Ginnie Mae Data Privacy Policy

GinnieMae
Our Guaranty Matters

DocuSign Envelope ID: B343C3D8-7304-4047-B6A6-E921DAFA2462

POLICY 4060.02.2001

SUBJECT. Ginnie Mae Data Privacy Policy.

OVERVIEW. This policy provides guidance and requirements pertaining to the maintaining and handling of sensitive data (Personally Identifiable Information (PII), sensitive financial data, proprietary information, etc.) that is owned or managed for the benefit of Ginnie Mae.

PURPOSE. The Ginnie Mae Data Privacy Policy outlines a list of privacy guidelines and standards that all Ginnie Mae employees, contractors, subcontractors, and program participants such as issuers, subservicers, document custodians, and funds custodians must comply with.

SCOPE. The scope of this policy applies to all Ginnie Mae employees, contractors, subcontractors, and program participants such as issuers, subservicers, document custodians, and funds custodians who use, manage, and/or maintain Ginnie Mae data.

EFFECTIVE DATE. Policy 4060.02.2001 Privacy Policy is effective upon the date of approval.

EXPIRATION DATE. This policy remains in effect until officially superseded or retired.

FREQUENCY OF REVIEW. This document will be reviewed annually and updated as needed. This document contains a revision history log. When changes occur, the version number will be updated to the next increment and the date, owner making the change, and change description will be recorded in the revision history log of the document.

CERTIFICATION. Include approval signatures by applicable Ginnie Mae personnel.

DocuSigned by:
Kimberly Hersey
A8838898BD9F4A6...

Kimberly Hersey
Ginnie Mae Acting CISO

Date: 8/14/2023 | 1:33 PM EDT

DocuSigned by:
Barbara Cooper-Jones
8BF514D70973472...

Barbara Cooper-Jones
Sr. Vice President

Date: 8/14/2023 | 12:45 PM EDT

DocuSign Envelope ID: B343C3D8-7304-4047-B6A6-E921DAFA2462

Document Name	Insert Policy Name
Policy Number	4060.02.2001
Version Number	V1
Date Approved	August 15, 2023
Effective Date	August 15, 2023
Author	Ashraf (Ash) Aziz OEDTS
Owner	Kimberly Hersey, Program Manager OEDTS
Approver	Troy Icenhour, CISO OEDTS
Required Approver	Barbara Cooper-Jones, SVP OEDTS

DOCUMENT HISTORY

Revision History			
Version	**Date**	**Author**	**Description**
Insert Version Number	Date of Revision	Author of Revision	Describe what was modified and/or updated from the previous version.
1	03/02/23	Ashraf (Ash) Aziz	Initial Publication
1	08/09/23		Reviewed
1	08/16/23		Published

DocuSign Envelope ID: B343C3D8-7304-4047-B6A6-E921DAFAD462

TABLE OF CONTENTS

DocuSign Envelope ID: B343C3D8-7304-4047-B6A6-E921DAFA2462

1.0 INTRODUCTION

1.1 PURPOSE

The Ginnie Mae Data Privacy Policy ("Privacy Policy") defines the privacy guidelines that all Ginnie Mae employees, contractors, subcontractors, and program participants such as issuers, subservicers, document custodians, and funds custodians who access, manage, and/or store Ginnie Mae sensitive data (Personally Identifiable Information (PII), proprietary information, sensitive financial data, etc.) must comply. This policy and its guiding principles direct how sensitive data, that is attributed to Ginnie Mae, must be handled and protected to comply with federal privacy laws as listed in section 8.2 of this policy. The data protection and reporting requirements outlined in this policy must be understood and followed by Ginnie Mae employees, contractors, subcontractors, and program participants in order to avoid negative impacts to the Ginnie Mae mission, business or operations.

Personally Identifiable information is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (Privacy Act Public Law 93-579). An organization cannot properly protect PII it does not know about. This document uses a broad definition of PII to identify as many potential sources of PII as possible. Set forth below is a non-exclusive list of information that may constitute PII on its own or in combination with other information. To determine whether information is PII, the agency shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available - in any medium or from any source - that would make it possible to identify an individual.

