

U.S. Department of Housing and Urban Development



Government National Mortgage Association (Ginnie Mae)



General Support System (GSS) Privacy Impact Assessment (PIA)

March 1, 2016
Version 1.0

Prepared by:
Bank of New York Mellon



Document Endorsement

I have carefully assessed the Privacy Impact Assessment (PIA) for Ginnie Mae General Support System (GNMA GSS). This document has been completed in accordance with the requirement set forth by the E-Government Act of 2002 and OMB Memorandum 03-22 which requires that "Privacy Impact Assessments" (PIAs) be conducted for all new and/ or significantly altered IT Systems, and Information Collection Requests.

ENDORSEMENT SECTION

Please check the appropriate statement.

- The document is accepted.**
 The document is accepted pending the changes noted.
 The document is not accepted.

Based on our authority and judgment, the data captured in this document is current and accurate.

Dan Boling



SYSTEM OWNER

Office Enterprise Data & Technology Solutions
Ginnie Mae

3/4/16
Date

John Daugherty

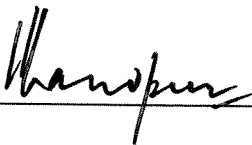


INFORMATION OWNER

Office of Securities Operations
Ginnie Mae

3/14/16
Date

Chitranjan Khandpur



PRIVACY OFFICER

Office of Security & Compliance

3/14/16
Date

TABLE OF CONTENTS

TABLE OF CONTENTS	3
SECTION 1: BACKGROUND.....	4
Importance of Privacy Protection – Legislative Mandates:.....	4
What is the Privacy Impact Assessment (PIA) Process?	5
Who Completes the PIA?.....	5
When is a Privacy Impact Assessment (PIA) Required?.....	5
What are the Privacy Act Requirements?	6
Why is the PIA Summary Made Publicly Available?	6
SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT.....	7
Question 1:.....	7
Question 2:.....	9
Question 3:.....	10
Question 4:.....	13
Question 5:.....	13
Question 6:.....	14
Question 7:.....	14
Question 8:.....	15
Question 9:.....	15
SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER.....	16

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:**

**GINNIE MAE ENTERPRISE PORTAL (GMEP)
Unique Identifier: NON-WCF-GMEP-GMNA**

March 31, 2014

SECTION 1: BACKGROUND

Importance of Privacy Protection – Legislative Mandates:

HUD is responsible for ensuring the privacy and confidentiality of the information it collects on members of the public, beneficiaries of HUD programs, business partners, and its own employees. These people have a right to expect that HUD will collect, maintain, use, and disseminate identifiable personal information only as authorized by law and as necessary to carry out agency responsibilities.

The information HUD collects is protected by the following legislation and regulations:

- Privacy Act of 1974, as amended affords individuals the right to privacy in records that are maintained and used by Federal agencies. (See <http://www.usdoj.gov/foia/privstat.htm>; see also HUD Handbook 1325.1 at www.hudclips.org);
- Computer Matching and Privacy Protection Act of 1988 is an amendment to the Privacy Act that specifies the conditions under which private information may (or may not) be shared among government agencies. (See <http://www.usdoj.gov/foia/privstat.htm>);
- Freedom of Information Act of 1966, as amended (http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm) provides for the disclosure of information maintained by Federal agencies to the public, while allowing limited protections for privacy. See also HUD's Freedom of Information Act Handbook (HUD Handbook 1327.1 at www.hudclips.org);
- E-Government Act of 2002 requires Federal agencies to conduct Privacy Impact Assessments (PIAs) on its electronic systems. (See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf; see also the summary of the E-Government Act at http://www.whitehouse.gov/omb/egov/pres_state2.htm);
- Federal Information Security Management Act of 2002 (which superseded the Computer Security Act of 1987) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, etc. See also the codified version of Information Security regulations at Title 44 U.S. Code chapter 35 subchapter II (<http://uscode.house.gov/search/criteria.php>); and

- OMB Circular A-130, Management of Federal Information Resources, Appendix I (http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) defines Federal Agency responsibilities for maintaining records about individuals.

Access to personally identifiable information will be restricted to those staff that has a need to access the data to carry out their duties; and they will be held accountable for ensuring privacy and confidentiality of the data.

What is the Privacy Impact Assessment (PIA) Process?

