SLI Compliance Election Auditing Services

Overview

SLI Compliance is accredited by the U.S. Election Assistance Commission (EAC) as a Voting System Test Lab (VSTL) qualified to test voting systems to Federal standards. As an ISO/IEC 17025 accredited test lab under the National Voluntary Accreditation Program (NVLAP) of the National Institute of Standards and Technology (NIST) (NVLAP Lab Code 200733-0: TESTING), SLI Compliance provides a full range of voting system testing services and election support services to international organizations, and state and local governing bodies. We have applied our testing methodology to certification engagements since 2001 and we have tested the systems of virtually every voting system manufacturer currently engaged in designing and implementing electronic voting systems.

The SLI Compliance team has extensive expertise in election and voting system technology. Our team brings the CTFL, CISSP, and CEH* credentials and relevant experience and knowledge to ensure our clients have access to the most qualified voting systems expertise in the industry. Our extensive knowledge of election processes, software security practices, and voting system industry standards assures that each engagement receives the high-quality testing or auditing rigor required to meet today's security and compliance standards. *ISTQB Foundation Level, Certified Information Systems Security Professional and Certified Ethical Hacker

SLI Compliance understands that in today's world, system security is a top priority. Included in our list of services are end-to end audits to identify weaknesses in the security chain and to validate the security of all aspects of the voting system. Our focus is on identifying vulnerabilities within the system and facility configurations that could compromise security, confidence, and integrity.

Security audits include many facets of analysis and review. At SLI Compliance we consider the importance of auditing the entire election environment including both the facility and the voting systems themselves. Because we also understand that organizations may require customized audits based on their own interests, needs and individual configurations, we offer a "menu" of selections, so an organization is able to pick and choose the services that best suit their needs.

Based on a client's needs, we offer various auditing analysis options, including but not limited to:

1. Verifying the election environments, which includes both polling place and central count locations (pre & post-election)
2. Verifying that the software installed on the voting system equipment is the same as the software certified (pre & post-election)
3. Verifying that no malicious software is running on any component; this includes voting system equipment as well as the broader range of election equipment (pre & post-election)

4. Verifying that components are not connected to the internet and that they have not been connected to the internet (pre & post-election)
5. Performing a physical audit of the components to verify there is no unexpected hardware (pre & post-election)
6. Verifying post-election data

Below is a list of the security auditing services provided by SLI Compliance:

Polling Place Environment Audit

The polling place environment is the more fluid of the two environments. With poll workers, maintenance people, poll watchers, media and a steady stream of voters passing through, a verified implementation of processes and policies is very valuable. SLI Compliance audits aspects within the polling place environment that are pertinent to both a pre- and post-election audit. These include:

- Physical Access Control
    - Public areas
        - Controlled access to polling areas
        - Appropriate privacy provisions
            - Distance apart (voters waiting, each polling station)
            - Appropriate layout (not facing each other, windows, lines of people)
        - Sufficient oversight personnel
            - Number of personnel
            - Stations for oversight
    - Poll Officials only areas
        - Controlled access
        - Control of non-public materials
    - Polling place policy/procedure verification
        - Policy around security seal management (application, removal, auditing)
        - Policy around control of sensitive objects and data (authentication tokens, passwords, keys, removable media, replacement security seals)

Central Count Environment Audit

In the central count environment, with election officials, maintenance people, poll watchers, media and a steady stream of poll workers passing through delivering election artifacts, the need for a verified implementation of processes and policies is very valuable here as well. SLI Compliance audits aspects within the central count environment that are pertinent to both a pre- and post-election audit. These include:

- Facility & physical security auditing
    - Controlled access to central count areas
    - Infrastructure physical security control validation
        - Lock/keyed server cabinets
        - Lock/keyed networking cabinets
        - Access controls to sensitive areas (lock/keys, badge access etc.)
        - Monitoring and response (CCTV, alarms, on duty guards)
        - Disposal of election materials: secure paper bins, secure trash dumpsters
        - Fire suppression
        - Redundant power
        - Verification of election infrastructure including air-gap of isolated voting networks
        - Physical security mitigations (lock/keys, port security, seal validation)
    - Business continuity and disaster recovery
        - Backup solution examination
        - Risk analysis for election disruption sources
        - Emergency and cybersecurity response plans
- Policy Auditing
    - Written security policies
    - Air-gap policy
    - Policy for security seal management
    - Policy for sensitive objects and data control
    - Access control policy
    - Incident response policy
    - Security breach policy
    - Disposal/decommissioning policy for election systems
    - Election worker training
    - General IT policies (access, password, usage, etc.)
    - Visitor guest access policy

Warehouse Environment Audit

The warehouse environment requires physical security safeguards to protect voting systems and related facilities and equipment from environmental threats, as well as from tampering, vandalism, and theft. Physical security needs to be considered for voting systems in storage (e.g., warehouses, storage rooms) as well as in the polling places and central count location. SLI Compliance audit aspects within the warehouse environment that are pertinent to both a pre- and post-election audit. These include:

- Facility & physical security auditing
  - Controlled access to central count areas
  - Infrastructure physical security control validation
    - Lock/keyed server cabinets
    - Lock/keyed networking cabinets
    - Access controls to sensitive areas (lock/keys, badge access etc.)
    - Monitoring and response (CCTV, alarms, on duty guards)
    - Disposal of election materials: secure paper bins, secure trash dumpsters
    - Fire suppression
    - Redundant power
    - Physical security mitigations, (lock/keys, port security, seal validation)
  - Business continuity and disaster recovery
    - Backup solution examination
    - Risk analysis for election disruption sources
    - Emergency and cybersecurity response plans
- Policy Auditing
  - Written security policies
  - Policy for sensitive objects and data control
  - Access control policy
  - Incident response policy
  - Security breach policy
  - Disposal/decommissioning policy for election systems
  - General IT Policies (access, password, usage, etc.)
  - Visitor/guest access policy

Pre-Election Configuration Verification and Assessment Audit

Prior to the election, SLI Compliance conducts a verification of the vendor setup and deployment documentation to make sure that the election system is correctly deployed per the vendor’s documentation and that the setup follows all documented processes, procedures and recommendations.

The SLI Compliance team also verifies that only certified or expected versions of the software and no unauthorized software is present on the election solution that could compromise the integrity of the systems. We pay particular attention to any aspects of the overall design that could place the system at risk. FIPS compliant hashing algorithms are used to confirm that the software and data have not been modified in any manner from the originally tested baseline.

SLI Compliance pre-election auditing tasks are available on the following component types: Precinct Optical Scanner, Precinct Ballot Marking Device (BMD), Precinct Hybrid Optical Scanner/BMD, Precinct Direct Recording Electronic (DRE) device, Precinct Ballot on Demand (BOD) printer, Precinct Electronic Pollbook, Precinct Network, Central Count Scanner, Central Count Election Management System (EMS), Administrative Workstation, Central Count peripheral/miscellaneous equipment/workstation, Central Count Network, Election Night Reporting System and Voter Registration Database.

Our wide selection of **pre-election** configuration verification and assessment audit tasks includes the following:

- Jurisdiction policy and procedure documentation audit
- Voting system vendor policy and procedure documentation audit
- Baseline imaging of electronic storage
- Firmware correctness/hash validation
- Environment correctness (all resident files valid/expected, no invalid/unexpected files)
- Configuration settings correctness (all configuration settings correct and appropriate)
- Hardware correctness (all resident hardware is valid/expected, no invalid/unexpected hardware)
- Telecommunications check (no unauthorized telecom enabled)
- Port exposure check (no ports (usb, lan, etc.) left unprotected
- Physical access control check (all physical access paths are protected)
- Programmatic access control check (all programmatic access paths are protected)

Post-Election Voting System Forensic Assessment and Audit

SLI Compliance compares the static and semi-static files of the voting system and each of its components through before and after images to ensure the system is functioning and tabulating according to specified parameters. We confirm that election systems haven't been compromised and don't contain unauthorized updates, which includes unauthorized software, malicious software or scripts which may adversely affect or change the systems. SLI Compliance identifies all added, altered, or deleted files, programs, scripts, or other operating components.

SLI Compliance post-election auditing tasks are available on the following component types: Precinct Optical Scanner, Precinct Ballot Marking Device (BMD), Precinct Hybrid Optical Scanner/BMD, Precinct Direct Recording Electronic (DRE) device, Precinct Ballot on Demand (BOD) printer, Precinct Electronic Pollbook, Precinct Network, Central Count

Scanner, Central Count Election Management System (EMS), Administrative Workstation, Central Count peripheral/miscellaneous equipment/workstation, Central Count Network, Election Night Reporting System and Voting Registration Database.

