APPENDIX III-29
GOVERNMENT NATIONAL MORTGAGE ASSOCIATION ENTERPRISE PORTAL (GMEP) REGISTRATION FORMS

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

Purpose: To obtain access to Ginnie Mae's Enterprise Portal in order to access systems and meet reporting requirements.

Prepared by: Issuer and document custodians.

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 can be faxed to:

Ginnie Mae Security Administrator
(212) 313-0132
Note: Completed forms with original signatures must be mailed and received before the Security Officer ID can be activated.

Completion Instructions:

In order to register for access to the Ginnie Mae Enterprise Portal, all organizations will be required to designate at least two (2) security officers (SO), one for registering users into the new Portal, and a second to approve those users. This will provide the required separation of duties. Each SO must complete the Security Officer portal registration form.

Each organization will be required to submit two Security Officer portal 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 Resolution of Board of Directors and Certificate of Authorized Signatures ("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, a Ginnie Mae's Security Administrator will register the Security Officer in the Ginnie Mae portal registration system. 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.)

Ginnie Mae Enterprise Portal (GMEP)
User Registration for Issuer ONLY
(Please Print Details Below)

Name of Issuer:		Issuer Number:
Last Name:	First Name:	Middle:
Name Suffix:	Prefix: (Mr., Ms., Mrs., Miss)	Office Phone No.:
Office Email:		Fax No.:

Select Roles (Select all that apply):

☐	HMBS User	☐	Upload & Exception Feedback User	☐	SCRA User
☐	GPADS User	☐	Pool Accounting User	☐	e-Notification User

User's Rules of Behavior

As a user of the GMEP, 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:
   a. Safeguard the information to which you have access at all times.
   b. Obtain your supervisor's written approval prior to taking any Ginnie Mae sensitive information home or otherwise away from the office. The supervisor's approval must identify the business necessity for removing such information.
   c. Adhere to the security policies and procedures when approval is granted to take sensitive information home or away from the office. This includes compliance with applicable Federal Information Processing Standards (FIPS), such as encryption of data obtained from or destined to be processed by GMEP.
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 GMEP.
5. The GMEP 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 GMEP 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 law (e.g., reconnaissance techniques, hacking, phishing, spamming, etc) is prohibited. Violations will be turned over to the appropriate Federal law enforcement organization for prosecution.
10. GMEP 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 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 60 days and a password history will prevent you from using the same password from the previous 13 password changes.
14. After three 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.
15. The user's Supervisor and Security Officer must authorize and approve the employee's level of access in writing via documented account management procedures.
16. 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.
17. Remote off-site (e.g., dial-in) access to a computer system must be approved and authorized in writing by the appropriate management authority and the system owner.
18. Authorized users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time.

19. Only devices that are formally certified and approved by the system owner shall be connected to the GMEP. At no time should personally owned equipment be connected to the system.
20. Any security problems or password compromises must be reported immediately to the appropriate Help Desk or Security Officer.
21. I understand that Federal law provides for punishment under Title 18, U.S. Code, including a fine and up to 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.
22. Screen-savers must be password protected.
23. Movable media (such as diskettes, CD-ROMs, and Zip disks) that contain sensitive and/or official information must be secured when not in use.
24. 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.
25. Upon initial log-on I will be required to select and answer three security questions for future use to change or reset my password.

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 GMEP's information resources. 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 Phone number** ☐ **Verify Email 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 Enterprise Portal (GMEP)
Security Officer Registration for Issuer ONLY
(Please Print Details Below)

Name of Issuer:			Issuer Number:
Security Officer Last Name:	First Name:		Middle:
Name Suffix:	Prefix: (Mr., Ms., Mrs., Miss)	Office Phone No.:	
Office Email:			Fax No.:

Rules of Behavior

As a user of the GMEP, 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:
   a. Safeguard the information to which you have access at all times.
   b. Obtain your supervisor's written approval prior to taking any Ginnie Mae sensitive information home or otherwise away from the office. The supervisor's approval must identify the business necessity for removing such information.
   c. Adhere to the security policies and procedures when approval is granted to take sensitive information home or away from the office.
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 GMEP.
5. The GMEP 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 GMEP 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 law (e.g., reconnaissance techniques, hacking, phishing, spamming, etc) is prohibited. Violations will be turned over to the appropriate Federal law enforcement organization for prosecution.

10. GMEP 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 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 60 days and should never be repeated.
14. Password history will prevent users from using the same password from the previous 13 password changes.
15. After three 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.
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) access to a computer system must be approved and authorized in writing by the appropriate management authority and the system owner.
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. Only devices that are formally certified and approved by the system owner shall be connected to the GMEP. 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 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'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 log-on I will be required to select and answer three security questions for future use to change or reset my password.

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 GMEP's information resources. 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 also certify that I am an authorized officer on the Resolution of Board of Directors and Certificate of Authorized Signatures form, HUD 11702 and 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** ☐ **11702 signature verified**

1st Security Administrator Name **Administrator Phone Number**

1st Security Administrator Signature **Date**

☐ **Security Officer Registration Approved** ☐ **Security Officer added to the portal**

2nd Security Administrator Name **Administrator Phone Number**

2nd Security Administrator Signature **Date**

Ginnie Mae Enterprise Portal (GMEP)
Security Officer Registration for Custodian ONLY

(Please Print Details Below)

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

RULES OF BEHAVIOR

As a user of the GMEP, 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:

(a) Safeguard the information to which you have access at all times.

(b) Obtain your supervisor's written approval prior to taking any Ginnie Mae sensitive information home or otherwise away from the controlled access environment. The supervisor's approval must identify the business necessity for removing such information.

(c) Adhere to the security policies and procedures when approval is granted to take sensitive information home or away from the office.

(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 GMEP.

(5) The GMEP 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 GMEP 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) GMEP 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 (13) 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 Ginnie Mae Information System Security Officer must approve and authorize the Security Administrator'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) Security Administrators 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 Information System 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) 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 Ginnie Mae Information System Security Officer immediately in writing so that access can be terminated.

(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.

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 GMEP's information resources. 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**