact information, demographic) is being collected, used, disseminated, or maintained in the System/Collection?	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); and • 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; and • Information collected to support market analysis, research, and policy.

1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	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.
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 or otherwise obtained by 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 and 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), receiving this information via site-to-site virtual private network (VPN) connection. 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	Are Social Security Numbers (SSN) being collected or used in the System? • If yes: 1) Describe in detail the business justification for collecting or using SSNs. 2) The consequences if SSNs are not collected or used. 3) How the SSNs will be protected while in use, in transit and in storage. • If no, state "N/A" in the response section.	SSNs are not specifically collected and stored by the GSS. Rather, they are collected and stored in specific applications that have separate PIAs as required. 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 measures or processes 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 the principle of "least privilege" by which access is granted to data, resources, and applications as needed for official business purposes only. 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 National Archives and Records Administration (NARA)? If yes, provide the corresponding General Record Schedule (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 the addendum attached to this PIA.

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	Is the information in this System/Collection retrieved by an individual's name or personal identifier such as an SSN or other identification? • If no, please put "no" in the Response section. • If yes, the System/Collection will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)). Please provide the SORN(s) name and number or indicate that a SORN is in progress.	Yes. 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	How is notice about the collection of PII provided to individuals prior to the collection for the System/Collection (e.g., direct notice, Privacy Act Statement or public notice, SORN)? • If notice is not provided, explain why not. • If notice is provided, please provide a screenshot or PDF of the notice statement.	N/A. Information is obtained from the FHFA Active Directory and from the wireless and telecommunications carriers associated with the agency managed mobile, voice, and network devices and is not directly collected from individuals.
4.3	Is an individual's response to the request for information voluntary or mandatory?	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 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.
4.5	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).
4.6	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	Is information shared with internal office(s) or division (s)? • If yes, please identify the office(s) or division(s) and describe the information shared and for what purpose. • If no, please state "N/A" in the response section.	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	Is information shared with external (outside FHFA) agencies, organization(s), contractors, or other entities? For purposes of this Section, external organization(s) include Federal, state, and local government, and the private sector. • If yes, please identify the information shared, and for what purpose. If documents describe the information shared, please provide a copy. • If no, skip to Section 6.	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.
5.3	Is the sharing of PII outside the agency compatible with the stated purpose of the original information collection? • If yes, identify any applicable routine uses in the SORN listed in question 4.1 • If no, 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.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	Will FHFA Office of Inspector General (OIG) or non-FHFA personnel (e.g., contractor personnel, regulated entity personnel) have access to the System/Collection and information contained therein? • If yes, how will they gain access to the System? • If no, how will the agency control access to and use of that information? Are there procedures or criteria documented in writing? If so, please describe.	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. 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	Are there any conflicts of interest with respect to the System/Collection or information? If so, describe how those conflicts are addressed.	No.
6.3	Describe the type and frequency of training that is provided to users either generally or specifically that is relevant to the System/Collection.	All FHFA employees are required to undergo Security, Privacy, and Records and Information Management (RIM) training at new employee onboarding training and annually thereafter. In addition, all FHFA users with elevated privileges receive specialized security training, and role-based privacy awareness training for those individuals whose work duties and responsibilities involve the collection, use, storage, access, or maintenance of PII.

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); and • Centralized audit logging and incident detection. The GSS undergoes annual control testing to verify the sufficiency of technical and administrative safeguards.

7.0 Risk

The following questions describe the risk to the information within the system or collection.

#	Question	Response
7.1	Given the amount and type of information collected, what are the risks to an individual's privacy associated with collection of the data? Explain in detail how the loss or compromise of the information will/can affect an individual's privacy and describe how these risks are mitigated.	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.
7.2	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The risks associated with the duration of retention include the disposition (e.g., 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. The responsive mitigation consists of the instituted annual reviews of disabled accounts to update status as necessary so that disposition is not delayed any longer than necessary by, e.g., a litigation hold.

7.3	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.

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 are described by this PIA:

1. **Kiteworks** – **Purpose**: Kiteworks is a secure file transfer tool that enables users to send and receive encrypted information to/from external partners and share content via secure folders for secure document collaboration. All activity is encrypted and logged, and the Kiteworks platform provides insight of all content movement and user activity whether internal or external. Kiteworks allows application administrators to provision user access easily and quickly to the system to allow secure exchange of data; **Record Retention Requirements**: FHFA CRS Item 5.4 Information Technology and Management Records, 5.4a: Records related to IT program planning, enterprise architecture, network and IT operations, IT capital investment, infrastructure, information and systems security, oversight and compliance, records management, and information governance, annual FISMA reporting, and other reporting requirements. Disposition: TEMPORARY. Cutoff is when the project/activity/transaction is completed or superseded. Records will be destroyed or deleted 7 years after the cutoff (in other words, implementation of a replacement system); and **Applicable SORN(s)**: In addition to every FHFA SORN, EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeals Record, DOL/GOVT-1 Office of Worker's Compensation Programs, DOL/GOVT-2 Jobs Corps Student Records, DOT/ALL-8 Employee Transportation Facilitation, GSA/GOVT-2 Employment Under Commercial Activities Contracts, EPA/GOVT-2 Federal Docket Management System (FDMS), GSA/GOVT-3 Travel Charge Card Program, GSA/GOVT-4 Contracted Travel Services Program, GSA/GOVT-6 GSA SmartPay Purchase Charge Card Program, GSA/GOVT-7 Personal Identity Management Systems (PIV IDMS), GSA/GOVT-8 Excluded Parties List System (EPLS), MSPB/GOVT-1 Appeal and Case Records, OGE/GOVT-1 Executive Branch Public Financial Disclosure Reports and Other Ethics Program Records, OGE/GOVT-2 Confidential Statements of Employment and Financial Interests, OPM/GOVT-1 General Personnel Records, OPM/GOVT-2 Employee Performance File System Records, OPM/GOVT-3 Records of Adverse Actions, OPM/GOVT-5 Recruiting, Examining and Placement Records, OPM/GOVT-6 Personnel Research and Test Validation Records, OPM/GOVT-7 Applicant – Race, Sex, National Origin and Disability Status Records, OPM/GOVT-9 File on Position Classification Appeals, Job Grading Appeals, and Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints, OPM/GOVT-10 Employee Medical System Records, and OSC/GOVT-1 OSC Complaint Litigation and Political Activity Files.
2. **SailPoint IdentityIQ (SailPoint)** – **Purpose**: SailPoint is FHFA's Identity Governance and Administration (IGA) system that is supported by FHFA's Office of Technology and Information Management (OTIM) Identity, Credential, & Access Management (ICAM) Program. SailPoint IdentityIQ supports processes including onboarding of people to FHFA and monthly certifications of contractors to determine their contract status. The system is also used to automate provisioning, modification, and deletion of active directory accounts, group membership, and other Active Directory attributes. In addition, SailPoint integrates with FHFA applications to collect user entitlements and user attributes to form a single master user record. Access reviews can then be conducted off the master user record to certify user access; **Record Retention Requirements:** FHFA CRS Item 5.4 Information Technology and Management Records, 5.4a: Records related to IT program planning, enterprise architecture, network and IT operations, IT capital investment, infrastructure, information and systems security, oversight and compliance, records management, and information governance, annual FISMA reporting, and other reporting requirements. Disposition: TEMPORARY. Cutoff is when the project/activity/transaction is completed or superseded. Records will be destroyed or deleted 7 years after the cutoff (in other words, implementation of a replacement system); and **Applicable SORN(s):** FHFA-19 Computer Systems Activity and Access Records System.
3. **Amazon Web Services East/West (AWS)** – **Purpose:** OTIM utilizes AWS to extend its network and add virtual AWS computing resources to its on-premises hardware and software infrastructure.

AWS is a cloud computing platform that provides a wide range of services, including computing, storage, databases, networking, machine learning, and security services. OTIM uses these services to build, deploy, and manage FHFA applications and websites. AWS is a FedRAMP'ed system; **Record Retention Requirements**: FHFA CRS Item 5.4 Information Technology and Management Records, 5.4a: Records related to IT program planning, enterprise architecture, network and IT operations, IT capital investment, infrastructure, information and systems security, oversight and compliance, records management, and information governance, annual FISMA reporting, and other reporting requirements. Disposition: TEMPORARY. Cutoff is when the project/activity/transaction is completed or superseded. Records will be destroyed or deleted 7 years after the cutoff (in other words, implementation of a replacement system); and **Applicable SORN(s)**: FHFA-19 Computer Systems Activity and Access Records System.