- Full name
- Home address
- Business Contact Information
- Personal e-mail address
- Social security number
- Passport number
- Driver's license number
- Certificate number
- Credit card numbers
- Date of birth
- Telephone number
- Log in details
- Personnel number
- Vehicle identifier or serial number
- Photograph or video identifiable to an individual
- Biometric information
- Medical information
- Criminal history
- Other information related to an individual that may directly or indirectly identify that individual (e.g., salary, performance rating, purchase history, call history, etc.)

In addition, to the elements above, Sensitive PII (as defined in the Handbook for Safeguarding Sensitive PII Privacy Policy Directive 047-01-007, Revision 3) requires special handling due to the increased risk of harm to an individual if it is compromised. The

DocuSign Envelope ID: B343C3D8-7304-4047-B6A6-E921DAFAD462

loss or compromise of SPII can result in embarrassment, inconvenience, reputational harm, emotional harm, financial loss, unfairness, and in rare cases, a risk to Personal safety.

1.2 GINNIE MAE FINANCIALLY SENSITIVE DATA

Financially sensitive data refers to information related to Ginnie Mae's financial operations that could be damaging to the organization if accessed, altered, or disclosed without authorization. This could include financial statements, bank account information, payment card information, transaction records, and other financial data that could be used for fraudulent activities or financial gain.

Proprietary data refers to information that is owned by Ginnie Mae and is not publicly available. This could include intellectual property such as patents, trademarks, copyrights, and trade secrets. It could also include business plans, pricing information, marketing strategies, customer lists, and other confidential information that, if disclosed, could harm Ginnie Mae's business operations or reputation. Proprietary data is commonly considered the driving force of an enterprise and is critical to its success, making it a prime target for cybercriminals seeking to steal valuable information for their financial gain or to damage the enterprise's reputation.

Additionally, Ginnie Mae personnel are expressly prohibited from unlawfully disclosing proprietary, non-public information that Ginnie Mae has or receives from its program participants, such as issuers and document custodians, under the Trade Secrets Act (18 U.S.C. § 1905). This Act prohibits the disclosure of trade secrets by federal agencies and personnel. Personnel are made criminally liable if they publish, divulge, disclose, or make known in any manner or to any extent, not authorized by law, any information coming to them in the course of their employment or official duties.

Throughout this policy, **Ginnie Mae sensitive data** refers to PII, financially sensitive and proprietary data that if obtained in an unauthorized manner could cause serious impact to business operations.

The protection of financially sensitive and proprietary data is critical to the success and stability of Ginnie Mae. Example:

- Financial losses: A successful cyber-attack on an enterprise's financially sensitive data can result in significant financial losses, which can damage Ginnie Mae's financial stability and its ability to operate.
- Legal liabilities: The theft or unauthorized disclosure of financially sensitive or proprietary data can result in legal liabilities and regulatory fines. These liabilities can have a significant impact on Ginnie Mae's financial health.
- Reputational damage: A cyber-attack on financially sensitive or proprietary data can damage Ginnie Mae's reputation, leading to a loss of trust from program participants,

DocuSign Envelope ID: B343C3D8-7304-4047-B6A6-E921DAFA2462

stakeholders, and investors. This can have long-term consequences for the overall organization's financial performance.

- Intellectual property theft: Proprietary data, such as intellectual property, is critical to Ginnie Mae's business operations. A cyber-attack that results in the theft or disclosure of proprietary data can harm the enterprise's competitive position and financial performance.

1.3 STRATEGIC GOALS AND OBJECTIVES

Ginnie Mae's goals and objectives for Data Privacy are as follows:

- To protect and manage all sensitive data in such a manner that prevents any unauthorized access or data disclosure.
- To maintain compliance with federal privacy laws, regulations, and best practices, per NIST 800-122, (Guide to Protecting of Confidentiality of Personally Identifiable Information PII) FIPS 199, (Standards for Security Categorization of Federal Information and Information Systems), NIST 800-53 rev 4, (Security and Privacy Controls for Information Systems and Organizations).
- Foster a culture of privacy protection and demonstrate leadership through policy and strategic partnership.
- Provide outreach, training, and education to promote and enhance privacy across Ginnie Mae.
- Develop and maintain privacy professionals that can serve as trusted privacy advisors for Ginnie Mae.

