



NMLS Technical Details and Data Security Protocols

State Regulatory Registry, LLC provides NMLS on behalf of, and under contract with, state and federal regulatory agencies (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 Socket Layer (SSL)). SSL encrypts and decrypts data as it transfers from the user page requests to the web server.
 - NMLS supports IE 7.0 and Firefox 3.0 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.
 - The production environment of NMLS is hosted at an Equinix Data Center in Secaucus, NJ.

- User Accounts
 - Only users granted a specific role in NMLS (e.g. account administrators for a company or regulator) are able to view the full social security number (SSN) or full date of birth.
 - 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 120 days.
 - Users are prompted to change their passwords upon expiration.
 - Company and institution user accounts are disabled after 120 days of inactivity.
 - Individual user (loan originators & control persons) accounts are disabled after 15 months of inactivity.
 - Users are locked out after 5 invalid attempts within a 24 hour period.
 - Users sessions expire after 30 minutes of inactivity

- Data Protection
 - Infrastructure, applications, and data are protected by multiple layers of security to guard against both outsider and insider threats.
 - SSNs are masked except for the last four digits with the exception of a single page where a user who has been granted a Confidential Information role by their Account Administrator may view the full SSN.
 - NMLS uses 256-bit encryption
 - Personally Identifying and other sensitive information (e.g. MLO Batch Upload, Criminal History Record Information) are encrypted when at rest in the database (Oracle).
 - Data is encrypted via SSL when in transit between component servers of NMLS.
 - Between the web server tier and the application server tier, data is encrypted using TLS/SSL.

- Between the application server tier and the database server tier, data is encrypted using the IPsec protocol features of the respective servers' operating systems.
 - Between the web server tier and the database server tier, data is encrypted using the IPsec protocol features of the respective servers' operating systems. IPsec 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 files are scanned by virus protection software prior to being written to the disk drives. Once files are written to the drive they are not scanned again, it is the downloader's responsibility to test any files they download for viruses.
- **Fingerprint Record Security**
 - Fingerprint records are securely received, stored, and transmitted by the NMLS Fingerprint (NFP) system. Through each step of the processing lifecycle security is in place for those records. This security is a combination of restricting physical access to the servers as well as security at the data level in terms of encryption and the limitation of access to users with specific permissions, logins, and roles. The following are the details regarding the security applied throughout the fingerprint record processing lifecycle:
 - Beginning of lifecycle: Fieldprint, the authorized Live Scan vendor, utilizes S/MIME encryption when transmitting the fingerprint record to NFP
 - Upon receipt of the fingerprint record NFP queries NMLS via an HTTPS web service connection for authorization to transmit that print to the FBI
 - Upon receipt of authorization NFP utilizes a secure VPN channel to transmit the packaged fingerprint record to the FBI
 - The FBI response is then received over the same secure VPN channel
 - NFP sends NMLS the background check results (the fingerprint record itself is never sent to NMLS) over the HTTPS web service
 - Once the result has been received from the FBI the NFP system will send the fingerprint record to the Secaucus Data Center for archiving
 - End of lifecycle: The background check results are then purged from NFP 30 days after its receipt. 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 basis of NFP is Commercial Off-The-Shelf (COTS) software from Cogent Systems. This software and its database are completely separate from that of NMLS. This software is hosted on a pair of production Windows servers located within the FINRA Rockville data center. Physical access to those servers is restricted to only those individuals with special badge access to the server room. In addition, once an individual is inside the server room they would need to have login accounts with the proper permissions in order to gain access to NFP.
 - Firewalls are in place to restrict network access to the NFP servers. These firewalls restrict access from the Internet where the system is receiving the incoming transmission of records from Fieldprint. In addition, firewalls are in place restricting access between the Rockville Data Center and its GlobalNet access to the archive

servers in the Secaucus Data Center. The Secaucus servers are also restricted by badge access as well as login accounts and file permission settings.

- Testing, Reviews and Compliance
 - NMLS undergoes a rigorous Application Certification process to ensure NMLS meets the specified standards.
 - There is an SAS 70 Type II evaluation performed on Equinix (formerly Hewlett Packard), who hosts NMLS hardware.
 - NMLS complies with the moderate baseline security controls contained in National Institute of Standards and Technology (NIST) Special Publication 800-53¹, and is fully accredited (FISMA Certification & Accreditation) by the Federal Agencies².
 - There is an annual independent penetration test performed on NMLS.
 - NMLS complies with the requirements of U.S. Department of Justice-Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy³ for the storage of fingerprint and background check results records.
 - NMLS is in compliance with the Payment Card Industry (PCI) Security Council standards.
 - Business Information Group (BIG) and their subsidiary, Fieldprint, which collects and processes fingerprints is PCI Compliant, conducts an annual SSAE 16 Type 2 report and adheres to the CJIS Security Policy.
 - TransUnion, which is integrated with NMLS for the purpose of Credit Reports undergoes an annual SAS70

- Federal Registry Specifics
 - NMLS Federal Registry users will require a "two-factor" authentication mechanism at assurance level 3⁴ 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 Symantec VIP Manager (formerly VeriSign) and meets the NIST Level 3 Assurance level when combined with a user name and password. NMLS supports hard, 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.

¹Recommended Security Controls for Federal Information Systems, Revision 3, August 2009

² Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, Farm Credit Administration, and the National Credit Union Administration

³ Version 4.5, December 2008 (CJISD-ITS-DOC-08140-4.5)

⁴ 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)