The Privacy Impact Assessment (PIA) is a process that evaluates issues related to the privacy of personally identifiable information in electronic systems. See background on PIAs and the 7 questions that need to be answered, at: <http://www.hud.gov/offices/cio/privacy/pia/pia.cfm>. Personally identifiable information is defined as information that actually identifies an individual, e.g., name, address, social security number (SSN), or identifying number or code; or other personal/ sensitive information such as race, marital status, financial information, home telephone number, personal e-mail address, etc. Of particular concern is the combination of multiple identifying elements. For example, knowing name + SSN + birth date + financial information would pose more risk to privacy than just name + SSN alone.

The PIA:

- Identifies the type of personally identifiable information in the system (including any ability to combine multiple identifying elements on an individual);
- Identifies who has access to that information (whether full access or limited access rights); and
- Describes the administrative controls that ensure that only information that is necessary and relevant to HUD's mission is included.

Who Completes the PIA?

Both the program area System Owner and IT Project Leader work together to complete the PIA. The System Owner describes what personal data types are collected, how the data is used, and who has access to the personal data. The IT Project Leader describes whether technical implementation of the System Owner's requirements presents any risks to privacy, and what controls are in place to restrict access of personally identifiable information.

When is a Privacy Impact Assessment (PIA) Required?

- 1. New Systems:** Any new system that will contain personal information on members of the public requires a PIA, per OMB requirements (this covers both major and non-major systems).
- 2. Existing Systems:** Where there are significant modifications involving personal information on members of the public, or where significant changes been made to the system that may create a new privacy risk, a PIA is required.

3. Information Collection Requests, per the Paperwork Reduction Act (PRA):

Agencies must obtain OMB approval for new information collections from ten or more members of the public. If the information collection is both a new collection and automated, then a PIA is required.

What are the Privacy Act Requirements?

Privacy Act. The Privacy Act of 1974, as amended (<http://www.usdoj.gov/foia/privstat.htm>) requires that agencies publish a Federal Register Notice for public comment on any intended information collection. Privacy Act Systems of Records are created when information pertaining to an individual is collected and maintained by the Department, and is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to an individual. The E-Government Act of 2002 requires PIAs for electronic systems as well as information collection requests that are automated. So, there is a relationship between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notices (for both paper-based and automated records that are of a private nature). For additional information, contact the Departmental Privacy Act Officer in the Office of the Chief Information Officer.

Why is the PIA Summary Made Publicly Available?

The E-Government Act of 2002 requires that the analysis and determinations resulting from the PIA be made publicly available. The Privacy Advocate in HUD's Office of the Chief Information Officer (OCIO) is responsible for publishing the PIA summary on HUD's web site. See: <http://www.hud.gov/offices/cio/privacy/pia/pia.cfm>.

SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT

Program Area: Ginnie Mae Office of Securities Operations

Subject Matter Expert in the Program Area: Tamara Togans

Program Area Manager: Daniel Kahn

IT Project Leader: John Cump

For IT Systems:

- **Name of system:** Ginnie Mae General Support System (GNMA GSS)
- **PCAS #:** N/A
- **OMB Unique Project Identifier #:** N/A
- **System Code:** TBD
- **Development Date:** 1 Sep 2015
- **Expected Production Date:** 1 Jan 2016

For Information Collection Requests:

- **Name of Information Collection Request:** N/A
- **OMB Control #:** N/A

Question 1:

Provide a general description of the system that describes: The following questions are intended to define the scope of the information in the system (or information collection), specifically the nature of the information and the sources from which it is obtained.

- a. **What is the personal information being collected?**
 1. **Loan origination and servicing data:** Borrower/co-borrower name, social security number, gender, date of birth, and property address.
 2. **Physical security holders (investors) data:** Social security number / tax ID, name, mailing address, phone number, or email address of those holding the security.
 3. **Issuer and document custodian data:** Name, title, and phone number of the issuer and document custodian employees involved in the pooling, certification, and monthly reporting process.
 4. **Data associated with login and application permissions:** For Ginnie Mae Issuers, Ginnie Mae employees, and contracted personnel in accessing the system

- b. **From whom is the information collected (i.e., government employees, contractors, or consultants)?**

Information is collected from Issuers and Document custodians involved in the pooling and certification process for the issuance of Ginnie Mae-guaranteed mortgage-backed securities.

Information is collected from Ginnie Mae Issuers and Document Custodians, Ginnie Mae employees, and contracted personnel as part of the registration process in establishing and authenticating user credentials for system login.

c. What is the functionality of the system and the purpose that the records and/or system serves?