1.4 ROLES AND RESPONSIBILITIES

A. All Ginnie Mae employees, contractors, subcontractors, and program participants such as issuers, subservicers, document custodians, and funds custodians involved with handling PII and sensitive data must comply with PII handling requirements outlined in the Privacy Policy.

i. The Chief Information Security Officer is responsible for the overall risk advisory as it pertains to Personally Identifiable Information and for ensuring personnel understand the terms of the Data Privacy Policy and are adequately trained.

ii. Information System Security Officers (ISSO) are responsible for ensuring that adequate security controls have been implemented and documented to ensure data privacy protection of all systems authorized for operation within the Ginnie Mae IT enterprise.

iii. System Owners are responsible for ensuring the system design, use and operation is done in accordance with existing Ginnie Mae policies and procedures.

iv. Employees, contractors, subcontractors, and program participants such as issuers, subservicers, document custodians, and funds custodians, must comply with the standards set forth in this policy and notify the Privacy Liaison Officers (PLOs) of any Privacy Policy violations and noncompliance.

DocuSign Envelope ID: 93C53609-7F1E-4809-AAC1-EBA805EA3DF2

v. Service providers and program participants, financial institutions, and issuers who have been authorized to manage, store, and maintain Ginnie Mae sensitive data sharing will support the U.S. Department of Housing and Urban Development (HUD) goals of ensuring proper handling of Ginnie Mae sensitive data transmissions. If the need for system interconnection arises, additional protections will be required.

B. The HUD privacy office has executive oversight of privacy data as delegated by the Senior Agency Official for Privacy (SAOP) of the Department of Housing and Urban Development (HUD). The HUD Chief Privacy Officer (CPO) has executive oversight.

C. Ginnie Mae appointed Privacy Liaison Officers (PLOs) are responsible for tracking violations of the Privacy Policy and reporting them to the HUD Privacy Office. Each Ginnie Mae business unit can appoint, and designate PLOs based upon their specific needs. There are no limitations on the number of PLOs that can be appointed across the organization. Appointment letters are to be submitted to the HUD CPO, where additional and recurring PLO training will be provided.

DocuSign Envelope ID: B343C3D8-7304-4047-B6A6-E921DAFA2462

1.5 CONTACTS

If further questions, inquiries, or policy related requests exist, contact the following:

Subject	Party	Contact
INFOSEC/PLO	Ashraf Aziz	OGrp-INFOSECTeam@hudgov.onmicrosoft.com
INFOSEC Program Manager	Kimberly Hersey	OGrp-INFOSECTeam@hudgov.onmicrosoft.com

DocuSign Envelope ID: B343C3D8-7304-4047-B6A6-E921DAFAD462

2.0 SENSITIVE INFORMATION HANDLING

2.1 INTRODUCTION

Ginnie Mae requires strict handling guidelines for employees and contractors who handle PII due to the nature of the data and the increased risk to an individual or the organization if the data were to be compromised.

2.2 CATEGORIZATION OF PII AND SENSITIVE DATA

Ginnie Mae systems and processes that access, transmit and store Ginnie Mae sensitive data will be evaluated by the use of the PII Confidentiality Impact Level, (PICL) https://www.hud.gov/sites/dfiles/OCHCO/documents/PCILCategorizationTemplate.pdf to determine the categorization of the data and PII confidentiality impact level so that the appropriate safeguards can be applied to protect the PII. The PII confidentiality level – Low, Moderate or High indicates the potential harm that could result to the subjects, individuals and /or the organization if PII were inappropriately accessed, used, or disclosed. The following are the deciding factors that will be used for the determination of confidentiality impact levels:

- Identifiability- The ease with which PII can be utilized to identify certain individuals will be considered by organizations. For instance, whereas a telephone area code identifies a group of people, an SSN specifically and immediately identifies a single person.
- Quantity of PII- agency will think about how many people can be recognized from the PII. Different effects may result from breaches of 25 records as opposed to 25 million records. Based on this factor, the PII confidentiality effect level will only be increased, never decreased.
- Obligations to Protect Confidentiality - PII will consider such obligations when determining the PII confidentiality impact level.
- Obligations to protect generally include laws, regulations, or other mandates (e.g., Privacy Act, OMB guidance)

DocuSign Envelope ID: B343C3D8-7304-4047-B6A6-E921DAFAD462

3.0 GENERAL HANDLING OF PII / GINNIE MAE SENSITIVE DATA

Methods for handling PII include, but are not limited to the following, and must be done in accordance with HUD and Ginnie Mae policies, training, NIST standards, Privacy Act of 1974 and all other applicable guidelines.

- Post or store PII only on secure Ginnie Mae networks, systems, applications and Ginnie Mae media that are approved and accredited for PII storage and transmission.
- Minimize the use, collection, processing, storage, dissemination, and retention of PII to what is defined in the PICL as strictly necessary to accomplish business, a legally authorized purpose, and mission.
- Have detailed procedures and processes to safeguard the privacy of PII.
- Must have compliance by Ginnie Mae government employees and authorized contractors with HUD Privacy Handbook 1325.1 Rev. 1.0 (or current revision) for Privacy and PII handling and maintain annual HUD-privacy training.
- Must sign will be required to sign the “Rules of Behavior” before being granted system/information environment access and participate in recurring training and awareness, as required by Ginnie Mae IT Support contractors, vendors and program participants.
- Assess the combined sensitivity of the PII data fields. Each PII data field's sensitivity must be evaluated to ensure the necessity of the information to meet the needs of the organization, mission, system, etc. A person's SSN or financial account number, for instance, are typically more sensitive than their phone number or ZIP code.
- Secure paper PII data by locking it in desks and filing cabinets.
- Remove visible PII from desks and office spaces when not in use (e.g., at the end of each day)
- Destroy paper PII by shredding when no longer needed in accordance with Ginnie Mae and federal records retention policies.
- Must encrypt sensitive data on computers, media, and other devices at all times, both when it is in-transit and at rest. Only use Ginnie Mae-provided email addresses for conducting official business.
- Do not email PII to personal accounts or devices, outside of the protection of Ginnie Mae approved and authorized storage systems and media.

3.1 SYSTEM SECURITY CONTROLS

All Ginnie Mae sensitive data must be contained within a business system that has an active Authority to Operation (ATO) based on the NIST SP 800-53 and specifically has the required security controls associated with protecting sensitive data. There can be no sensitive or production data within a business system until after the final approval of the system’s ATO without an approved Risk Acceptance (RA) through Ginnie Mae’s Authorizing Official (AO). Additionally, all business systems that contain PII, sensitive, and financially sensitive data must have controls in place that limit access to only those who are authorized to view the information. All Ginnie Mae program participants (contractors, subcontractors, and program participants such as issuers, subservicers, document custodians, and funds custodians) that store and maintain Ginnie Mae sensitive data as defined in this policy are required to complete and satisfy the PICL, PIA and completed SORN, (if required) while addressing the entirety of NIST 800-53 Privacy Controls.

3.2 DISTRIBUTION AND TRANSMISSION

PII may be distributed or released to other individuals and redacted for events that need to be released with information that includes PII and not within the allowed definitions of this policy only if: (1) it is within the scope of the recipient's official duties; (2) the recipient has an official, job-based need to know; (3) the distribution is done in accordance with a legitimate underlying authority (e.g., a routine use to a SORN); and (4) sharing information is done in a secure manner. When in doubt Ginnie Mae employees must treat PII as sensitive and must keep the transmission of PII to a minimum, even when it is protected by secure means. Other ways for communicating, sending, and receiving PII include:

- Facsimile – When faxing information, Ginnie Mae personnel should include an advisory statement about the contents on the cover sheet and should notify the recipient before and after transmission.
- Mail – Ginnie Mae personnel should physically secure PII when in transit by sealing it in an opaque envelope or container, and mail it using First Class or Priority Mail, or a comparable commercial service. Ginnie Mae personnel should not mail, or send by courier PII on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted.
- Email – When emailing PII outside of Ginnie Mae, save it in a separate document and password-protect or encrypt it. Send the encrypted document as an email attachment and provide the password to the recipient in a separate email or by phone. Ginnie Mae Internal email that contains PII should be digitally signed and encrypted.
- Hard Copy – Ginnie Mae personnel should also hand-deliver documents containing PII whenever needed. Ginnie Mae personnel should not leave PII unattended on printers, facsimile machines, copiers, or in other common places.
- Upload and transmit documents through Ginnie Mae enterprise portals. Whenever uploading or submitting documents through enterprise portals or external systems, ensure that the system is accredited and authorized to store PII.

DocuSign Envelope ID: B343C3D8-7304-4047-B6A6-E921DAFA2462

4.0 DATA PRIVACY GUIDING PRINCIPLES

The processing of PII is subject to the enumerated principles. These principles are based on the Fair Information Practice Principles (FIPPs) and are reflected in Federal privacy legislations as well as OMB requirements.

