...safeguard your systems, and your reputation.

SLI COMPLIANCE®

VOTING SYSTEM SECURITY TESTING

In today's world, system security is a top priority in any voting and election program. So, how can you be sure that your voting systems and technologies are secure? Fortunately, there's SLI Compliance. We offer end-to-end security test methods designed to validate the security and privacy of all aspects of your voting system.

SECURITY TESTING

Our focus is on vulnerabilities that could compromise confidentiality, integrity, and availability of each aspect of the system, voter experience, election official experience, servers, and websites. Where risks are identified, we itemize corrective actions and compensating controls, including system configurations and architecture that can mitigate concerns.

SLI security staff analyzes the security techniques being used to ensure they are valid and that effective security procedures are contained in the design.

Security features are compared for validity against industry-standard techniques. The end-to-end security process is reviewed to identify any weaknesses in the security chain. We pay particular attention to any aspects of the overall design that could place the system at risk.

In addition to component or feature-level tests, our end-to-end security test methods are designed to validate the security of all aspects of the system. Testing can include voter registration, creation of ballots, transmission of ballots and receiving of marked ballots, recording and tallying of results, providing voter confidentiality, and the audit/recount process. Susceptibility to hacking, denial of service, modification of results, penetration testing, man in the middle, insertion of Trojan horses, ballot stuffing, modification of the ballot itself and votes marked on the ballot are all tested and verified.

IN TODAY'S WORLD, THE ABSENSE OF A PROPER SECURITY PROGRAM IS SIMPLY **NOT AN OPTION.**

With more than **191 million** compromised records, the December 2015 hack of the U.S. voter database counts as one of the largest online data breaches worldwide.

- Statista, The Statistics Portal

NVLAP®
TESTING
NVLAP Lab Code 200733-0

SECURITY SOFTWARE REVIEWS

Source Code is subjected to analysis using various tools to determine possible security risks. SLI checks the system to confirm methods exist to prevent issues like buffer overflows, pointers not being freed, penetration attacks, and unauthorized insertions of code.

Security algorithms and policies are reviewed to validate correct implementation. Our experience shows that industry-standard algorithms may be present, but if the policies are not correctly implemented, the system may not be as secure as stated.

Finally, we ensure that the code contains no hidden functionality, such as Trojan horses, conditional compilation flags, test flags, or hardcoded passwords.

TRUSTED BUILDS

The final reviewed source code is compiled and tested using a trusted build process to ensure that a clean environment is used and only approved elements go into the build.

SLI will perform a Trusted Build, using procedures provided by the voting system vendor, where source code is converted to machine-readable binary instructions (executable code) in a manner providing security measures that help ensure that the executable code is a verifiable and faithful representation of the source code.

When performing trusted builds SLI uses hash checking methods to confirm the software and data have not been modified in any manner from the originally tested baseline.

PRE-ELECTION CONFIGURATION VERIFICATION AND FORENSICS

SLI independently verifies and validates the systems to ensure only the proper versions of the software and no unauthorized software is present that could exploit vulnerabilities on the system. We sample hash codes from the Trusted Build and perform validation tests on the system onsite.

SLI conducts system audits and tests to ensure that the deployed system is identical to the certified baseline and that no improper data entry or security penetration occurred that would affect count accuracy. SLI conducts audits to ensure security techniques being used are valid and that effective security procedures are contained in the design. Security features are compared for validity against NIST Special Publications and ANSI Standards and Guidelines. SLI ensures that techniques being used are effective as built and can recommend enhanced techniques that should be implemented where needed.

Overall, the end to end security process is reviewed to identify any weakness in the security chain. SLI pays particular attention to any aspects of the overall design that could place the system at risk. SLI uses FIPS Compliant hashing algorithms to confirm the software and data have not been modified in any manner from the originally tested baseline.

Finally where risks are identified, SLI itemizes corrective actions and compensating controls, including system configurations and architecture that can mitigate risks.

POST-ELECTION CONFIGURATION VERIFICATION AND FORENSICS

SLI performs Forensic audits which compare 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.

SLI also ensures that the code contains no hidden functionality, back doors, Trojan horses, conditional compilation flags, test flags or hardcoded passwords.

SLI confirms the election system hasn't been compromised and does not contain unauthorized updates or any type of malicious applications, and identifies all added, altered or deleted files, programs, scripts or other operating components.

CONTACT SLI COMPLIANCE® TODAY

Helping to ensure elections are reliable, accurate, secure and transparent. That's SLI.

4720 Independence St • Wheat Ridge, Colorado 80033
slicompliance.com • info@slicompliance.com
844-754-8683

SLI COMPLIANCE®

A Division of GLI®, LLC