The Ginnie Mae (GNMA) General Support System (GSS) system serves as the common infrastructure of Ginnie Mae's information system design and plays a hierarchical role to the "legacy" systems. The GSS includes the GNMA infrastructure, platforms, software, portals, and business logic to support the operations and management of the GNMA Major Applications (MA). The GNMA GSS is hosted and operated by the Bank of New York Mellon (BNYM). The GNMA GSS supports three MA Ginnie Mae Network (GNET), Integrated Pool Management System (IPMS), and Unclaimed Funds System (UFS). The GNMA MA provides transactional services and functions, via a web-based publicly facing application.

GNET is a MA that is used by Issuers to electronically submit Mortgage Backed Securities (MBS) pools, final certifications and recertification information. GNET is also used by Document Custodians to certify or reject submissions. IPMS is a MA proprietary mainframe application that has three major component subsystems; New Pool Processing, Pool Reporting and Generalized Mortgage Backed Securities. UFS is an MA used to track the principal and interest payments sent to Ginnie Mae I and II security holders and never presented for payment and are six or more months old.

In response to the growing need for increased transparency and improved service delivery to its Issuers and Investors, Ginnie Mae is undertaking a major effort to modernize its Securitization Platform technology, processes, and related policy that will integrate several functional and technological capabilities into a common infrastructure known as GNMA GSS. Common enterprise-level security policies and procedures defined by GNMA GSS may be inherited by any of the GNMA MA system security plan (SSP).

Ginnie Mae uses this data to administer and carry out its functions as guarantor of securities under Section 306(g) of the National Housing Act, 12 U.S.C. 1721(g).

d. How is information transmitted to and from the system?

Issuers and service bureaus, via HTTPS and SFTP.

e. What are the interconnections with other systems.

GSS interconnects with the Ginnie Mae business applications that it consolidates into one common presentation layer via system portlets. This includes the Reporting and Feedback System (RFS). It also interfaces with Unclaimed Funds (UFS) and the Integrated Pool Management System (IPMS).

f. What specific legal authorities, arrangement, and/or agreement authorize the collection of information (i.e. must include authorities that cover all information collection activities, including Social Security Numbers)?

Ginnie Mae uses the information collected to carry out its functions as guarantor of securities under Section 306(g) of the National Housing Act, 12 U.S.C. 1721(g).

Question 2:

Type of electronic system or information collection.

A. If a new electronic system (or one in development) (implemented after April 2003, the effective date of the E-Government Act of 2002)?	Yes	No
Does the system require authentication?	X	
Is the system browser-based?	X	
Is the system external-facing (with external users that require authentication)?	X	

B. If this is existing electronic system, has the system undergone any changes (since April 17, 2003)? If an existing system, when was the system developed? <u>June 30, 2009</u>	Yes	No
Do the changes to the system involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system?		
If yes, please explain:		

C. For your new and/or existing electronic system, please indicate if any of the following changes have occurred: Mark any of the following conditions for your existing system that OMB defines as a “trigger” for requiring a PIA or PIA update (if not applicable, mark N/A):	
N/A	Conversion: When paper-based records that contain personal information are converted to an electronic system
N/A	From Anonymous (Non-Identifiable) to “Non-Anonymous” (Personally Identifiable): When any systems application transforms an existing database or data collection so that previously anonymous data becomes personally identifiable
X	Significant System Management Changes: When new uses of an existing electronic system significantly change how personal information is managed in the system. (Example #1: when new “relational” databases could combine multiple identifying data elements to more easily identify an individual. Example #2: when a web portal extracts data elements from separate databases, and thereby creates a more open environment for exposure of personal data)
X	Merging Databases: When government databases are merged, centralized, matched, or otherwise significantly manipulated so that personal information becomes more accessible (with special concern for the ability to combine multiple identifying elements)

N/A	New Public Access: When <u>new</u> public access is given to members of the public or to business partners (even if the system is protected by password, digital certificate, or other user-authentication technology)
N/A	Commercial Sources: When agencies systematically incorporate into databases any personal data from commercial or public sources (ad hoc queries of such sources using existing technology does not trigger the need for a PIA)
N/A	New Inter-agency Uses: When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
X	Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data
N/A	Alteration in Character of Data: When adding new personal data raises the risks to personal privacy (for example, adding financial information to an existing database that contains name and address)

D. If an Information Collection Request (ICR): Is this a <u>new</u> Request that will collect data that will be in an <u>automated</u> system? Agencies must obtain OMB approval for information collections from 10 or more members of the public. The E-Government Act of 2002 requires a PIA for ICRs only if the collection of information is a <u>new</u> request and the collected data will be in an <u>automated</u> system.	
X	Yes, this is a new ICR and the data will be automated
	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>)
	Comment:

Question 3:

Explain by Line of Business why the personally identifiable information being collected? How will it be used?