- Access and Amendment – Ginnie Mae will provide individuals with appropriate access to PII and the opportunity to correct or amend PII.
- Accountability – Ginnie Mae will be accountable for complying with these principles and applicable privacy requirements, and will appropriately monitor, audit, and document compliance. Ginnie Mae will also clearly define the roles and responsibilities with respect to PII for all employees and contractors and will provide guidance to all employees and contractors who have access to PII.
- Authority – Ginnie Mae will only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and will identify this authority in the appropriate notice.
- Minimization – Ginnie Mae will only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and will only maintain PII for as long as is necessary to accomplish the purpose. Ginnie Mae maintains an inventory of PII holdings and uses the PIA, and SORN processes to identify methods to further reduce the data the Agency collects and to ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete.
- Quality and Integrity – Ginnie Mae will create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.
- Individual Participation – Ginnie Mae will involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Ginnie Mae will also establish procedures to receive and address individuals' privacy-related complaints and inquiries.
- Transparency – Ginnie Mae will be transparent about information policies and practices with respect to PII, and will provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

5.0 PRIVACY IMPACT ASSESSMENT AND SYSTEM OF RECORDS NOTICE

All business systems that contain Ginnie Mae data must complete a Privacy Impact Assessment (PIA) which is an analysis of how PII is collected, used, shared, and maintained. The PIA must be reviewed and approved by Ginnie Mae's Privacy Liaison Officer and will also be included as part of the ATO process. Each system PIA must be reviewed on an annual basis and updated as required based on any changes to the data involved that would have a material impact to the PIA.

The PIA is also the instrument used to determine if a System of Record Notice (SORN) is required based on the type of PII that is maintained within the system and how it is retrieved. A System of Records is a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. Ginnie Mae adheres to the Privacy Act requirements for publishing notices of its systems of records in the Federal Register, which are referred to as SORNs.

Each System of Records Notice (SORN) describes what, why and how Ginnie Mae collects, maintains, uses, and disseminates records in the system. Some systems maintain information on Ginnie Mae employees while others maintain information from or about individuals outside of Ginnie Mae. These Government-wide systems are maintained by other Federal agencies that hold some of the operating authority over the records such as the Office of Personnel Management's Employee Performance File system. Ginnie Mae adheres to the Privacy Act of 1974 requirements for publishing notices of its systems of records in the Federal Register, which are referred to as SORNs.

6.0 BREACH RESPONSE AND MANAGEMENT

Ginnie Mae has an obligation to protect the information entrusted to the Agency. Management of incidents involving PII or other sensitive data often requires close coordination among personnel from across the organization, such as the CIO, CPO, system owner, data owner, legal counsel, and public relations officer. Additionally, due to the unique nature of Ginnie Mae's business, open communication and shared situational awareness with program participants is vital to safeguard protected information. Because of this need for close coordination, system level incident response plans must be developed and tested annually in order to ensure that clear roles and responsibilities have been established to ensure effective management when an incident occurs.

All systems (government owned or contractor owned) that contain Ginnie Mae data must have an incident response plan that includes all of the roles and responsibilities of a data breach that has been approved by Ginnie Mae's CIO and CISO. Incident response plans must include instructions on how data breaches involving PII will be handled. Incident response plans will also address how to minimize the amount of PII necessary to adequately report and respond to a breach. Specific policies and procedures for handling breaches involving PII can be added to each of the following phases identified in *NIST SP 800-61*: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity. This section provides additional details on PII-specific considerations for each of these four phases.

Preparation – All systems (government owned or contractor owned) that contain Ginnie Mae data must have an incident response plan and this plan must be tested on an annual basis. Additionally, all organizations that have systems with Ginnie Mae data must have a training program that informs applicable staff on how to handle sensitive data appropriately.

Detection – All systems (government owned or contractor owned) that contain Ginnie Mae data must have applicable controls and procedures to effectively detect any unauthorized access to Ginnie Mae sensitive data or the breach of Ginnie Mae sensitive data.

Reporting – All Ginnie Mae employees, contractors, or organizations that maintain or store Ginnie Mae data, or support Ginnie Mae's business operations, must report any unauthorized access or data breach immediately (within 60 minutes) to a Ginnie Mae Privacy Liaison Officer, upon discovery.

Incident Response – All organizations that maintain or store Ginnie Mae data must work with Ginnie Mae and any other involved organizations (HUD, law enforcement, etc.) to effectively contain the incident. This includes the required notification to impacted individuals, mitigating privacy risks (i.e., credit monitoring, etc.), incident investigation, incident closeout, and post incident evaluation. The Ginnie Mae PLO and HUD Privacy Office will investigate the facts and circumstances surrounding the potential incident and further requires the SAOP and CPO or their designee to investigate whether PII was potentially or actually compromised.

Ginnie Mae has an obligation to protect the information entrusted to the Agency. Ginnie Mae's process for responding to a breach of PII is part of the Agency's program participants formal Incident Response Policy and Procedures and is based on OMB Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information and requires:

The SAOP determines which remediation methods should be used in the event of an actual compromise of PII based on the type of harm caused to the individual(s).

The Ginnie Mae PLO and HUD Privacy Office will conduct after action reports for high- and moderate-risk incidents that document the details of the incidents and the steps taken to remediate the gaps that caused the incident to occur.

If a privacy incident happens, the program participant must inform PLO within one hour of identifying it. The report should contain the incident date, data type, system name that holds the data, and the actions taken before and after identifying the incident.

7.0 PRIVACY ACT OF 1974 (5 U.S.C. § 552A)

The Privacy Act of 1974 is a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

The Ginnie Mae Privacy Policy will be reviewed by key points of contact and updated annually for major changes, audits as well as system assessments and authorization efforts.

8.0 REFERENCE MATERIAL

8.1 DEFINITIONS

Term	Definition
Aggregated Information	Information elements collated on a number of individuals, typically used for the purposes of making comparisons or identifying patterns.
Anonymized Information	Previously identifiable information that has been de-identified and for which a code or other association for re-identification no longer exists.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting Personal privacy and proprietary information.
Context of Use	The purpose for which PII is collected, stored, used, processed, disclosed, or disseminated.
De-identified Information	Records that have had enough PII removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.
Distinguishable Information	Information that can be used to identify an individual.
Harm	Any adverse effects that would be experienced by an individual (i.e., that may be socially, physically, or financially damaging) or an organization if the confidentiality of PII were breached.
Linkable Information	Information about or related to an individual for which there is a possibility of logical association with other information about the individual.
Linked Information	Information about or related to an individual that is logically associated with other information about the individual.
Obscured Data	Data that has been distorted by cryptographic or other means to hide information. It is also referred to as being masked or obfuscated.
Personally Identifiable Information (PII)	Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

DocuSign Envelope ID: B343C3D8-7304-4047-B6A6-E921DAFA2462

PII Confidentiality Impact Level	The PII confidentiality impact level—low, moderate, or high—indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.
Privacy Impact Assessment (PIA)	An analysis of how information is handled that ensures handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determines the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks.
System of Records	A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
Traceable	Information that is sufficient to make a determination about a specific aspect of an individual's activities or status
Program Participants	Issuers, subservicers, document custodians, contractors, subcontractors, and funds custodians

8.2 AUTHORITIES AND REFERENCES:

- Privacy Act, Public Law 93-579, December 1974.
- Office of Management and Budget (OMB), Circular A-130, Managing Information as a Strategic Resource, July 28, 2016.
- Office of Management and Budget (OMB), Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 2003.
- Office of Management and Budget (OMB), Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Minimum Security Requirements for Federal Information and Information Systems, and controls.
- Federal Information Security Modernization Act (FISMA) of 2014.
- Office of Management and Budget (OMB), Memorandum M-20-04, Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements, November 19, 2019.
- Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.
- Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.
- Federal Information Processing Standards (FIPS) 201-1, Personal Identity Verification for Federal Employees and Contractors, March 2006.
- Handbook for Safeguarding Sensitive PII Privacy Policy Directive 047-01-007, Revision 3 published by DHS Privacy Office, December 2017.
- The Trade Secrets Act, 18 U.S.C. § 1905.
- HUD Privacy Act Handbook 1325.1 Rev. 1.0

DocuSign Envelope ID: 93C53609-7F1E-4809-AAC1-EBA805EA3DF2

425 3rd Street, SW,
Washington, DC 20024
www.ginniemae.gov