APPENDIX III-29 INSTRUCTIONS
GOVERNMENT NATIONAL MORTGAGE ASSOCIATION
SYSTEMS ACCESS FORMS

Applicability: Ginnie Mae I MBS Program and Ginnie Mae II MBS Program.

Purpose: To obtain access to Ginnie Mae's Systems in order to access business applications that are used by program participants to conduct business with Ginnie Mae.

Prepared by: Issuer and Document Custodian

Distribution: Please return the completed and signed form to:

Ginnie Mae Security Administrator
Ginnie Mae Relationship Services
C/O The Bank of New York
101 Barclay Street - 8 East
New York, NY 10286-0001

Completed forms should be scanned as a PDF document and emailed to ginniemae1@bnymellon.com :

Completion Instructions:

In order to register for access to the Ginnie Mae Systems, including the Ginnie Mae Enterprise Portal and Ginnie*NET*, all organizations will be required to designate at least two (2) security officers (SO), one SO for registering users into the new Portal and/or Ginnie*NET*, and a second SO to approve those users. This will provide the required separation of duties. Each SO must complete a Security Officer Registration Form. A Security Officer for any Ginnie Mae Issuer must be listed as an authorized signatory in the organization's Resolution of Board of Directors and Certificate of Authorized Signatures, or its equivalent ("form HUD-11702").

Each Issuer will be required to submit two Security Officer Registration Forms, advising who the two Security Officers are. Each Security Officer will fill out the form, sign it, and then give it to their Supervisor to review and sign. The Supervisor will pass the form to the organization's Authorized Officer, who must also be named on the form HUD 11702. After the Authorized Officer reviews and signs the form, he/she will send the completed form to the Ginnie Mae Security Administration office.

Upon receipt, Ginnie Mae's Security Administrator will validate the signature on the registration form against the signatures on the form HUD 11702. Once verified, Ginnie Mae's Security Administrator will register the SO in the Ginnie Mae portal registration system and/or GinnieNET as requested. One Ginnie Mae Security Administrator will add the Security Officer to the portal and another Security Administrator will approve the new Security Officer user. The Ginnie Mae Security Administrator will call the new Security Officer using the verified contact information, confirm the identity of the SO, and notify them of the ID and password by phone.

When the ID and password is received, the SO will be required to login with their new ID and system generated password. Once the login is successful, the SO will be prompted to enter a new password and answer 3 security questions. If the password is confirmed, the Portal will send a message back to the Ginnie Mae Security Administrator that the password has been changed.

Note that a representative from the Ginnie Mae Security Administrator office must create the initial SO in an organization. Additionally, the Ginnie Mae Security Administrators must have the fully completed paperwork as described previously before they can create the Security Officer. The Security Officer will be associated with a group type i.e. custodian, issuer, etc. This group type will be used to restrict types of roles that can be assigned by that organization's Security Officer.

(Note: Issuers are strongly encouraged to assign a backup SO in the event that one of the two primary Security Officers is unavailable.)

This appendix contains the following registration and request forms.

- Appendix III-29(A)-Issuer Security Officer Registration
- Appendix III-29(B)-Issuer User Registration
- Appendix III-29(C)- Custodian Security Officer Registration
- Appendix III-29(D)-Custodian User Registration
- Appendix III-29(E)-RSA SecurID Token Request

Ginnie Mae Systems Access
Issuer Security Officer Registration

Instructions:

(1) Complete the information in the box below – please print.
(2) Read the Rules of Behavior.
(3) Sign and date this registration request on page 4.
(4) Have an authorized officer sign the registration document on page 4.
(5) Mail the completed and signed form to:

Ginnie Mae Security Administrator
Ginnie Mae Relationship Services
The Bank of New York Mellon
101 Barclay - 8 East
New York, NY 10286-0000

Name of Issuer:	Issuer Number(s):	
Security Officer Last Name:	First Name:	Middle Name:
Name Suffix:	Prefix: (Mr., Ms., Mrs.)	Office Phone No.:
Office E-Mail:		Fax No.:

USER RULES OF BEHAVIOR

As a user of Ginnie Mae Systems, I understand that I am personally responsible for all use and any misuse of my user account and password. I understand that by accessing a U.S. Government information system, I must comply with the following requirements:

(1) Users must safeguard the information to which you have access at all times.

(2) The system may be used only in support of Ginnie Mae business.

(3) The system may not be used for any purpose other than those functions related to Ginnie Mae's business.

(4) The government reserves the right to monitor the activities of any user and/or any machine connected to Ginnie Mae Systems.

(5) The Ginnie Mae Systems and the information contained within are the property of the federal government. Ginnie Mae owns the data stored on these systems, including all messages and information, even those deemed personal.

(6) No data may be transmitted on the system that is more sensitive than the level for which that system has been approved.

(7) Information that was obtained via Ginnie Mae Systems may not be divulged outside of government channels without the express, written permission of the system owner.