4. **Microsoft Office 365 (M365)** – **Purpose**: M365 is a cloud computing platform that provides a wide range of services, including cloud versions of Exchange Online (EXO), SharePoint Online (SPO), which also includes Access Online, Project Online, and OneDrive for Business, Skype for Business (SFB), Information Protection (IP), Office Online (WAC), Office 365 Suite User Experience (SUE), Microsoft Teams (MS Teams), Bing, Customer Insights and Analysis (CIA), and Delve; **Record Retention Requirements**: FHFA CRS Item 5.4 Information Technology and Management Records, 5.4a: Records related to IT program planning, enterprise architecture, network and IT operations, IT capital investment, infrastructure, information and systems security, oversight and compliance, records management, and information governance, annual FISMA reporting, and other reporting requirements. Disposition: TEMPORARY. Cutoff is when the project/activity/transaction is completed or superseded. Records will be destroyed or deleted 7 years after the cutoff (in other words, implementation of a replacement system); and **Applicable SORN(s)**: FHFA-19 Computer Systems Activity and Access Records System.
5. **Nextranet** – **Purpose**: The Nextranet serves as a multifactor authentication enabled framework for FHFA to securely allow trusted external users from the Government Sponsored Entities (i.e., Fannie Mae, Freddie Mac, Federal Home Loan Banks, Office of Finance) and other partners to access Extranet applications via the Internet. The Extranet applications fall outside of the Nextranet boundary, as does DUO, the multifactor authentication solution; **Record Retention Requirements**: FHFA CRS Item 5.4 Information Technology and Management Records, 5.4a: Records related to IT program planning, enterprise architecture, network and IT operations, IT capital investment, infrastructure, information and systems security, oversight and compliance, records management, and information governance, annual FISMA reporting, and other reporting requirements. Disposition: TEMPORARY. Cutoff is when the project/activity/transaction is completed or superseded. Records will be destroyed or deleted 7 years after the cutoff (in other words, implementation of a replacement system); and **Applicable SORN(s)**: FHFA-19 Computer Systems Activity and Access Records System.
6. **Mobile (Secure Proxy Service)** – **Purpose**: The Secure Proxy Service (i.e. FHFA Mobile) serves as a framework to allow remote FHFA mobile devices (iPhones, iPads, etc.) secure connectivity to internal FHFA resources while using cellular or non-FHFA Wi-Fi connections; **Record Retention Requirements**: FHFA CRS Item 5.4 Information Technology and Management Records, 5.4a: Records related to IT program planning, enterprise architecture, network and IT operations, IT capital investment, infrastructure, information and systems security, oversight and compliance, records management, and information governance, annual FISMA reporting, and other reporting requirements. Disposition: TEMPORARY. Cutoff is when the project/activity/transaction is completed or superseded. Records will be destroyed or deleted 7 years after the cutoff (in other words, implementation of a replacement system); and **Applicable SORN(s)**: FHFA-7 Mail, Contact, Telephone, and Other Lists and FHFA-19 Computer Systems Activity and Access Records System.
7. **ServiceNow** – **Purpose**: ServiceNow is a cloud platform designed to improve operational efficiencies by streamlining and automating routine work tasks. It can also improve decision-making by providing decision-makers with a holistic view of operations. FHFA's initial focus is on IT issue management, facilities' work order management, space planning, reservation management, and hardware asset management. **Record Retention Requirements**: FHFA CRS Item 5.4 Information

Technology and Management Records, 5.4a: Records related to IT program planning, enterprise architecture, network and IT operations, IT capital investment, infrastructure, information and systems security, oversight and compliance, records management, and information governance, annual FISMA reporting, and other reporting requirements. Disposition: TEMPORARY. Cutoff is when the project/activity/transaction is completed or superseded. Records will be destroyed or deleted 7 years after the cutoff (in other words, implementation of a replacement system); **Applicable SORN(s)**: FHFA-7 Mail, Contact, Telephone, and Other Lists and FHFA-20 Telecommunications Systems.

8. **Splunk** – **Purpose**: Splunk is a software platform widely used for monitoring, searching, analyzing, and visualizing the machine-generated data in real time. It performs capturing, indexing, and correlating the real time data in a searchable container and produces graphs, alerts, dashboards, and visualizations. Splunk provides easy to access data over the whole organization for easy diagnostics and solutions to various business problems; **Record Retention Requirements**: FHFA CRS Item 5.4 Information Technology and Management Records, 5.4a: Records related to IT program planning, enterprise architecture, network and IT operations, IT capital investment, infrastructure, information and systems security, oversight and compliance, records management, and information governance, annual FISMA reporting, and other reporting requirements. Disposition: TEMPORARY. Cutoff is when the project/activity/transaction is completed or superseded. Records will be destroyed or deleted 7 years after the cutoff (in other words, implementation of a replacement system); and **Applicable SORN(s)**: FHFA-19 Computer Systems Activity and Access Records System.
9. **Zix Hosted** – **Purpose**: Zixmail is used to send encrypted email outside of FHFA. Emails sent by FHFA users to external recipients are routed through FHFA's instance of Zix where policies are applied to automatically encrypt the message in transit or place the message in the Zix Secure Portal. External users can retrieve the message, If an external, non-FHFA user is registered with Zix or uses an email server configured to use Transport Layer Security (TLS), the secure e-mail will automatically arrive in an external user's regular e-mail inbox and no further action will be required to access the email or attachments thereto. If the external user is not registered with Zix, that user must create a login for and then log into the Zix Portal to view the message and any attachments and the message never reaches the external user's inbox; **Record Retention Requirements**: FHFA CRS Item 5.4 Information Technology and Management Records, 5.4a: Records related to IT program planning, enterprise architecture, network and IT operations, IT capital investment, infrastructure, information and systems security, oversight and compliance, records management, and information governance, annual FISMA reporting, and other reporting requirements. Disposition: TEMPORARY. Cutoff is when the project/activity/transaction is completed or superseded. Records will be destroyed or deleted 7 years after the cutoff (in other words, implementation of a replacement system); and **Applicable SORN(s)**: FHFA-7 Mail, Contacts, Telephone, and Other Lists.