State Regulatory Registry LLC provides NMLS on behalf of, and under contract with, state regulatory agencies and the Consumer Financial Protection Bureau (Agencies) and has been approved for use by these Agencies. NMLS undergoes rigorous testing and reviews to ensure that sensitive and non-public data is protected. What follows is a summary of the technical details and data security protocols.

- **Technical Details**
  - NMLS is a web-based system that uses HTTPS (HTTP over Secure Transport Layer). Protocols older than TLS 1.0 are not supported.
  - RSA 2048 bit certificates are used to encrypt and decrypt data as it transfers from the user page requests to the NMLS web server. The system performs a certificate revocation list (CRL) check during the communication process to ensure that the certificate presented by the server being communicated with has not been revoked.
  - NMLS supports IE 9.0 and Firefox 32 or greater. The browser must be java script enabled and it is recommended that cookies are enabled.
  - Email notifications sent from NMLS come from NMLS_Notifications@NmlsNotifications.com. They do not contain sensitive information.

- **User Accounts**
  - System passwords must be between 8 and 16 characters in length and must include 3 of 4 of the following: upper case, lower case, special character or number.
  - Passwords expire every 90 days. Users are prompted to change their passwords upon expiration.
  - An account is considered dormant if it contains no data such as testing and education results, regulatory actions or submitted licensure applications on the record. NMLS will delete a dormant account after 180 days for company and individual users. Pending filings do not prevent an account from dormancy and will be deleted after 180 days along with any related dormant accounts.
  - For accounts with education and testing results or submitted or approved filings, NMLS will disable the account if it has not been accessed in 120 days by a company account user or 15 months by an individual user. If a user account is disabled, the System prompts the user to provide identifying information before they can log into their account.
  - Users are locked out after 3 invalid attempts within a 24 hour period.
  - Users’ sessions expire after 30 minutes of general inactivity and after 15 minutes of inactivity on payment processing pages.
  - Multi-factor authentication is required for some state regulatory agencies, Federal Registry institutions and support users. This is provided by using hardware and software tokens.
  - Access to NMLS from both a user and administrator perspective is controlled through the use of unique usernames and passwords. Accounts are provided access through a Role Based Access Control (RBAC) wherein each user identifier is given a
role. Depending on the user role, that individual will be provided access to specific areas of the application

- Only users granted a specific role in NMLS (e.g. account administrators for a company or regulator) are able to view NPPI\(^1\) (e.g. social security number or date of birth).

**Data Protection**

- Infrastructure, applications, and data are protected by multiple layers of security to guard against both external and insider threats.
- SSNs and other sensitive personal information is accessible to only authorized individuals. Each access event is logged in order to capture the information viewed and the authorized individual who accessed it.
- NMLS utilizes encryption that is NIST 197 compatible and uses a NIST 256-bit certified encryption algorithm (AES).
- Personally Identifying and other sensitive information (e.g. MLO Batch Upload, Criminal History Record Information) are encrypted when at rest in the database.
- Data is encrypted via TLS when in transit between the web server tier and the application server tier of NMLS.
- Between the database server tier and the other NMLS tiers, data is encrypted using the IPsec protocol, which has been configured to encrypt all TCP traffic (including database transaction traffic) between these servers.
- All NMLS staff, contractors and agents with access to data undergo annual Privacy and Security Awareness training.
- No file uploaded to NMLS (CSV, XML, PDF) is written directly to the database server. All uploaded files are scanned by virus protection software as they are being written to the disk drives and immediately quarantined if malware is detected.

**Fingerprint Record Security**

- Fingerprint records are securely received, stored, and transmitted by the NMLS Fingerprint (NFP) system. Technologies utilized include session encryption including secure web access and secure transport. The background check results are purged from NFP 30 days after receipt, though the Fingerprints themselves are archived for a minimum of 3 years.
- In addition to the secure transmission of fingerprint records, there are layers of physical and network security applied. The NFP system is segregated from that of NMLS and additional physical controls have been established. Firewalls are used to restrict network access to the NFP servers.

**Testing, Reviews and Compliance**

- NMLS undergoes a rigorous Application Certification process to ensure NMLS meets the specified standards.
- There is an SSAE SOC 1 Type 2\(^2\) and SOC 2 Type 2 evaluation performed on the primary data center which hosts NMLS hardware. CSBS also conducts a biennial independent third-party SSAE SOC 1 Type 2 audit of financial controls within NMLS.
- NMLS complies with the "moderate" baseline security controls contained in National Institute of Standards and Technology (NIST) Special Publication 800-53\(^3\), and is

\(^1\) Non-Public Personal Information (NPPI)
\(^2\) Previously this used to be a SAS70 report
\(^3\) Recommended Security Controls for Federal Information Systems, Revision 3, August 2009
fully accredited (FISMA Certification & Accreditation) by the Consumer Financial Protection Bureau (CFPB). FISMA security controls within NMLS are reviewed by an independent third-party security assessor annually.

- There is an independent third-party security penetration test performed on NMLS annually.
- NMLS complies with the requirements of U.S. Department of Justice-Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy\(^4\) for the storage of fingerprint and background check results records and is periodically audited by the FBI for compliance to the CJIS.
- NMLS receives annual Attestation of Compliance from appropriate Service Providers to the Payment Card Industry (PCI) Data Security Standards (DSS).
- Business Information Group (BIG) and their subsidiary, Fieldprint, which collects and processes fingerprints is PCI Compliant, conducts an annual SSAE 16 SOC 2 report and adheres to the CJIS Security Policy.
- TransUnion, which is integrated with NMLS for the purpose of credit report processing, undergoes an annual SSAE SOC 2.

- **Federal Registry Specifics**
  - NMLS Federal Registry users require a "two-factor" authentication mechanism at assurance level 3\(^5\) for all user accounts (Federal Agency, Agency-regulated institution and NMLS Call Center staff with federal record access) that permit access to multiple records.
    - First factor is user name and password.
    - Second factor is provided by third-party service provider and meets the NIST Level 3 Assurance level when combined with a user name and password. NMLS supports hardware, mobile and browser based tokens.
  - The MLO Batch Upload feature is only available to users that have been authenticated into NMLS and have been granted the role necessary to perform batch upload.
    - The uploaded file is encrypted and stored in the database.

---

\(^4\) Version 4.5, December 2008 (CJISD-ITS-DOC-08140-4.5)

\(^5\) Consistent with OMB Memo M-04-04, E-Authentication Guidance for Federal Agencies, 16 December 2003, and NIST SP 800-63-1, Electronic Authentication Guidance, 8 December 2008 (DRAFT)