Our wide selection of **post-election** voting system forensic assessment and audit tasks includes the following:

- Imaging of electronic storage
- Firmware correctness/hash validation
- Environment correctness (all resident files valid/expected, no invalid/unexpected files)
- Configuration settings correctness (all configuration settings correct and appropriate)
- Hardware correctness (all resident hardware valid/expected, no invalid/unexpected hardware)
- Telecommunications check (no unauthorized telecom enabled)
- Port exposure check (no ports (usb, lan, etc.) left unprotected)
- Physical access control check (all physical access paths are protected)
- Programmatic access control check (all programmatic access paths are protected)

Additional Offerings, Cybersecurity Assessments

In addition to our Environment Audits, Pre-Election Audits and Post-Election Audits described above, SLI Compliance completes a wide range of cybersecurity assessments with the goal of examining the jurisdictional security controls to determine how well the election system mitigations stand up against vulnerabilities and security threats to the democratic process. There are two different generalized assessment types provided by SLI Compliance listed below. These assessments may be done individually or as a complete security assessment to verify and validate the overall security posture of the in-place election system.

Vulnerability Assessment

This assessment identifies risks and vulnerabilities in computer networks, systems, hardware, applications, and other parts of the election system infrastructure. Vulnerability assessments provide jurisdictions and other stakeholders with the information they need to analyze and prioritize risks for remediation. Vulnerability assessments are a critical component of the vulnerability management and election risk management lifecycles, helping protect systems and data from unauthorized access and data breaches. These assessments allow states and or jurisdictions to apply a consistent, comprehensive, and clear approach to identifying and resolving security threats and risks.

Benefits of a vulnerability assessment:

1. Early and consistent identification of threats and weaknesses in security
2. Remediation actions to close any gaps and protect sensitive systems and information
3. Protection against data breaches and other unauthorized access

Penetration Testing

A penetration test is an evaluation of election infrastructure security controls by attempting to safely exploit identified vulnerabilities. The testing includes the use of both manual and automated technologies to systematically compromise systems and devices within the election system infrastructure. Once systems are compromised, the testers usually attempt to use the compromised systems and devices to compromise other internal systems. A penetration test allows states and jurisdictions to test the security controls of their election systems against malicious attackers, in a safe controlled environment, while being able to identify and mitigate vulnerable systems and weakness.

Reasons why penetration testing is important:

1. Allows for identification and prioritization of security risks
2. Provides for the efficient management of vulnerabilities and threats
3. Fosters a proactive security approach over a reactionary approach
4. Verifies that current security programs and policy are working
5. Reinforces confidence in the security strategy
6. Helps ensure conformance to regulatory requirements

Why SLI Compliance

- SLI Compliance has extensive knowledge of the voting and elections industry including practical application of its promoted standards and best practices and provides an end-to-end understanding of the election process.
- SLI Compliance is accredited by the U.S. Election Assistance Commission (EAC) as a Voting System Test Laboratory (VSTL) and has been an Independent Test Authority (ITA) since the National Association of State Election Directors (NASED) first established an ITA certification program in 2001.
- SLI Compliance is accredited under the National Voluntary Laboratory Accreditation Program (NVLAP) of the National Institute of Standards and Technology (NIST) (NVLAP Lab Code 00733-0: TESTING).
- SLI Compliance also serves as a member of the Election Infrastructure Sector Coordinating Council (EI SCC), led by the Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security (DHS).

- SLI VSTL staff maintains security and internationally recognized software testing certifications including CTFL, CISSP, and CEH.

Statement of Independence

The SLI Compliance Voting Systems Compliance Testing Statement of Independence reads as follows:

The management and staff of SLI Compliance, along with SLI Compliance's testing subcontractors and their employees, shall maintain an independent decisional relationship between themselves and SLI Compliance's clients, affiliates, or other organizations so that the Company's capacity to render test reports objectively and without bias is not adversely affected.

SLI Compliance, along with SLI Compliance's testing subcontractors and their employees, shall maintain independence from Voting System Manufacturing clients whose systems are under VSTL test or are scheduled for a VSTL voting system test campaign. Specifically, employees shall not have a direct beneficial interest in a voting system product. In addition, as a VSTL:

- SLI Compliance will not perform engineering development work on voting systems.
- The Test Laboratory, whether on-site at SLI Compliance, at SLI Compliance's testing subcontractors' facility, or at a client's site, shall be organized so that staff members are not subjected to undue pressure or inducement that might influence their judgment or the results of their work.
- All staff involved in any way with voting systems Manufacturers must avoid even the appearance of conflict of interest in all verbal and written communications with voting system Manufacturers, and their employees, officers, agents and representatives. Statements to any person who is not a member of SLI Compliance's management or the SLI Compliance testing team working on a particular testing project that may be understood as predicting or anticipating any testing results, whether general or specific, express or implied are prohibited.
- All employees or contractors of SLI Compliance involved in the testing of voting systems are required to attend SLI Compliance's Laboratory Independence Training and sign the SLI Compliance Laboratory Independence Policy Acknowledgement form when hired and annually thereafter.

For further information about our services please contact us at 844-754-8683 or

Email: info@slicompliance.com.

www.SLICompliance.com