(8) Any activity that would discredit Ginnie Mae, including, but not limited to, seeking, transmitting, collecting, or storing defamatory, discriminatory, sexually explicit, obscene, harassing, or intimidating messages or material, is prohibited.

(9) Any activity that violates Federal laws for information protection (e.g., reconnaissance techniques, hacking, phishing, spamming, etc.), is expressly prohibited. Violations will be turned over to the appropriate Federal law enforcement organization for prosecution.

(10) Ginnie Mae System user accounts are provided solely for the use of the individual for whom they were created. Passwords or any other authentication mechanism should never be shared or stored any place easily accessible. If a password is stored it may not be stored in a clear-text or readable format. Sharing of user accounts is grounds for terminating system access.

(11) Per Ginnie Mae Policy, GMEP has the following password format requirements:

Passwords must be at least eight (8) alphanumeric characters in length, and contain the following five (5) character types:

- Maximum twenty (20) characters in length;
- Must have at least one (1) English upper case letter (A, B, C, etc.);
- Must have at least one (1) English lower case letter (a, b, c, etc.);
- Must have at least one (1) Arabic number (0, 1, 2, 3, etc.);
- Must have at least one (1) special character from the following set: (! @#$%^&*()_+).

(12) Passwords should not be created using the following:

- Dictionary words or common names, such as Betty, Fred, Rover;
- Portions of associated account names, for example, user ID, login name;
- Consecutive character strings, such as abcdef, 123456;
- Simple keyboard patterns, such as asdfgh, qwerty;
- Generic passwords, such as a password consisting of a variation of the word "password" (e.g., P@ssword1).

(13) Passwords must be changed every ninety (90) days and should never be repeated.

(14) Password history will prevent users from using the same password from the previous (24) password changes.

(15) After three (3) invalid password attempts, the user account will be locked. The user must contact the appropriate Help Desk or Security Officer in person for identification verification and to unlock the account.

(16) The Security Officer must approve and authorize the employee's level of access in writing via documented account management procedures. The Security Officer is responsible for maintaining records of user requests for system access, including completed Appendix III-29 forms.

(17) The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), pre-public release information such as economic indicators, proprietary data, or export controlled software or data is

prohibited. All use of copyrighted software must comply with copyright laws and license agreements.

(18) Remote off-site, (e.g., dial-in, VPN) access to GMEP Administrative Functions must be approved and authorized in writing by the appropriate management authority and the Ginnie Mae Information System Security Officer.

(19) Authorized users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time.

(20) At no time should personally owned equipment be connected to the system.

(21) Any security problems or password compromises must be reported immediately to the Ginnie Mae Security Administrator.

(22) I understand that Federal law provides for punishment under Title 18, U.S. Code, including a fine and up to ten (10) years in jail for the first offense for anyone who commits any of the following violations:

- Knowingly accesses an information system without authorization, or exceeds authorized access, and obtains information that requires protection against unauthorized disclosure.
- Intentionally, without authorization, accesses a government information system and impacts the government's operation, including availability of that system.
- Intentionally accesses a government information system without authorization, and alters, damages, or destroys information therein.
- Prevents authorized use of the system or accesses a government information system without authorization, or exceeds authorized access, and obtains anything of value.

(23) Screensavers must be password protected.

(24) Movable media, (such as diskettes, CD-ROMs, and Zip disks) that contain sensitive and/or official information must be secured when not in use.

(25) When the user no longer has a legitimate need to access the system, the user's Supervisor must notify the Security Officer immediately in writing so that access can be terminated. The Security Officer will notify the Ginnie Mae Security Administrator.

(26) Upon initial login I will be required to select and answer three (3) Security questions for future use to change or reset my password.

(27) If Ginnie Mae or the Security Administrator issues a one-time password token (e.g. RSA SecurID Tokens) or other secondary authentication device, you accept the responsibilities and obligations presented on the forms and documents provided when the device is issued. This includes but is not limited to initiation, usage, storage, return, and reporting procedures for the authentication device.

Actions violating any of these rules will result in immediate termination of your assigned identifier/password from the system.

SECURITY OFFICER CERTIFICATION:

I have read the above statement of policy regarding system security awareness and practices when accessing Ginnie Mae System's information resources, including GMEP and Ginnie*NET*. I understand the policies as set forth above, and I agree to comply with these requirements as a condition of being granted limited access to the Ginnie Mae's computer resources. I certify that I have been designated as an authorized Security Officer by my organization and will abide by all of the policies and rules as set forth by Ginnie Mae. I will make sure that I only assign Ginnie Mae IDs to active employees and to the best of my knowledge there will be no sharing of IDs. I understand that all accounts will be accessing government information systems. I agree to deactivate users when they leave my company, go on extended leave, are reassigned to other positions, etc. where their Ginnie Mae access is no longer needed.

I recognize that a violation of this certification could result in disciplinary action against my organization.

Certified By:

_____ _____

Security Officer Signature **Date**

AUTHORIZED SIGNATURE CERTIFICATION:

I hereby certify that I am authorized and empowered in the name of and on behalf of this corporation to act on behalf of my company and designate a Security Officer for my organization who will abide by all of the policies and rules as set forth by Ginnie Mae. I further authorize and empower the above named Security Officer to register other employees in my organization as Security Officers within Ginnie Mae's portal, as needed. I understand that all accounts will be accessing government information systems.

I recognize that a violation of this certification could result in disciplinary action against my organization.

Approved By:

_____ _____

Name of Authorized Officer **Title of Officer**

_____ _____

Signature of Authorized Officer **Date** **Officer Phone Number**

GINNIE MAE SECURITY ADMINISTRATORS' CERTIFICATION:

☐ **Authorized signer called-back**

☐ **11702 Signature verified**

_____
1st Security Administrator Name

_____
1st Security Administrator Phone No.

_____
1st Security Administrator Signature

_____
Date

☐ **Security Officer Registration Approved**

☐ **Security Officer added to Portal**

_____
2nd Security Administrator Name

_____
2nd Security Administrator Phone No.

_____
2nd Security Administrator Signature

_____
Date

Ginnie Mae Systems Access
Issuer User Registration

Instructions

(1) Complete the information in the boxes below – please print.
(2) Select the requested roles(s).
(3) Read the Rules of Behavior.
(4) Sign and date this registration request.
(5) Have your supervisor sign this registration request.
(6) Submit this request to your Security Officer for processing.

Organization:	
Prefix (Mr., Ms., Mrs.):	
First Name:	
Middle Name:	
Last Name:	
Suffix:	
Office Phone Number:	
Office Email:	
Fax Number:	

Select Roles (Select All That Apply):

RFS User Roles

☐ Upload & Exception Feedback User	☐ Pool Accounting User	☐ SCRA User	☐ GPADS User	☐ HMBS User	☐ e-Notification User	☐ IOPP User
Exception feedback	Pool Accounting - Single Family	Servicemembers Civil Relief Act (SCRA)	Issuer feedback	Pool accounting and reporting	Communication of system generated announcements	Issuer Feedback
Matching and Suspense (MAS)	Pool Accounting – Multifamily/Multifamily Prepayment Penalty Report (MFPP)	File upload				
File upload	Exception feedback					
	CAV Report					
	Matching and Suspense (MAS)					
	File upload					

IPMS User Roles

☐ RPN Issuer	☐ CM Issuer	☐ PTS Issuer	☐ SecurID Token Holder
Enter pool number request	View requests and reports	*Selling Issuer*: Submit request for Transfer	Enables the user to activate a Ginnie Mae Issued SecurID Token for use in Ginnie Mae systems and applications. SecurID Tokens may be requested using the form found in Appendix III-29(E) below. This role may only be granted to individuals who are listed on this entity's Form HUD-11702.
Request maximum pool number calculation override	Request commitment and accept commitment fee	*Buying Issuer*: Accept and authorize Transfer	
View reports			
☐ MAMS Issuer	☐ MAMS Subservicer	☐ MAMS Participation Agent	☐ SecurID Temporary Bypass
Search and view agreements and reports	View HUD-11707 agreements in which Issuer is Subservicer	View HUD-11703-II agreements in which Issuer is Subservicer	Token holders authenticate if they have forgotten or lost their token
Create and submit agreements	Search HUD-11707 agreements in which Issuer is Subservicer	Search HUD-11703-II agreements in which Issuer is Subservicer	
Upload documents	Submit HUD-11707 agreements in which Issuer is Subservicer	Submit HUD-11703-II agreements in which Issuer is Subservicer	

GINNIENET USER ROLES

Section 1. Roles assigned within Ginnie*NET* : Assigning any of the roles in this Section 1, enables the user to edit and view data in GinnieNET, but does not enable the user to submit data or documents through Ginnie*NET*. To enable the user to also submit data or documents through Ginnie*NET*, the user must be able to perform the SecurID Token Authentication Process in GinnieNET. The SecurID Authentication process requires a SecurID Token, and the user must have been assigned the "SecurID Token Holder" and "Authorized GinnieNET Signer Role" in Section 2 of this page in addition to one or more roles in this Section 1.

- ☐ **Single and Multifamily Issuer**.
- ☐ **Single Family Issuer**
- ☐ **Multifamily Issuer**
- ☐ **HECM Issuer**
- ☐ **Investor Reporting**
- ☐ **Certification**

Section 2. Roles assigned within GMEP to Enable User's SecurID Token to function in GinnieNET.

- ☐ **SecurID Token Holder Role—**Enables the user to activate a Ginnie Mae Issued SecurID Token for use in Ginnie Mae systems and applications. SecurID Tokens may be requested using the form found in Appendix III-29(E) below. This role may only be granted to individuals who are listed on this entity's Form HUD-11702.
- ☐ **Authorized Ginnie*NET* Signer Role—**Enables SecurID Token Holders to use their Ginnie Mae –issued SecurID Token to perform the authentication process required to submit data or documents through GinnieNET. This role may only be granted to individuals who are listed on this entity's Form HUD-11702.

USER RULES OF BEHAVIOR

As a user of Ginnie Mae Systems, I understand that I am personally responsible for my use and any misuse of my user account and password. I understand that by accessing a U.S. Government information system that I must comply with the following requirements:

(1) Users must safeguard the information to which you have access at all times.

(2) The system may be used only in support of Ginnie Mae business.

(3) The system may not be used for any purpose other than those functions related to Ginnie Mae's business.

(4) The government reserves the right to monitor the activities of any user and/or any machine connected to Ginnie Mae Systems.

(5) The Ginnie Mae Systems and the information contained within are the property of the federal government. Ginnie Mae owns the data stored on these systems, including all messages and information, even those deemed personal.

(6) No data may be transmitted on the system that is more sensitive than the level for which that system has been approved.

(7) Information that was obtained via Ginnie Mae Systems may not be divulged outside of government channels without the express, written permission of the system owner.

(8) Any activity that would discredit Ginnie Mae, including, but not limited to, seeking, transmitting, collecting, or storing defamatory, discriminatory, sexually explicit, obscene, harassing, or intimidating messages or material, is prohibited.

(9) Any activity that violates Federal laws for information protection (e.g., reconnaissance techniques, hacking, phishing, spamming, etc.), is expressly prohibited. Violations will be turned over to the appropriate Federal law enforcement organization for prosecution.

(10) Ginnie Mae Systems' user accounts are provided solely for the use of the individual for whom they were created. Passwords or any other authentication mechanism should never be shared or stored any place easily accessible. If a password is stored it may not be stored in a clear-text or readable format. Sharing of user accounts is grounds for terminating system access.

(11) Per Ginnie Mae Policy, GMEP has the following password format requirements:

Passwords must be at least eight (8) alphanumeric characters in length, and contain the following five (5) character types:

- Maximum twenty (20) characters in length;
- Must have at least one (1) English upper case letter (A, B, C, etc.);
- Must have at least one (1 English lower case letter (a, b, c, etc.);
- Must have at least one (1) Arabic number (0, 1, 2, 3, etc.);
- Must have at least one (1) special character from the following set: (! @#$%^&*()_+).

(12) Passwords should not be created using the following:

- Dictionary words or common names, such as Betty, Fred, Rover;
- Portions of associated account names, for example, user ID, login name;

- Consecutive character strings, such as abcdef, 123456;
- Simple keyboard patterns, such as asdfgh, qwerty;
- Generic passwords, such as a password consisting of a variation of the word "password" (e.g., P@ssword1).

(13) Passwords must be changed every ninety (90) days and should never be repeated.

(14) Password history will prevent users from using the same password from the previous (24) password changes.

(15) After three (3) invalid password attempts, the user account will be locked. The user must contact the appropriate Help Desk or Security Officer in person for identification verification and to unlock the account.

(16) The user's Supervisor and Security Officer must authorize and approve the employee's level of access in writing via documented account management procedures.

(17) The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), pre-public release information such as economic indicators, proprietary data, or export controlled software or data is prohibited. All use of copyrighted software must comply with copyright laws and license agreements.

(18) Remote off-site (e.g., dial-in, VPN) access to GMEP Administrative Functions must be approved and authorized in writing by the appropriate management authority and the Ginnie Mae Information System Security Officer.

(19) Authorized users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time.

(20) At no time should personally owned equipment be connected to the system.

(21) Any security problems or password compromises must be reported immediately to the appropriate Help Desk or Security Officer.

(22) I understand that Federal law provides for punishment under Title 18, U.S. Code, including a fine and up to ten (10) years in jail for the first offense for anyone who commits any of the following violations:

- Knowingly accesses an information system without authorization, or exceeds authorized access, and obtains information that requires protection against unauthorized disclosure.
- Intentionally, without authorization, accesses a government information system and impacts the government's operation, including availability of that system.
- Intentionally accesses a government information system without authorization, and alters, damages, or destroys information therein.
- Prevents authorized use of the system or accesses a government information system without authorization, or exceeds authorized access, and obtains anything of value.

(23) Screen-savers must be password protected.

(24) Movable media, (such as diskettes, CD-ROMs, and Zip disks), that contain sensitive and/or official information must be secured when not in use.

(25) When the user no longer has a legitimate need to access the system, the user must notify his/her Supervisor. The Supervisor must notify the Security Officer immediately in writing so that access can be terminated. The Security Officer will notify the Ginnie Mae Security Administrator.

(26) Upon initial login I will be required to select and answer three (3) Security questions for future use to change or reset my password.

(27) If your Security Officer issues a one-time password token (e.g. RSA Token) or other secondary authentication device, you accept the responsibilities and obligations presented on the forms and documents provided when the device is issued. This includes but is not limited to initiation, usage, storage, return, and reporting procedures for the authentication device.

Actions violating any of these rules will result in immediate termination of your assigned identifier/password from the system.

USER CERTIFICATION:

I have read the above statement of policy regarding system security awareness and practices when accessing Ginnie Mae System's information resources, including GMEP and GinnieNet. I understand the policies as set forth above, and I agree to comply with these requirements as a condition of being granted limited access to the Ginnie Mae's computer resources.

User Signature **Date**

SUPERVISOR CERTIFICATION:

I certify that I have been designated as an authorized Supervisor to approve user registration forms by my organization and will abide by all of the policies and rules as set forth by Ginnie Mae. I will make sure that I only assign active employees as users and to the best of my knowledge there will be no sharing of IDs. I will verify the identity of the user by the approved listing of identification. I understand that all accounts will be accessing government information systems.

I recognize that a violation of this certification could result in disciplinary action against my organization.

☐ **Verify User Phone number** ☐ **Verify User E-Mail address**

CERTIFIED BY:

Supervisor Name **Supervisor Phone Number**

Supervisor Signature **Date**

FOR SECURITY OFFICER USE ONLY

SECURITY OFFICER CERTIFICATION:

☐ **Authorized Supervisor Called-Back**

☐ **Verified User and Permissions**

_____ _____

1st Security Officer Name **Officer Phone Number**

_____ _____

1st Security Officer Signature **Date**

☐ **User Registration Approved**

☐ **User Added to the Portal**

_____ _____

2nd Security Officer Name **Officer Phone Number**

_____ _____

2nd Security Officer Signature **Date**

Ginnie Mae Systems Access
Custodian Security Officer Registration

Instructions:

(1) Complete the information in the box below – please print.
(2) Read the Rules of Behavior.
(3) Sign and date this registration request on page 4.
(4) Have an authorized officer sign the registration document on page 4.
(5) Mail the completed and signed form to:

Ginnie Mae Security Administrator
Ginnie Mae Relationship Services
The Bank of New York Mellon
101 Barclay - 8 East
New York, NY 10286-0000

Organization Name:	Custodian Number(s):	
Security Officer Last Name:	First Name:	Middle Name:
Name Suffix:	Prefix: (Mr., Ms., Mrs.)	Office Phone No.:
Office E-Mail:		Fax No.:

RULES OF BEHAVIOR

As a user of Ginnie Mae Systems, I understand that I am personally responsible for all use and any misuse of my user account and password. I understand that by accessing a U.S. Government information system, I must comply with the following requirements:

(1) Users must safeguard the information to which you have access at all times.

(2) The system may be used only in support of Ginnie Mae business.

(3) The system may not be used for any purpose other than those functions related to Ginnie Mae's business.

(4) The government reserves the right to monitor the activities of any user and/or any machine connected to Ginnie Mae Systems

(5) The Ginnie Mae Systems and the information contained within are the property of the federal government. Ginnie Mae owns the data stored on these systems, including all messages and information, even those deemed personal.

(6) No data may be transmitted on the system that is more sensitive than the level for which that system has been approved.

(7) Information that was obtained via Ginnie Mae Systems may not be divulged outside of government channels without the express, written permission of the system owner.

(8) Any activity that would discredit Ginnie Mae, including, but not limited to, seeking, transmitting, collecting, or storing defamatory, discriminatory, sexually explicit, obscene, harassing, or intimidating messages or material, is prohibited.

(9) Any activity that violates Federal laws for information protection (e.g., reconnaissance techniques, hacking, phishing, spamming, etc.) is expressly prohibited. Violations will be turned over to the appropriate Federal law enforcement organization for prosecution.

(10) Ginnie Mae Systems'user accounts are provided solely for the use of the individual for whom they were created. Passwords or any other authentication mechanism should never be shared or stored any place easily accessible. If a password is stored it may not be stored in a clear-text or readable format. Sharing of user accounts is grounds for terminating system access.

(11) Per Ginnie Mae Policy, GMEP has the following password format requirements:

Passwords must be at least eight (8) alphanumeric characters in length, and contain the following five (5) character types:

- Maximum twenty (20) characters in length;
- Must have at least one (1) English upper case letter (A, B, C, etc.);
- Must have at least one (1) English lower case letter (a, b, c, etc.);
- Must have at least one (1) Arabic number (0, 1, 2, 3, etc.);
- Must have at least one (1) special character from the following set: (! @#$%^&*()_+).

(12) Passwords should not be created using the following:

- Dictionary words or common names, such as Betty, Fred, Rover;
- Portions of associated account names, for example, user ID, login name;
- Consecutive character strings, such as abcdef, 123456;
- Simple keyboard patterns, such as asdfgh, qwerty;
- Generic passwords, such as a password consisting of a variation of the word "password" (e.g., P@ssword1).

(13) Passwords must be changed every ninety (90) days and should never be repeated.

(14) Password history will prevent users from using the same password from the previous (24) password changes.

(15) After three (3) invalid password attempts, the user account will be locked. The user must contact the Ginnie Mae Information System Security Officer to unlock the account.

(16) The Security Officer must approve and authorize the Security Administrator's level of access in writing via documented account management procedures. The Security Officer is responsible for maintaining records of user requests for system access, including completed Appendix III-29 forms.

(17) The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), pre-public release information such as economic indicators, proprietary data, or export controlled software or data is prohibited. All use of copyrighted software must comply with copyright laws and license agreements.

(18) Remote off-site, (e.g., dial-in, VPN) access to GMEP Administrative Functions must be approved and authorized in writing by the appropriate management authority and the Ginnie Mae Information System Security Officer.

(19) Authorized users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time.

(20) At no time should personally owned equipment be connected to the system.

(21) Any security problems or password compromises must be reported immediately to the Ginnie Mae Security Administrator.

(22) I understand that Federal law provides for punishment under Title 18, U.S. Code, including a fine and up to ten (10) years in jail for the first offense for anyone who commits any of the following violations:

- Knowingly accesses an information system without authorization, or exceeds authorized access, and obtains information that requires protection against unauthorized disclosure.
- Intentionally, without authorization, accesses a government information system and impacts the government's operation, including availability of that system.
- Intentionally accesses a government information system without authorization, and alters, damages, or destroys information therein.
- Prevents authorized use of the system or accesses a government information system without authorization, or exceeds authorized access, and obtains anything of value.

(23) Screensavers must be password protected.

(24) Movable media, (such as diskettes, CD-ROMs, and Zip disks) that contain sensitive and/or official information must be secured when not in use.

(25) When the user no longer has a legitimate need to access the system, the user's Supervisor must notify the Security Officer immediately in writing so that access can be terminated. The Security Officer will notify the Ginnie Mae Security Administrator.

(26) Upon initial login I will be required to select and answer three (3) Security questions for future use to change or reset my password.

(27) If Ginnie Mae or the Security Administrator issues a one-time password token (e.g. RSA Tokens) or other secondary authentication device, you accept the responsibilities and obligations presented on the forms and documents provided when the device is issued. This includes but is not limited to initiation, usage, storage, return, and reporting procedures for the authentication device.

Actions violating any of these rules will result in immediate termination of your assigned identifier/password from the system.

SECURITY OFFICER CERTIFICATION:

I have read the above statement of policy regarding system security awareness and practices when accessing Ginnie Mae System's information resources, including GMEP and Ginnie*NET*. I understand the policies as set forth above, and I agree to comply with these requirements as a condition of being granted limited access to the Ginnie Mae's computer resources. I certify that I have been designated as an authorized Security Officer by my organization and will abide by all of the policies and rules as set forth by Ginnie Mae. I will make sure that I only assign Ginnie Mae IDs to active employees and to the best of my knowledge there will be no sharing of IDs. I understand that all accounts will be accessing government information systems. I agree to deactivate users when they leave my company, go on extended leave, are reassigned to other positions, etc. where their Ginnie Mae access is no longer needed.

I recognize that a violation of this certification could result in disciplinary action against my organization.

Certified By:

_____ _____

Security Officer Signature **Date**

AUTHORIZED SIGNATURE CERTIFICATION:

I hereby certify that I am authorized and empowered in the name of and on behalf of this corporation to act on behalf of my company and designate a Security Officer for my organization who will abide by all of the policies and rules as set forth by Ginnie Mae. I further authorize and empower the above named Security Officer to register other employees in my organization as Security Officers within Ginnie Mae's portal, as needed. I understand that all accounts will be accessing government information systems.

I recognize that a violation of this certification could result in disciplinary action against my organization.

Approved By:

_____ _____

Name of Authorized Officer **Title of Officer**

_____ _____

Signature of Authorized Officer **Date** **Officer Phone Number**

GINNIE MAE SECURITY ADMINISTRATOR CERTIFICATION:

☐ **Authorized signer called-back**

1st Security Administrator Name	**Administrator Phone No.**
1st Security Administrator Signature	**Date**

☐ **Security Officer Registration Approved** ☐ **Security Officer added to Portal**

2nd Security Administrator Name	**Administrator Phone No.**
2nd Security Administrator Signature	**Date**

Ginnie Mae Systems Access
Custodian User Registration

Instructions

(1) Complete the information in the boxes below – please print.
(2) Select the requested roles(s).
(3) Read the User Rules of Behavior.
(4) Sign and date this registration request.
(5) Have your supervisor sign this registration request.
(6) Submit this request to your Security Officer for processing.

Organization Name:		
User Last Name:	First Name:	Middle Name:
Name Suffix:	Prefix: (Mr., Ms., Mrs.)	Office Phone No.:
Office E-Mail:		Fax No.:

Select Roles (Select All That Apply):

Section 1. GMEP Only Users

☐ **MAMS Document Custodian User**	☐ **PTS Document Custodian Report Access**
Access to retain the physical document of the Master Agreement.	Access to view reports.
☐ **SecurID Token Holder**	☐ **eNotification User**
Provide means for users to test their token access.	e-Notification (eN)
☐ **SecurID Temporary Bypass**	
Provide means for token holder to authenticate if they have forgotten or lost their token.	

Section 2. GinnieNET Users

GinnieNET Role Basic Access:	**GinnieNET Authorized Signer**
☐ **Custodian Role:** allows user to edit and view data in GinnieNET only. Role assignment is made within GinnieNET.	☐ **GinnieNET Authorized Signer:** allows user to submit certifications and process requests for release of loan documents (HUD-11708). Must be assigned within GMEP. User must also have SecurID Token Holder Role in Section 1.

USER RULES OF BEHAVIOR

As a user of Ginnie Mae Systems, I understand that I am personally responsible for all use and any misuse of my user account and password. I understand that by accessing a U.S. Government information system, I must comply with the following requirements:

(1) Users must safeguard the information to which you have access at all times.

(2) The system may be used only in support of Ginnie Mae business.

(3) The system may not be used for any purpose other than those functions related to Ginnie Mae's business.

(4) The government reserves the right to monitor the activities of any user and/or any machine connected to Ginnie Mae Systems.

(5) Ginnie Mae Systems and the information contained within are the property of the federal government. Ginnie Mae owns the data stored on these systems, including all messages and information, even those deemed personal.

(6) No data may be transmitted on the system that is more sensitive than the level for which that system has been approved.

(7) Information that was obtained via Ginnie Mae Systems may not be divulged outside of government channels without the express, written permission of the system owner.

(8) Any activity that would discredit Ginnie Mae, including, but not limited to, seeking, transmitting, collecting, or storing defamatory, discriminatory, sexually explicit, obscene, harassing, or intimidating messages or material, is prohibited.

(9) Any activity that violates Federal laws for information protection (e.g., reconnaissance techniques, hacking, phishing, spamming, etc.), is expressly prohibited. Violations will be turned over to the appropriate Federal law enforcement organization for prosecution.

(10) Ginnie Mae Systems' user accounts are provided solely for the use of the individual for whom they were created. Passwords or any other authentication mechanism should never be shared or stored any place easily accessible. If a password is stored it may not be stored in a clear-text or readable format. Sharing of user accounts is grounds for terminating system access.

(11) Per Ginnie Mae Policy, GMEP has the following password format requirements:

Passwords must be at least eight (8) alphanumeric characters in length, and contain the following five (5) character types:

- Maximum twenty (20) characters in length;
- Must have at least one (1) English upper case letter (A, B, C, etc.);
- Must have at least one (1) English lower case letter (a, b, c, etc.);
- Must have at least one (1) Arabic number (0, 1, 2, 3, etc.);
- Must have at least one (1) special character from the following set: (! @#$%^&*()_+).

(12) Passwords should not be created using the following:

- Dictionary words or common names, such as Betty, Fred, Rover;
- Portions of associated account names, for example, user ID, login name;
- Consecutive character strings, such as abcdef, 123456;

- Simple keyboard patterns, such as asdfgh, qwerty;
- Generic passwords, such as a password consisting of a variation of the word "password" (e.g., P@ssword1).

(13) Passwords must be changed every ninety (90) days and should never be repeated.

(14) Password history will prevent users from using the same password from the previous (24) password changes.

(15) After three (3) invalid password attempts, the user account will be locked. The user must contact the appropriate Help Desk or Security Officer in person for identification verification and to unlock the account.

(16) The user's Supervisor and Security Officer must authorize and approve the employee's level of access in writing via documented account management procedures.

(17) The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), pre-public release information such as economic indicators, proprietary data, or export controlled software or data is prohibited. All use of copyrighted software must comply with copyright laws and license agreements.

(18) Remote off-site, (e.g., dial-in, VPN) access to GMEP Administrative Functions must be approved and authorized in writing by the appropriate management authority and the Ginnie Mae Information System Security Officer.

(19) Authorized users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time.

(20) At no time should personally owned equipment be connected to the system.

(21) Any security problems or password compromises must be reported immediately to the appropriate Help Desk or Security Officer.

(22) I understand that Federal law provides for punishment under Title 18, U.S. Code, including a fine and up to ten (10) years in jail for the first offense for anyone who commits any of the following violations:

- Knowingly accesses an information system without authorization, or exceeds authorized access, and obtains information that requires protection against unauthorized disclosure.
- Intentionally, without authorization, accesses a government information system and impacts the government's operation, including availability of that system.
- Intentionally accesses a government information system without authorization, and alters, damages, or destroys information therein.
- Prevents authorized use of the system or accesses a government information system without authorization, or exceeds authorized access, and obtains anything of value.

(23) Screen-savers must be password protected.

(24) Movable media, (such as diskettes, CD-ROMs, and Zip disks), that contain sensitive and/or official information must be secured when not in use.

(25) When the user no longer has a legitimate need to access the system, the user must notify his/her Supervisor. The Supervisor must notify the Security Officer immediately in writing so that access can be terminated. The Security Officer will notify the Ginnie Mae Security Administrator.

(26) Upon initial login I will be required to select and answer three (3) Security questions for future use to change or reset my password.

(27) If your Security Officer issues a one-time password token (e.g. RSA Token) or other secondary authentication device, you accept the responsibilities and obligations presented on the forms and documents provided when the device is issued. This includes but is not limited to initiation, usage, storage, return, and reporting procedures for the authentication device.

Actions violating any of these rules will result in immediate termination of your assigned identifier/password from the system.

USER CERTIFICATION:

I have read the above statement of policy regarding system security awareness and practices when accessing Ginnie Mae System's information resources, including GMEP and Ginnie*NET*. I understand the policies as set forth above, and I agree to comply with these requirements as a condition of being granted limited access to the Ginnie Mae's computer resources.

User Signature **Date**

SUPERVISOR CERTIFICATION:

I certify that I have been designated as an authorized Supervisor to approve user registration forms by my organization and will abide by all of the policies and rules as set forth by Ginnie Mae. I will make sure that I only assign active employees as users and to the best of my knowledge there will be no sharing of IDs. I will verify the identity of the user by the approved listing of identification. I understand that all accounts will be accessing government information systems.

I recognize that a violation of this certification could result in disciplinary action against my organization.

☐ **Verify User Phone number** ☐ **Verify User E-Mail address**

CERTIFIED BY:

Supervisor Name **Supervisor Phone Number**

Supervisor Signature **Date**

FOR SECURITY OFFICER USE ONLY

SECURITY OFFICER CERTIFICATION:

☐ **Authorized Supervisor Called-Back**

☐ **Verified User and Permissions**

_____ _____

1st Security Officer Name **Officer Phone Number**

_____ _____

1st Security Officer Signature **Date**

☐ **User Registration Approved**

☐ **User Added to the Portal**

_____ _____

2nd Security Officer Name **Officer Phone Number**

_____ _____

2nd Security Officer Signature **Date**

Ginnie Mae Systems Access
RSA SecurID Token Request

User(s) requesting an RSA SecurID token must be an authorized signer, as determined by the Issuer's form HUD 11702 – Resolution of Board of Directors and Certificate of Authorized Signatures.

General Instructions for completing RSA SecurID Token Order Form

(1) Complete all of the information in the boxes below- please print.

(2) Submit this request to your Security Officer for processing. The Security Officer must return the completed form via e-mail to Ginniemae1@bnymellon.com.

Additional Instructions for Section I

(1) Check the box in front of the action being requested: "New" requests for a token, "Add" personnel who need a token, "Delete" personnel who no longer need a token, or "Replace" a lost or damaged token.

Additional Instructions for Section II

(1) Enter the address of the Security Officer for receipt and distribution of the RSA SecurID Token Setup Package

Additional Instructions for Section III

(1) Enter the User's Full Name and GMEP User ID (Generated from the Portal)

(2) Signature of user requesting the token. The signatures represent the personnel designated by the Issuer or Custodian to sign on behalf of the Issuer or Custodian in the capacity of an Authorized Signer.

(3) Leave blank the fields under the column labeled "Token Serial No."

Note: Ginnie Mae's Pool Processing Agent will enter the token serial number for each user after the Security Officer submits this request by email.

Additional Instructions for Section IV

(1) This section will be completed by Ginnie Mae's Pool Processing Agent.

SecurID Token Order Form

For Ginnie Mae Use Only:
RSA SecurID Company ID: _____
Date: _____

Section I—Action Requested and Company Information

☐New ☐Add ☐ Delete ☐ Replace Lost/Damage

Ginnie Mae 4 digit Issuer Number: Or 6 digit Custodian Number:	**Company Name:**

Section II – Security Office Information:

Name: Security Officer GMEP ID:	Telephone:
Address:	Email address:
City State ZIP	

Section III – Token Card Authentication

Note for Issuers - The user requesting the RSA Token must be an authorized signatory on the form HUD 11702 and must use the RSA tokens for authentication when making submissions.

Full Name	GMEP User ID	Signature	Token Serial No. For Ginnie Mae Use Only

Section IV – Approvals For Ginnie Mae Use Only

RSA SecurID Company ID: Token Serial Assigned#

Name (Please Print):	Initials:	Date:	**Signature**
GNMA - PPA Administrator:			