



# Privacy Impact Assessment for Ginnie Mae Contractors

---

[Ginnie Mae Enterprise Portal \(GMEP\) GSS](#)

Information Management Division

October 26, 2010

Version 1.5

## Introduction

The purpose of this Privacy Impact Assessment is to help the Information Management Division (IMD) identify Ginnie Mae's information systems that process, store, use, and distribute data covered under the Privacy Act of 1974.

Ginnie Mae is responsible for ensuring the privacy and confidentiality of Personally Identifiable Information (PII) it collects, maintains, or disseminates from or about members of the public. Personally Identifiable Information includes information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.)

### Instructions:

**1. Fill out Part 1 of this study.**

You may fill out the study electronically, but you must print it out to sign and mail it.

**2. If you check yes to any of the questions about PII data in Section c of Part 1, you must also fill out Part 2.**

Please be as descriptive as possible in answering the questions. You may use additional paper if necessary.

**3. Sign and date the form, and then mail it to the following address via a secure mail service:**

Ginnie Mae  
Attention: Chitranjan Khandpur  
451 7th Street SW  
Room # B-133  
Washington, DC 20410

If your organization processes, stores, uses, or distributes PII data, a security analyst working with the Ginnie Mae Information Management Division (IMD) will contact you to arrange a brief interview regarding how the PII data is being protected from unauthorized use, disclosure, or loss. These interviews usually last less than an hour, and you are not required to travel (the security team will come to your site).

Thank you for helping protect Ginnie Mae PII/privacy data.

## Part 1: Privacy Data Determination

Please review Section A and fill out Sections B and C of Part 1.

### A. System Information

If any information is incorrect in this section, please strike through it, correct it, and then initial the correction.

System Information	
System Name	GMEP GSS
System Description	The GMEP GSS will combine security for some of Ginnie Mae's applications so that users who are granted access rights to such applications are presented with a consistent, unified web-based interface, giving the user access to different information and tools in a single place. Users need only to log on once for all granted content and applications within the Portal. By integrating with EWODS, (the Enterprise Wide Operational Data Store), RFS, (Report Feedback System), and Business Objects, the cost and effort in developing and maintaining all Ginnie Mae applications can be significantly reduced as these critical parts of Ginnie Mae's applications will be controlled in one single place.
Name of System Provider	Bank of New York
Ginnie Mae Information Owner	Cheryl Owens

### B. System Provider Contact Information

Please enter the names and contact information for those personnel with primary responsibility for the Ginnie Mae information system.

Contact Name	Title	Phone	Email
Jumedia Buchner	Vice President	212-815-2605	jumedia.buchner@bnymellon.com
Brian Lavelle	Managing Director	718-315-5045	brian.lavelle@bnymellon.com
Teddy Herlihy	Vice President	718-315-5087	teddy.herlihy@bnymellon.com

---

---

**C. PII Data Processed by System**

What Personally Identifiable Information (PII) is collected or stored on your Ginnie Mae information system(s)? Please check yes or no in the box provided.

Type of PII Data	Yes	No
1. Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2. Social Security Number (SSN)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3. Home address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4. Home telephone	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5. Personal email address	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6. Date of birth	<input type="checkbox"/>	<input checked="" type="checkbox"/>
7. Driver's license/state ID number	<input type="checkbox"/>	<input checked="" type="checkbox"/>
8. Race (e.g., Caucasian, African-American, American Indian, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9. Religion	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10. Ethnicity/national origin (e.g., Canadian, South African, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11. Biometric information (e.g., fingerprint, voiceprint, photograph, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
12. Financial information (loan number, credit score, credit card number, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
13. Passport number	<input type="checkbox"/>	<input checked="" type="checkbox"/>
14. Permanent and Alien registration number (Green Card)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
15. Insurance policy number	<input type="checkbox"/>	<input checked="" type="checkbox"/>
16. Digital/electronic signature information	<input type="checkbox"/>	<input checked="" type="checkbox"/>
17. Medical/psychological information	<input type="checkbox"/>	<input checked="" type="checkbox"/>
18. Criminal history	<input type="checkbox"/>	<input checked="" type="checkbox"/>
19. Mother's maiden name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
20. Drug test results	<input type="checkbox"/>	<input checked="" type="checkbox"/>
21. Marital status	<input checked="" type="checkbox"/>	<input type="checkbox"/>
22. Education history	<input type="checkbox"/>	<input checked="" type="checkbox"/>
23. Gender/sex	<input type="checkbox"/>	<input type="checkbox"/>
24. Income data	<input type="checkbox"/>	<input type="checkbox"/>
25. Employment history	<input type="checkbox"/>	<input type="checkbox"/>
25. Tax Identification Number, Employee Identification Number	<input type="checkbox"/>	<input type="checkbox"/>
26. Other (please specify):	<input type="checkbox"/>	<input checked="" type="checkbox"/>

## Part 2: Privacy Data Details

If you answered yes to any question in Part 1, Section c of this form, please answer the questions below as completely as possible.