Mark any that apply:

Homeownership:

	Credit checks (eligibility for loans)
	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
	Loan default tracking
	Issuing mortgage and loan insurance
X	Other (specify): Ginnie Mae uses PII to administer and carry out its functions as guarantor of securities backed by mortgage loans.
	Comment:

Rental Housing Assistance:

	Eligibility for rental assistance or other HUD program benefits
	Characteristics on those receiving rental assistance (for example, race/ethnicity, # of children, age)
	Property inspections
	Other (specify):
	Comment:

Grants:

	Grant application scoring and selection – if any personal information on the grantee is included
	Disbursement of funds to grantees – if any personal information is included
	Other (specify):
	Comment:

Fair Housing:

	Housing discrimination complaints and resulting case files
	Other (specify):
	Comment:

Internal operations:

	Employee payroll or personnel records
	Payment for employee travel expenses
	Payment for services or products (to contractors) – if any personal information on the payee is included
	Computer security files – with personal information in the database, collected in order to grant user IDs
	Other (specify):
	Comment:

Other lines of business (specify uses):

X	Security/access authentication for system users

Question 4:

Will you share the information with others? (e.g., another agency for a programmatic purpose, internal HUD application/module or outside the government)?

Mark any that apply:

X	Federal agencies?
	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
	HUD module/application? (specify the module(s)/application(s) name)
	Others? (specify):
	Comment:

Question 5:

Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?

	Yes, they can “opt-out” by declining to provide private information or by consenting only to particular use
X	No, they can’t “opt-out” – all personal information is required
	Comment: The data is not collected from the individuals identified by the information. It already exists within GNMA database(s).

If Yes, please explain the issues and circumstances for opting-out (either for specific data elements or specific uses of the data):

Question 6:

How will the privacy of the information be protected/ secured? What are the administrative and technological controls?

Mark any that apply and give details if requested:

X	System users must log-in with a password (Please specify password type): User IDs are disabled immediately after an employee is terminated or transferred. <i>Disabled IDs are removed after 6 months of non-usage.</i>
X	When an employee leaves: <ul style="list-style-type: none"> • How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? <i>Immediately.</i> • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): <i>Accounts are disabled immediately and then monitored for attempts to use the account.</i>
X	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either: <ul style="list-style-type: none"> • <i>Full access rights to all data in the system: 0 Roles based access control prevents one user from having too much access.</i> <i>Limited/restricted access rights to only selected data: 2,395</i>
X	Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? (explain your procedures, or describe your plan to improve): <i>The data is stored on SAN unit on an isolated network. Access to the data on the SAN unit to which access is restricted to BNY employees whose job descriptions require access to that data. All data is stored in secured facilities and card key access is required.</i>
	If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? Explain the existing privacy protections, or your plans to improve: <i>Currently, personal data is not shared with other systems of data warehouses outside of Ginnie Mae.</i>
	Other methods of protecting privacy (specify):
	Comment:

Question 7:

If privacy information is involved, by what data element(s) is it retrieved from the system?

Mark any that apply

X	Name
X	Social Security Number (SSN)
X	Identification number (specify type): Driver License/State ID#, Tax ID/EIN
X	Birth date

	Race/ ethnicity
	Marital status
	Spouse name
X	Home address
X	Home telephone
X	Personal e-mail address
X	Other (specify): Financial (Loan data), Tax, Income data
	None
	Comment:

Question 8:

What type of Notice(s) are provided to the individual on the scope of information collected, the opportunity to consent to uses of said information, the opportunity to decline to provide information.

- a. **Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on form(s), and/or a system of records notice published in the Federal Register.) If notice was not published, why not?**

Yes, the EWODS component of this system is considered a System of Record and has a published SORN.

- b. **Do individuals have an opportunity and/or right to decline to provide information? No.**
- c. **Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent? No.**

Question 9:

What are the Retention Use and Disposal Practices. Guidance for this section should obtain from HUD retention use and disposal policy. It should also be validated that these procedures are outlined in the contracted service agreement to ensure that the contracted system does not hold onto data after services are no longer provided.

- a. **How long is information retained?**

Data within GSS is retained in accordance with HUD Disposition Schedule 64. Meaning that most information is retained 7 years after the closure of the loan.

- b. Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?**

This would have to be verified by Ginnie Mae, it is our understanding that NARA has approved Schedule 64.

- c. Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.**

The only risk is that older media may not be readable due to advances in technology. GinnieNET avoids this risk because it is using a virtual disk system that upon upgrade moves all existing backups to the new platform.

SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER