



PRIVACY IMPACT ASSESSMENT

Agency: Farm Credit Administration

System Name: Nationwide Mortgage Licensing System and Registry

System Acronym: NMLSR

System Owner/Division or Office: Office of Management Services

A. Information and Privacy

To fulfill the commitment of the Farm Credit Administration (FCA or Agency) to protect personal data, the following requirements must be met:

- Use of the information must be controlled.
- Information may be used only for necessary and lawful purposes.
- Information collected for a particular purpose must not be used for another purpose without the data subject’s consent unless such other uses are specifically authorized or mandated by law.
- Information collected must be sufficiently accurate, relevant, timely, and complete to ensure the individual’s privacy rights.

Given the vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the FCA, to share sensitive personal information.

B. Contact Information:

1. Who is the person completing this PIA?

Name: Jeffrey C. Pienta
Title: Attorney - Advisor
Organization: Office of General Counsel
Contact Information:
Address: 1501 Farm Credit Drive, McLean, VA 22101
Telephone number: 703-883-4431

2. Who is the Program Manager for this system or application?

Name: Gary Van Meter
Title: Acting Director
Organization: Office of Regulatory Policy
Contact Information:
Address: 1501 Farm Credit Drive, McLean, VA 22101
Telephone number: 703-883-4026

3. Who is the Project Manager for this system or application?

Name: Jeffrey C. Pienta
Title: Attorney-Advisor
Organization: Office of General Counsel
Contact Information:
Address: 1501 Farm Credit Drive, McLean, VA 22101
Telephone number: 703-883-4431

4. Who is the IT Security Manager for this system or application?

Name: Kathleen Reddaway
Title: Information Technology Specialist
Organization: Office of Management Services
Contact Information:
Address: 1501 Farm Credit Drive, McLean, VA 22101
Telephone number: 703-883-4418

5. Who is the Chief Privacy Officer or designee who reviewed this document?

Name: Douglas Valcour
Title: Chief Information Officer and Deputy Director
Organization: Office of Management Services
Contact Information:
Address: 1501 Farm Credit Drive, McLean, VA 22101
Telephone number: 703-883-4166

C. System Description

This section of the Privacy Impact Assessment (PIA) describes the application and the method used to collect, process, and store information. Additionally, it includes information about the business functions the system supports.

Individuals employed with a depository institution, a subsidiary owned and controlled by a depository institution and regulated by a Federal banking agency, or an institution regulated by the Farm Credit Administration (FCA) (Agency-regulated institutions) who act as residential mortgage loan originators (MLOs) are required per the Secure and Fair Enforcement for Mortgage Licensing Act (S.A.F.E. Act) to register in the Nationwide Mortgage Licensing System and Registry (NMLSR), to obtain unique identifiers, and to maintain their registrations. The Federal banking agencies and the FCA issued a final rule implementing the federal registration requirements of the S.A.F.E. Act which is published at 75 Fed. Reg. 44656 (July 28, 2010) (Final Rule). NMLSR is a Web-based system developed by the State Regulatory Registry LLC (SRR), a wholly owned subsidiary of the Conference of State Bank Supervisors (CSBS), and SRR's subcontractor, the Financial Industry Regulatory Authority (FINRA). The system has been built and is maintained by FINRA. NMLSR is a modification of the Nationwide Mortgage Licensing System (NMLS), which is owned and operated, by SRR and was launched in January of 2008 for State licensing and registration purposes in participating States. MLOs in those States complete a single uniform form (known as the MU4) electronically. The data provided on the form is stored electronically in a secure, centralized repository available to State mortgage regulators who use it to process license applications and for supervisory purposes. The Federal banking agencies [through the Federal Financial Institutions Examination Council (FFIEC)] and FCA worked with SRR to modify NMLS so that it can accept registrations from MLOs employed by Agency-regulated institutions. This enhancement added data requirements, system access requirements, security requirements, and system functionality requirements. A consumer web portal will be the focus of a future system enhancement.

Federal agencies that regulate institutions who employ MLOs and who may need access to the data for supervisory purposes include: Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), and FCA (collectively the "Agencies").

D. Data in the System

1. What personal information about individuals or other information that can personally identify an individual (name, social security number, date of birth, address, etc.) is contained in the system? Explain.

Individuals employed by Agency-regulated institutions who act as MLOs are required, once the NMLSR is operational, to submit information regarding their identity (name and former names, Social Security Number, gender, date of birth, and place of birth); home and business contact information; date the employee became an employee of the Agency-regulated institution; financial services-related employment and history for the past 10 years; criminal history involving certain felonies and misdemeanors; history of financial services-related civil actions, arbitrations and regulatory and disciplinary actions or orders; financial services-related professional license revocations or suspensions. Table 1 below describes the personal information that is collected and access privileges for MLOs, Agency-regulated institutions, Federal Agencies (Regulators) and the General Public. Note that data on state license(s) held, status, and license numbers is not required to be provided by Federal Registrants pursuant to the Final Rule because the NMLSR provides the information. (In Table 1 below, “relevance” means the entity if the Federal Agency is the primary federal regulator of the Agency-regulated institution.) Once a MLO is viewable to a regulatory agency the data will remain viewable, even after that MLO is no longer employed by an institution regulated by that agency.

The S.A.F.E. Act requires fingerprints and background checks for all MLOs, including state licensees. Federal Registrants also have to submit fingerprints to NMLSR and any accompanying information required for a Federal Bureau of Investigation (FBI) background check. The results of the FBI background check will also be stored in the NMLSR. (Access to this information is not reflected in the table below.)

The NMLSR will assign a unique identifier to every MLO. The unique identifier number for all MLOs will be available to the public.

The employee registering as a MLO or renewing or updating his or her registration under the rule, and not the employing bank or other employees of the bank, must: (1) Authorize the NMLSR and the employing institution to obtain information related to sanctions or findings in any administrative, civil or criminal action, to which the employee is a party, made by any governmental jurisdiction; (2) Attest to the correctness of all information about the employee, whether submitted by the employee or on behalf of the employee by the employing bank (except MLO information that only the

institution must submit); and (3) Authorize the NMLSR to make available to the public specific employee information.

Additional information contained in the NMLSR includes data that must be entered by the Agency-regulated institution. In connection with the registration of each employee who acts as a mortgage loan originator, institution personnel must provide confirmation to the NMLSR that the institution: (i) employs the registrant, and (ii) within 30 days of the date the registrant ceases to be an employee of the Agency-regulated institution, notification that it no longer employs the registrant and the date the registrant ceased being an employee.

The Agency-regulated institution must enter data about itself on the MU1R form: name, main office address, primary Federal regulator, Employer Identification Number (EIN) issued by the Internal Revenue Service, Research Statistics Supervision Discount (RSSD) number (see below), primary point of contact information, and contact information for “system administrators.”

Information related to some MLOs may already be in the state system. However, the information collected under the state system differs from that to be collected for Federal Registrants and is collected based on separate legal authority. Therefore, all employees of Agency-regulated institutions must register in the Federal system.

As noted in Table 1 below, the public will also be provided access to information. Consumer portal access is explained further below. The table reflects the first phase of consumer access.

Table 1

(Key: A=Add; C=Change; V=View; R= See in a Report)

(Footnotes: 1-Changes made by company must be approved by individual through attestation;

2-Processed through entitlement group; 3-Must have confidential role)

| DATA | MLO | Institution With Relevance | Regulator With Relevance | Regulator Without Relevance | General Public |
|-----------------------------|---------------------|----------------------------|--------------------------|-----------------------------|----------------|
| Individual Name | A,C,V | A,C,V,R | V,R | V | V |
| Social Security Number | A,C ² ,V | A,C ² ,V,R | V ³ | | |
| Date Of Birth | A,C ² ,V | A,C ² ,V,R | V ³ | | |
| Gender | A,C,V | A,C,V,R | V,R | V | |
| State Of Birth | A,C,V | A,C,V,R | V,R | V | |
| Country Of Birth | A,C,V | A,C,V,R | V,R | V | |
| Business Phone | A,C,V | A,C,V,R | V,R | V | V |
| Cell Phone | A,C,V | A,C,V,R | V,R | V | |
| Business Fax | A,C,V | A,C,V,R | V,R | V | |
| Email address | A,C,V | A,C, V,R | V,R | V | |
| Other First Name | A,C,V | A,C,V,R | V,R | V | V |
| Other Middle Name | A,C,V | A,C,V,R | V,R | V | V |
| Other Last Name | A,C,V | A,C,V,R | V,R | V | V |
| Suffix | A,C,V | A,C,V,R | V,R | V | V |
| Employment History | A,C,V | A,C,V,R | V,R | V | V |
| Current Residential Address | A,C,V | A,C,V,R | V,R | | |

2. **Can individuals “opt-out” by declining to provide personal information or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?**

Yes Explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):

No Explain:

The S.A.F.E. Act specifically prohibits an individual from engaging in the business of residential mortgage loan origination without first obtaining and maintaining annually: (1) a registration as a registered mortgage loan originator and a unique identifier if employed by an Agency-regulated institution, or (2) a license and registration as a State-licensed mortgage loan originator and a unique identifier. A MLO must be Federally-registered if that individual is an employee of an Agency-regulated institution (subject to a *de minimis* exception for low-volume MLOs). All MLOs who are not employed by an Agency-regulated institution must be both registered in the NMLSR and state licensed. The S.A.F.E. Act requires that Federal registration and State licensing and registration must be accomplished through the same registration system, the NMLSR. The S.A.F.E. Act requires the Agencies, through the

FFIEC, and with FCA to develop and maintain a system for registering residential mortgage loan originators employed by Agency-regulated institutions.

In connection with the Federal registration, the Agencies, pursuant to the S.A.F.E. Act, at a minimum must ensure that the NMLSR is furnished with information concerning the mortgage loan originator's identity, including: (1) fingerprints for submission to the FBI and any other relevant governmental agency for a State and national criminal history background check; and (2) personal history and experience, including authorization for the NMLSR to obtain information related to any administrative, civil, or criminal findings by any governmental jurisdiction.¹

The S.A.F.E. Act also requires the Agencies, through the FFIEC and together with FCA, to coordinate with the NMLSR to establish protocols for assigning a unique identifier to each registered loan originator that will facilitate electronic tracking and uniform identification of, and public access to, the employment history of and publicly adjudicated disciplinary and enforcement actions against loan originators.

The NMLSR uses social security number and date of birth to validate the originator's identity. The NMLSR also uses this personally identifying information (PII) to confirm that the originator will receive only one unique identifier number, regardless of employment, throughout his/her life.

The Final Rule requires the collection of data specified in D.1. The Final Rule also provides that certain information will be accessible to the public.

To be "Federally" registered, a MLO must obtain a unique identifier and maintain their registration in NMSLR. The employee must also attest to the correctness of the information and the regulated institution must implement policies and procedures to confirm the adequacy and accuracy of employee registrations, including updates and renewals.

Note: A *depository institution* does not include bank or saving association holding companies or their non-depository subsidiaries. Employees of these entities who act as mortgage loan originators are not covered by the Federal registration requirement and, therefore, must comply with State licensing and registration requirements.

¹ S.A.F.E. Act at section 1507(a) (12 U.S.C. 5106(a)).

3. What are the sources of the information in the system? How are they derived? Explain.

Information is entered into the Registry by authorized system users including registrants, financial institution system administrators, and NMLS's Call Center Help Desk. The system will allow mortgage loan originators and their Agency-regulated institution employers to have access to the Registry, seven days a week, to establish and maintain their registrations.

4. What Federal agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

The Board provided the Registry with an extract of the Federal Reserve Board's database, indexed by RSSD number, for each agency-regulated financial institution to support the validation of account requests by the Registry staff. This information includes: RSSD Number, Primary Regulator; Financial Institution Name, Financial Institution Address, Financial Institution EIN, and RSSD of Parent (if subsidiary). Upon receiving the information for a new base record from an Agency-regulated institution, the Registry will confirm the information by comparing the institution application with RSSD data supplied by the Agencies.

MLOs or institutions will furnish to the Registry information concerning the MLO's identity, including fingerprints for submission to the FBI and other information as indicated in D1.

The FBI will be returning criminal background checks to the Registry for the viewing of the MLO's employer. Employers are required by the Final Rule to review these background checks and take appropriate action consistent with applicable law. Employers may make hiring or firing decisions about the MLO based on the background check information, or may take disciplinary actions against the MLO based on the background check information.

5. What state and local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

No data is provided by state and local agencies in connection with federal registration of MLOs.

State regulators may access information of dually regulated-licensed MLOs.

6. **What other third party sources will be providing data to the system? Explain the data that will be provided, the purpose for it, and how will it be used.**

MLOs or institutions will furnish to the Registry information concerning the MLO's identity, including fingerprints for submission to the FBI and other information as indicated in D1.

Potential uses of MLO data in system include:

1. Providing MLO Data to state and federal law enforcement agencies for legally-authorized or required purposes.
2. Communicating with Registrants regarding Federal Registration.
3. Communicating or releasing Registrant Data as required by law, rule or regulation, such as in response to public information disclosure laws such as the Freedom of Information Act, 5 USC 552, to the extent not otherwise shielded from disclosure under the S.A.F.E. Act or the Privacy Act of 1974, 5 USC 552a.
4. Use of Registrant Data by Agencies in any enforcement or disciplinary proceedings or complaint-related inquiries concerning a Registrant.
5. Institutions will have access to the information and could take disciplinary actions or make hiring/firing decisions based on the data.

E. Access to Data:

1. **Who will have access to the data in the system (e.g., users, managers, system administrators, developers, contractors, other)? Explain their purpose for having access to this information.**

NMLSR/"Registry" takes appropriate security measures to safeguard PII and other sensitive data. NMLSR is located in a locked and secured environment, 24/7, and access is strictly controlled and monitored.

Access to the data is strictly monitored and limited to individuals that have a "need to know" for access (except for consumer portal access). In addition, access to NMLSR PII is limited according to job function. Access control privileges are set according to the following roles:

- Account Administrator (company/regulator)
- Organization User (company)
- Organization User (regulator)
- Individual User
- Privileged Users

Access to the data in the system is based on a need to know, is role based, and is limited to the Agencies' authorized users, authorized state regulator users, authorized MLOs, authorized financial institution users, authorized system development staff and authorized operators of the system (except for consumer portal access).

The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to *explicitly authorized personnel*. Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions in development/test and production environments (e.g., system administrators, information system security officers, maintainers, system programmers).

The matrix below describes the levels of access and safeguards around each of these roles as they pertain to the protection of PII.

| ROLE | ACCESS | SAFEGUARDS |
|--|---|--|
| Account Administrator (company/regulator) | Create Account Modify Account Information Update User Account Role Unlock User Accounts Enable or Disable User Accounts Delete User accounts View Individual Composite View Institutional Composite View Confidential Information | Unique User IDs and passwords are established in accordance with the NMLS Rules of Behavior/User Access Agreement policy for non-Federal users. For the Registry, Federal Agencies require users with access to multiple federal agency-regulated Mortgage Loan Originator (MLO) records in NMLS to have a second factor login in addition to the authenticated NMLS user id and password. The second factor login must be an externally-controlled credential registered to the user in NMLS. Access is audited. Continuous National Institute of Standards and Technology (NIST) 800-37 Certification and Accreditation (C&A) process that includes a System Security Plan (SSP) that incorporates a Data Management Plan, and a Contingency Plan / Disaster Recovery Plan and Security Test and Evaluation monitoring |
| Organization User (company) | Create and submit MU1R filing Manage Notification Contacts Create and submit MU4R filings Manage institution Relationships Access Work Items View individual composite View subsidiary composite View Confidential Information Financial Administration Manage Reports Renewals | Same as above |
| Organization User (regulator) | Manage Notification Contacts View Individual Composite View institution Composite Manage Data Downloads | Same as above |

Manage Reports

| | | |
|-----------------|--|---------------|
| Individual User | Create Individual Account Create Password Change password as well as question and answer | Same as above |
|-----------------|--|---------------|

Federal registrant information will not be available to the state regulators generally. However, there will be originators who will be state licensed and federally regulated, for example, due to dual employment. State regulators will have access to MU4 data of those Federal Registrants who are (or were) also state licensed or applying for state licenses.

Consumer portal: The S.A.F.E. Act requires public access to the employment history of and publicly adjudicated disciplinary and enforcement actions against mortgage loan originators. Pursuant to the Agencies' rule, the NMLSR will make available to the public the bank employee mortgage loan originator's name; other names used; name of current employer(s); current duty station(s); business contact information; 10 years of relevant employment history; and disciplinary and enforcement actions and arbitrations against the employee. Table in D1 shows public access in the first phase. The public access database will be physically separated from the database that stores the PII. This information is expected to be made public in two phases. The first phase will provide for public access to the employee's name; other names used; name of current employer(s); current duty station(s); business contact information; and employment history. The information will be available after the 180-day Federal registration period ends.

The second phase will include the remaining categories of information at a later date, which is dependent upon the SRR designing and implementing system changes that permit Federally registered mortgage loan originators to voluntarily provide additional information to explain any positive response to any of the disclosure questions regarding criminal history or similar information. These explanations will also be available to the public through the public access database.

2. **How is access to the data determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Explain the process.**

Access to the data is limited to those with an operational need to access the information (except for consumer portal access). The system will restrict access to data based on roles and “need-to-know” basis. System access is granted via uniform registration forms known as MU Forms. Form MU4R (Uniform Individual Mortgage Registration & Consent Form) will be used by individuals to register as mortgage loan originators (MLO) and establish or amend a registration as an individual loan officer employed by an Agency-regulated institution. Form MU1R (Uniform Mortgage Lender or Broker Application) is to be completed by institutions and their federally-regulated subsidiaries. The MU1R form will also establish the institution’s administrators. Once a record is established in the Registry, access to data is granted based on a predetermined role. Agencies will have the ability to obtain a bulk download of all MLOs registered with a financial institution supervised by the agency. Access for SRR employees and its contractors is established by SRR. The system provides for structured authentication and account management as set forth in the system roles and the employed account management procedures. SRR employs automated mechanisms to support the management of information system accounts. These mechanisms will automatically terminate temporary and emergency accounts after a 24 hour time period. The information system automatically disables inactive accounts after (a) 120 days of inactivity for privileged users or (b) 15 months of inactivity for registrants (MLOs). Further, SRR employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

3. **Will users have access to all data on the system or will the user’s access be restricted? Explain.**

User access to the system and the system data will be restricted through predetermined roles that allow access to and actions on the system data.

The Registry restricts access to data on a “need-to-know” basis. Only a select few administrative and privileged users will have access to all the data, and these individuals undergo a rigorous background screening process.

Accessing privileged functions also requires multi-factor authentication.

General users will only have access to their personal data; this restriction is enforced by the role-based access system based on the defined user roles.

Users will be able to access and attest to the completeness and accuracy of their data prior to the company submitting data to the regulators.

See the matrix in response to E1. above for specific details on user access to data in the system.

4. **What controls are in place to prevent the misuse (e.g., browsing) of data by those having access? (Please list processes and training materials) Explain the controls that have been established and how are they monitored or reviewed.**

Role-based restrictions are in place and all users will have undergone background checks.

All data exchanges will take place over encrypted data communication networks, private networks and/or encryption technologies used during the transfer of information to ensure that Internet “eavesdropping” does not take place and that data is sent only to its intended destination and to an authorized user, by an authorized user.

Users accessing the Registry will agree to terms of use agreements. Persons given roles must also agree to terms of use agreements.

SRR has established an internal incident response capability and audit event logs for the system. SRR and OCC (acting on behalf of the Agencies) executed a contract on July 21, 2010 (Contract). Pursuant to the Contract, SRR will notify the Agencies immediately of any suspected or actual data breach through a single point of contact designated by the Agencies.

5. **Do other systems share data or have access to the data in the system? If yes, explain the purpose for the need to have access.**

No.

6. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface? Has policy or procedures been established for this responsibility and accountability? Explain.**

All users will have a role in protecting the privacy rights of the public and employees affected by the interface. All users who have access to the data or retrieve data from the system will have responsibility for and be accountable for data security. SRR has established terms of use of the system data. Each agency will be responsible for ensuring established rules of behavior are in place and adhered to by agency users.

For the FCA, policies exist for the treatment of sensitive business and PII data. Further, FCA employees receive mandatory annual training with regard to IT security requirements and the controlling provisions of the Privacy Act with respect to the collection, maintenance, use and dissemination of personal information by Federal agencies.

7. **If other agencies use the data, how will the data be used? Who establishes the criteria for what data can be shared? Have non-disclosure agreements been effected? Explain the purpose for the need to share the data?**

Federal users will have access to specific views of shared data. Federal regulators will have the ability to obtain a bulk download of MLO registrants employed by institutions that they supervise. The Contract has provisions governing the terms of use and access to data.

See #6 for potential Agency uses of data. See Table in D1 for access to data. State regulators will only view Federal Registrant data for MLOs who are or were also state licensees.

8. **Who is responsible for assuring proper use of the data? Is this individual fully accountable should the integrity of the data be compromised? Explain.**

SRR establishes and makes readily available to all information system users terms of use that describes their responsibilities and expected behavior with regard to information and information system usage. SRR receives an electronic acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

For FCA, data retrieved from the system becomes the responsibility of the Agency and its user-employees once the data exits the Registry system boundaries.

9. **Explain the magnitude of harm to the corporation if privacy related data is disclosed, intentionally or unintentionally. Would the reputation of the corporation be affected?**

If the FCA downloads information from the Registry, the FCA is responsible for the security of that data. Once transmitted to a regulator by SRR, any system data will be the regulator's responsibility and subject to any Federal or Agency-administered privacy policies and public information laws. SRR is not responsible for any data once it is outside of the Registry system boundaries. This would exclude any SRR-initiated transmission errors. If

disclosure (intentional or unintentional) occurs while data is possessed by the FCA or its personnel, the data disclosure would have an impact on the Corporation's reputation.

10. What involvement will a contractor have with the design and maintenance of the system? Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been developed for contractors who work on the system?

NMLS was created by the Conference of State Bank Supervisors (CSBS) and the American Association of Residential Mortgage Regulators (AARMR). It is owned and operated by the State Regulatory Registry LLC (SRR), a wholly owned subsidiary of CSBS. The system has been built and maintained by the Financial Industry Regulatory Authority (FINRA). SRR and FINRA employ contractors and subcontractors, and third party service providers. All groups are covered by applicable agreements. The NMLS is located at Electronic Data Systems.

11. Explain whether or not the data owner is contacted if it is not clear if other agencies share or have access to the data.

The data owner will be contacted in accordance with the regulations and policies that apply for the party responsible for the data breach. In the event that SRR becomes aware of a data breach which SRR believes has resulted or may result in the unauthorized access, use or disclosure to nonpublic personal information of end users, SRR will: (a) immediately notify a single point of contact designated by the Agencies and grant the Agencies immediate access to investigate; and (b) upon confirmation of an actual data breach promptly develop and implement a remediation plan in coordination with the relevant Agencies. The remediation plan will include procedures, in compliance with applicable laws, to promptly notify persons whose data is affected and to provide credit monitoring services or other appropriate remediation (at SRR's expense).

F. Accuracy, Timeliness, and Reliability

- 1. How is the data collected from sources other than FCA records verified? Has action been taken to determine its reliability that it is virus free and does not contain malicious code? Who is responsible for this making this determination? Explain.**

MLOs and their employing institutions are responsible for data accuracy as it is entered into the system. SRR and FINRA have no formal policies on data integrity. At this time, FCA will have no determined or assumed responsibility for data accuracy, timeliness and reliability.

- 2. How will data be checked for completeness? How is this being measured? What is the source for ensuring the completeness of the data? Explain the method used.**

NMLSR/Registry has built in “completeness” checks that determine if all data fields are completed.

NMLSR/Registry “Help Center” staff will review institution base record information to verify RSSD number, address, etc.

Data accuracy is the responsibility of the institution’s administrators when they verify the MLO’s record and acknowledge that the MLO in fact is employed by the institution.

MLOs attest to the completeness and accuracy of their data when submitting form MU4R.

The regulation requires a MLO to renew their registration with the NMLSR annually. To renew, the MLO must confirm that the information previously submitted to the NMLSR remains accurate and complete and update any information as needed. In addition to the annual renewal, the mortgage loan originator's information must be updated within 30 days of the occurrence of any of the following events: (1) a change in the registrant's name; (2) the registrant ceases to be an employee of the Agency-regulated institution; or (3) any of the registrant's responses to the certain of the information required for original registration become inaccurate.

Furthermore, in connection with the registration of each employee who acts as a mortgage loan originator, institution personnel must provide confirmation to NMLSR that the institution (i) employs the registrant; and (ii) within 30 days of the date the registrant ceases to be an employee of the Agency-regulated institution, notification that it no longer employs the registrant and the date the registrant ceased being an employee.

The regulation will require an Agency-regulated institution that employs mortgage loan originators to adopt and follow written policies and procedures designed to assure compliance with the requirements of the Final Rule. These policies and procedures must include provisions that establish reasonable procedures for confirming the adequacy and accuracy of mortgage loan originator registrations, including updates and renewals; establish reasonable procedures and tracking systems for monitoring compliance with registration and renewal policies and procedures; and provide for independent testing for compliance with the regulation by bank personnel or by an outside party at least annually.

G. Attributes of the Data?

- 1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? Is this part of the system design? Is this documented, if so, where is the document located? Explain.**

All data is collected from MLOs and is relevant and necessary per S.A.F.E. Act requirements. (See D2 for S.A.F.E. Act requirements and the Agencies' rule.)

The NMLSR uses SSN and birth date to validate the identity of the MLO.

For FCA, the data is relevant and necessary in fulfilling supervisory and examination responsibilities to ensure compliance with regard to the S.A.F.E. Act.

- 2. Will the system derive personal identifiable information from any new data previously non-inclusive, about an individual through aggregation from the information collected? What steps are taken to make this determination? Explain.**

No

- 3. Can the system make privacy determinations about employees that would not be possible without the new data? If so, explain.**

For the FCA, no such determinations will be made.

- 4. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Does the consolidation of data result in personal identifiable information? Explain.**

N/A

- 5. How is the data retrieved? Can it be retrieved by a personal identifier (e.g., social security number)? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**

Each MLO is assigned a unique identifier. It is anticipated that FCA will have the ability to obtain these identifiers from the system indexed by financial institution and will have ability to obtain special reports that contain most data fields provided for in the system to which a federal regulator is granted access.

The public will also be able to retrieve information on a MLO by searching a unique identifier.

- 6. What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them? Explain how they are distributed.**

Institutions will have access to the following reports that will assist in managing the registration process for associated MLOs:

1. Individual Roster Report – this report will contain a list of the institution’s associated MLOs and their registration status
2. Criminal Background Check report – this report will contain a list of the institution’s associated MLOs and whether they have submitted electronic Fingerprints to NMLS (this may be combined with the report above)

FCA will have access to the following reports:

1. Individual Roster Report – this report will contain a listing of MLOs with relevance to a particular agency. The information for each MLO will include NMLS ID, name, and registration status. The institution associated with each MLO will also be listed, including the RSSD number, NMLS ID, and institution name. FCA users will have the option to include all Federal Agency-regulated MLOs in the report, or limit the report to MLOs associated with a specific institution.
2. Institution Roster Report – this report will include a listing of all the Institutions with relevance to a particular agency. Data fields will include the RSSD, NMLS ID, and Institution name.

In addition, NMLSR provides ad-hoc reporting services to supplement the reporting and download capabilities. Ad-Hoc reports are available on a cost plus basis only to authorized recipients (institution Account Administrator(s))

and previously authorized agency staff), come in a variety of formats and contain data that is non-sensitive and relevant to the requesting institution or agency.

H. Maintenance and Administrative Controls:

- 1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites? Will the same controls be used? Explain.**

Financial Industry Regulatory Authority (FINRA) of Rockville, MD, which maintains background check system data for the NMLSR, operates the system which is hosted by a third party service provider HP Enterprise Services with physical locations in Charlotte, NC, and Plano, TX. The same management, technical, and operational controls are employed at both sites.

NMLS production systems are in the HP Enterprise Services Charlotte Datacenter. HP Enterprise Services Plano Datacenter as used as a dual use test and disaster recovery facility.

- 2. What are the retention periods of data in this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? Explain.**

SRR will retain data for a 5 year period and currently has no plan to remove data at any time. However, they may need to remove old, inactive data at some point in the future for performance reasons. Regardless of that, SRR would still have to retain the NMLS ID (and some minimal amount of associated data) related to such individuals as are removed so that SRR can continue to comply with the “unique identifier” requirements of the S.A.F.E. Act. Backup tapes are generated and retained, as per policy, then moved to an Iron Mountain off site storage facility.

- 3. What are the procedures for disposition of the data at the end of the retention period? How long will any reports produced be maintained? Where are the procedures documented? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the procedures? Explain.**

Backup tapes are generated and retained, as per policy, then moved to an Iron Mountain off site storage facility.

4. Is the system using technologies in ways that the Corporation has not previously employed (e.g., Monitoring software, Smartcards, Caller-ID, biometrics, PIV cards, etc.)? Explain.

No.

5. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology? Explain.

The existing system known as NMLS was not designed to support the Federal registration of Agency-regulated institution employees. Accordingly, the system was modified to accommodate the differences between the requirements for State licensing/registration and Federal registration. It also was modified to accommodate the migration of an individual between the State licensing/registration and the Federal registration regimes or the dual employment of an individual by both an Agency-regulated and non-Agency-regulated institution. Furthermore, the S.A.F.E. Act required new enhancements, such as the processing of fingerprints and public access to certain mortgage loan originator data. These modifications and enhancements require careful analysis and raise complex legal and system development issues that the Agencies are addressing through consultation with the CSBS and the SRR.

There is a risk that data could be compromised by either an internal or external party. The NMLS or Registry will expand the number and roles of individual and institution users. Additionally, the Registry will expand the data collected and retained plus the system access points to include a public web portal. Also, data can be introduced into the system via bulk uploads and extracted from the system when downloaded by the Agencies. All of these factors introduce new opportunities for compromise that did not exist prior to the system enhancements to meet the requirements of the Act. The risk is mitigated by multiple technical, physical, and administrative controls. Additionally, the NMLSR system must meet all Federal Information Security Management Act requirements, as well as Office of Management and Budget (OMB) and NIST policies and standards.

Specifically, these are the privacy risks and how FFIEC agencies are mitigating those risks:

- Risk: Information from the NMLSR could potentially get into the wrong hands, and “identity theft” could occur. Mitigation: Only those who hold “positions of trust” (such as Bank examiners, system security personnel and legal staff) are authorized to handle data from NMLSR. Restricting who can handle these documents greatly reduces

the risk of potential identity theft of such information as full name, Social Security Number, date of birth, place of birth, and home address. As shown in table 1, Social Security Numbers and date of birth have been suppressed, and place of birth and home address are not accessible for Federal system users.

- Risk: PII stored in the NMLSR could potentially be accessed by unauthorized persons. Mitigation: This system and its databases are restricted to those in positions of trust. NMLSR will require the user to have a log on ID and password and sign a system User Agreement prior to having access to the system. Authorized Federal users are required to complete IT security and privacy training annually and we have been trained on computer security rules, as well as the punishments and fines for deliberate or negligent violations of the Privacy Act.
- Risk: Background investigation information could be seen or taken by unauthorized persons. Mitigation: Only individuals with access to background data will be authorized to see the details of an individual's criminal history records. Federal system users will not have access to background information.

6. If monitoring is being performed, describe the data being collected. Is monitoring required? If so, describe the need for the monitoring and identify the requirements and explain how the information is protected.

FCA may use the system to monitor an institution's S.A.F.E. Act compliance; however, the FCA does not anticipate using the system for any individual monitoring. Information provided by the system is most likely also available through each Agency-regulated institution.

SRR maintains a strong security posture and network security to protect Personal Identifiable Information (PII) by the inherent security of the system (i.e., firewalls, passwords, and separation of roles). Any monitoring by SRR is strictly for system security and administration operations and would not specifically target individual users.

7. If monitoring is not required, explain the controls that will be used to prevent unauthorized monitoring?

Not applicable.

8. In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name.

Privacy Act of 1974; Establishment of a New System of Records, 76 Fed. Reg. 7204 (February 9, 2011). Name: Nationwide Mortgage Licensing System and Registry (NMLSR).

9. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

A Privacy Act system of records notice (SORN) is now required due to passage of the S.A.F.E. Act, which required significant changes to the original system known as the Nationwide Mortgage Licensing System, and which mandated registration of MLOs employed by Agency-regulated institutions in the enhanced system. The modified system is known as the Nationwide Mortgage Licensing and Registry System (NMLSR) and FCA did not have retrieval access to the NMLSR until the SORN comment period expired.

I. Business Processes and Technology

1. Does the conduct of this PIA result in circumstances that requires changes to business processes?

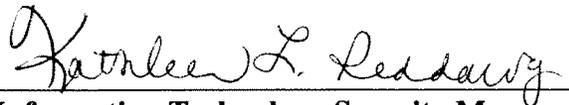
No

2. Does the completion of this PIA potentially result in technology changes?

No

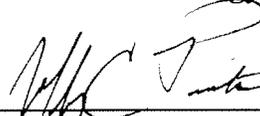
**Privacy Impact Assessment
Authorization Memorandum**

This system or application was assessed and its Privacy Impact Assessment approved for publication.



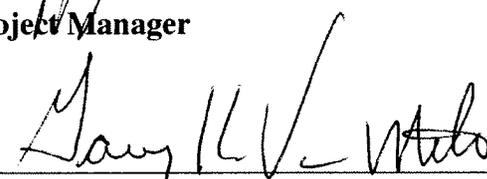
Information Technology Security Manager

1-28-2011
Date



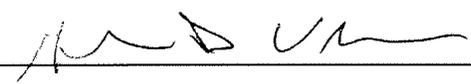
Project Manager

1-26-2011
Date



Program Manager

2-01-2011
Date



Chief Privacy Officer

1/28/2011
Date