1.	<b>Does your Ginnie Mae system process, store, or collect PII data about more than 10 individuals?</b>
	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
2.	<b>On what type of media is the PII data stored or collected? (For example, is the information collected via the Web, email, CDs, paper forms, etc.?)</b>
	Data is collected via the web and using an ETL tool that extracts data from the IPMS production databases. Data collected using the Reporting and Feedback System (RFS) is stored directly into EWODS. The data is stored on a SAN on an isolated network in a secured cage within the BNYM data center.
3.	<b>What are the sources of the PII data? From whom is the information collected (e.g., government employees, contractors, consultants, the public)?</b>
	Data is collected via web from the Security Administrators and Security Officers, some of whom are Ginnie Mae employees, issuer employees, or BNYM employees, and are stored in EWODS. An ETL tool extracts data from IPMS production databases and stored in EWODS.
4.	<b>Why is the PII data stored or collected? What is the functionality of the system and the purpose that the records and/or system serve?</b>
	EWODS is used to store the PII data as the central repository for all of Ginnie Mae's enterprise data. Some information is collected (name, mothers maiden name, marital status) is collected as part of security registration in GMEP. Other PII information regarding pool investors is extracted from IPMS and stored in EWODS, along with data collected by RFS and stored directly into EWODS.
5.	<b>How is information transmitted to and from the system?</b>
	Information is transferred internally from IPMS within BNYM over the BNYM secure network using an ETL tool.
6.	<b>What are the interconnections with other systems?</b>
	There is an interconnection with another Ginnie Mae information system, Integrated Pool Management System (IPMS).
7.	<b>What is the current / intended use of the PII data? What is the functionality of the system and the purpose that the records and/or system serve?</b>

	<p>In the portal, name, mother maiden name, marital status and it is used for user security authentication. The GMEP GSS will combine security for some of Ginnie Mae's applications so that users who are granted access rights to such applications are presented with a consistent, unified web-based interface, giving the user access to different information and tools in a single place. Users need only to log on once for all granted content and applications within the Portal. By integrating with EWODS, (the Enterprise Wide Operational Data Store), RFS, (Report Feedback System), and Business Objects, the cost and effort in developing and maintaining all Ginnie Mae applications can be significantly reduced as these critical parts of Ginnie Mae's applications will be controlled in one single place. As a data repository, EWODS contains PII information extracted from IPMS. That data is only being stored in EWODS and is not used for any other purpose currently. Data deposited into EWODS by RFS is utilized by RFS and the use of which will be analyzed in the PII documentation for RFS.</p>
<b>8.</b>	<b>With whom is the PII data shared (other agencies, organizations, systems, etc.)?</b>
	None for GMEP GSS.
<b>9</b>	<b>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)?</b>
	HUD and Ginnie Mae.
<b>10.</b>	<b>How is the PII data secured?</b>
	Stored on a SAN in a physically in a secured segregated environment within the BNYM data centers and is logically isolated behind 3 layers of firewalls.
<b>11.</b>	<b>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?</b>
	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Additional explanation if required:
<b>12.</b>	<b>Do individuals have an opportunity and/or right to decline to provide information?</b>
	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Additional explanation if required:
<b>13.</b>	<b>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?</b>
	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Additional explanation if required:

<b>14.</b>	<p><b>Is this IT system a System of Record?</b></p> <p>A System of Record is any group of records collected from the primary source under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. For example, a system that collects credit scores of individuals and is searchable by name or SSN would be a System of Record.</p>
	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p><b>Additional explanation if required:</b></p>
<b>15.</b>	<p><b>Is this system part of another System of Record?</b></p> <p>If your system receives a feed containing PII data from another agency's system that collects the PII data from the public, then that other agency's system is the System of Record and they are the sponsor of the collection. For example, if your system uses data from FHA that the agency has collected directly from the public, then your system is not the System of Record (the FHA system is).</p>
	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p><b>If yes, provide name of the System of Record and sponsor:</b></p>
<b>16.</b>	<p><b>Has a Systems of Record Notice (SORN) been published/approved by OMB for the system?</b></p> <p>A SORN is a notice that is published in the Federal Register whenever a new System of Record is implemented or an existing System of Record has modifications that impact the privacy data it collects.</p>
	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p><b>If yes, provide OMB form number and name:</b></p>
<b>17.</b>	<p><b>Is the system currently being modified or will it be modified this year?</b></p>
	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><b>If yes, describe modification:</b></p> <p>There are proposals to update to a later version of Oracle for EWODS and of BEA Weblogic for GMEP. Minor changes, mostly to support RFS, are made to GMEP and EWODS as necessary.</p>
<b>18.</b>	<p><b>If the system is being modified, will the SORN require amendment or revision?</b></p>
	<p>A revised notice must be published in the Federal register if the planned modifications to the System of Record will impact the privacy data the system collects.</p>
	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>

	If yes, explain:
19.	<p><b>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.</b></p>
	The data is being retained indefinitely.
20.	<p><b>How long is information retained?</b></p>
	The data is being retained indefinitely.
21.	<p><b>Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?</b></p>
	N/A. The data is being retained indefinitely.
22.	<p><b>Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated. Specify the risk associated with retention of this PII. Will it be retained only as necessary? Please include a statement regarding the inadvertent collection of PII, and how it is documented and destroyed.</b></p>
	Retaining information indefinitely allows the possibility of unauthorized persons gaining access to the PII information stored. The level of privacy risk of the stored information has been identified as low given the limited amount of privacy information that will be collected and maintained on the system. In addition, GMEP and EWODS are being retained in a segregated physical and logical environment. The GMEP and EWODDS servers and other hardware are located in a separate locked cage in the Bank of New York Mellon data centers. The GMEP and EWODS network is separated from other networks by firewalls. Access to the GMEP application and the EWODS data is on a "need to know" basis. User access to GMEP requires a user id and a complex password, which will periodically expire in compliance with NIST requirements.

Based on the authority of contractor representative, all data captured in this document is current and accurate.

<hr/>	
<b>Signature</b>	<b>Date</b>
 	<b>10/28/2010</b>
<hr/>	
<b>Printed Name</b>	<b>Title</b>
Brian Lavelle	Vice President

Reviewed by:

<hr/>	
<b>Chitranjan Khandpur</b>	<b>Date</b>
Ginnie Mae Chief Privacy Officer	

Reviewed by:

<hr/>	
<b>Deborah V. Holmes</b>	<b>Date</b>
Ginnie Mae Chief Information Officer	