



Managing technology risk

Leveraging Testing Results Across Jurisdictions

**Mark Phillips – President & CEO
SLI Global Solutions**

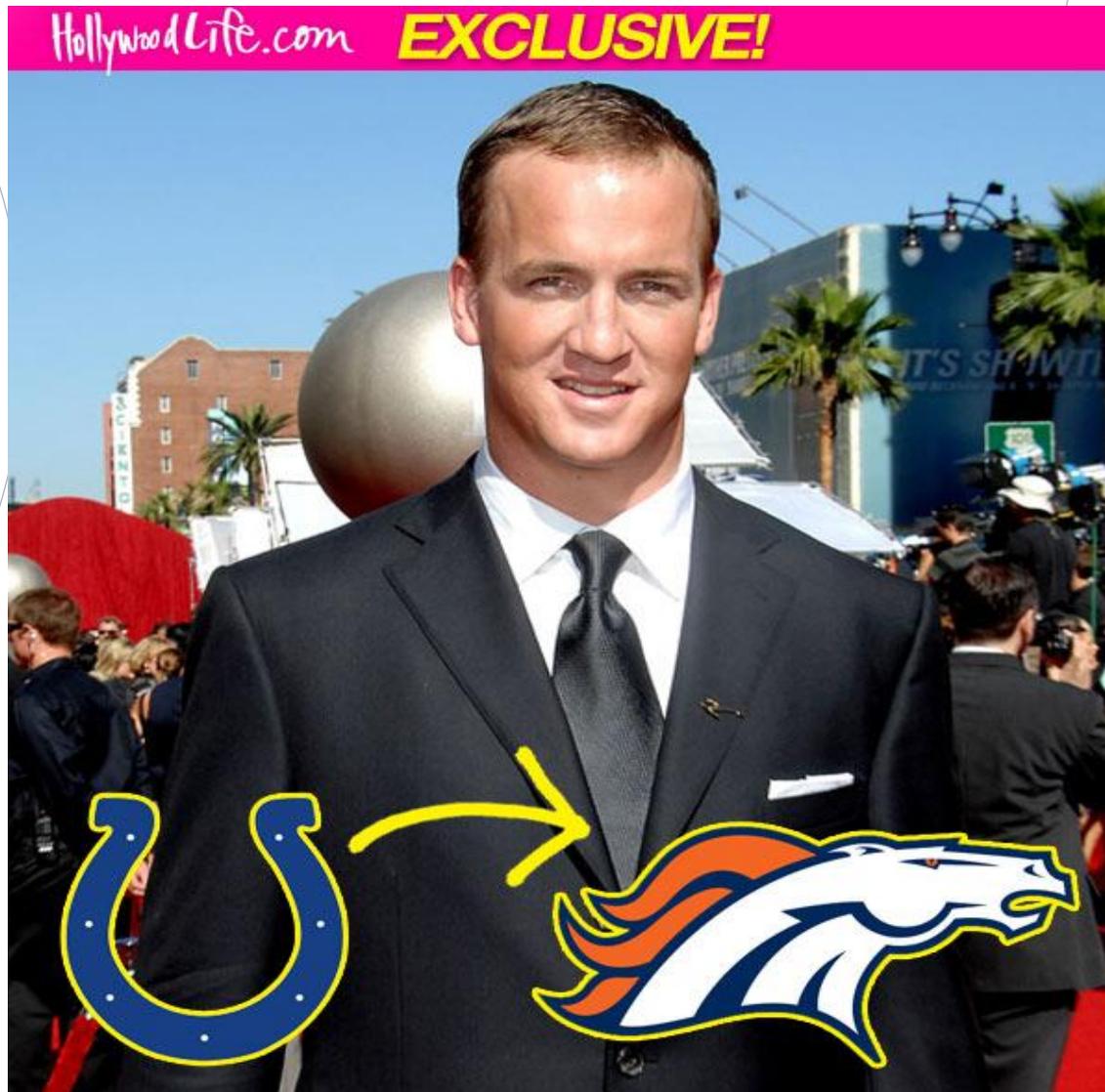
State Certification Testing of Voting
Systems National Conference

June 14-15, 2012



Greetings from the Mile High City

Managing technology risk





SLI Overview

Managing technology risk

- Testing, verification & validation, quality assurance services provided since 1996
- Accredited by the US National Institute of Standards and Technology to test voting systems using ISO 17025 standards
- Accredited by the United States Election Assistance Commission as a Voting System Test Laboratory (VSTL)
- In depth experience with most voting products used throughout the United States
- International voting system testing experience
- Remotely accessible Denver-based lab

State Requirements Vary

- 11 States Require Federal Certification
- 14 States Require Testing by a Federally Accredited Laboratory
- 10 States Require Testing to Federal Standards
- 15 States Have No Specific Federal Requirement





All Require Confidence in Election Results

- **Secure**
 - Protect against unauthorized manipulation; establish controls to minimize errors; identify erroneous changes; protect secrecy
- **Accurate**
 - Capture, record, store, and report ballot selections without error
- **Reliable**
 - Guard against improper information modification; ensure information non-repudiation and authenticity
- **Audit-able**
 - Record information in a way that it can be audited to verify steps followed without compromising voter secrecy

Managing technology risk



Challenge for Election Officials

Managing technology risk

- Ensure electronic election systems are secure, accurate, reliable & auditable
- Minimize overall expenditures for election support, including testing and certification, without compromising integrity

Leveraging Test Results



Managing technology risk

➤ Federal Testing

- Testing performed against the VVSG covers extensive technical requirements and standards
- Focus on unique state statutory requirements for any supplemental testing
- Consider sample verification audits of areas deemed most critical rather than doing a full scale test that may involve hundreds of hours of testing

Leveraging Test Results

➤ Re-use of Other State Testing Results

- Jurisdictions can take advantage of testing results published by other jurisdictions.
- Trace prior testing to required laws, technical requirements, election definitions & ballot types
- Maximize overall test coverage and minimize new test costs

Managing technology risk



Leveraging Test Results



Managing technology risk

- Review and Audit of Hardware Testing
 - Hardware testing can be costly
 - In the case of commercial off the shelf hardware, manufacturer test results are often available
 - Test reports from other accredited independent hardware labs may also be used
 - Validating these reports can give added confidence and reduce hardware testing costs

Leveraging Test Results



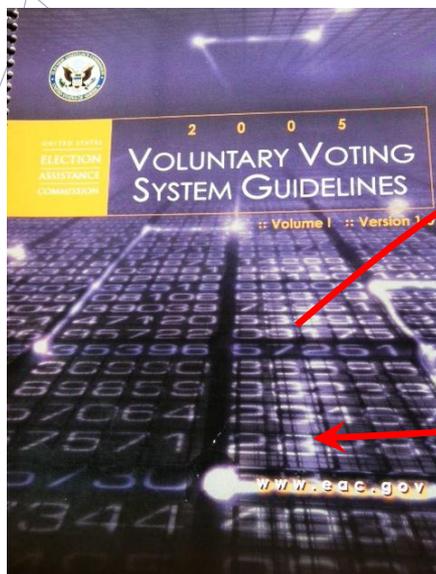
Managing technology risk

- **Review and Audit of Source Code Review Results**
 - Source code can include hundreds of thousands to over a million lines of code and can be very costly to review
 - Federal requirements allow the voting manufacturer to declare adherence to a industry accepted coding convention or be subject to the VVSG Volume II, section five requirements.
 - Making use of prior reviews provides a base for supplementary reviews to be conducted against additional standards if needed



Jurisdictional Requirement v. Federal Standards

Voting systems that undergo testing to the federal requirements are subjected to a considerable amount of testing and scrutiny. Determining how you can best take advantage of testing that has already been performed can create a significant cost savings for your jurisdiction.



Know how your own requirements trace to federal requirements.

Jurisdiction Requirements



Security

- Physical, Access Control, Software, Data Transmission and Telecommunications
- Validating these areas require specific expertise to ensure the testing is done properly

Managing technology risk



Accuracy

- Verify that the system accurately conducts and reports the results of all election types used
- Federal certification verifies accuracy of the system in less than ideal situations.
- Many states have particular requirements that often call for them to perform some type of accuracy testing
- Consider leveraging Federal testing to either eliminate or greatly reduce any additional testing cost



System Integrity

- Validating the integrity of the voting system to ensure its ability to withstand any data modification or deletion
- Federal standards verify that appropriate checks and non-repudiation mechanisms are in place
- Audit-ability provides re-assurance that anything and everything done within the election framework is known and recorded
- Election officials can reduce testing efforts by auditing a sample of what was done at the federal level and/or also including specific testing of their own jurisdiction's laws or requirements



Documentation

- Documentation review is very detailed and can be a cost driver
- A jurisdiction that maintains equipment itself may need more detail than a jurisdiction that plans to use outside support
- Election officials that anticipate creating election definitions themselves should look for documentation that clearly defines and illustrates the mechanics of the election management system

Source Code Review



Managing technology risk

- The ability to perform source code review requires a rigorous approach as well as knowledge of tools best suited for the purpose; “other duties as assigned” for development staff rarely yield reliable results
- Consider a source code verification audit on any source code review that was previously executed against the VVSG, rather than a new review
- Conduct additional reviews only against specific jurisdictional requirements, as applicable

Testing for Durability

- Federal standards test for durability, reliability, maintainability, and availability without excessive maintenance
- Commercial off the shelf hardware is commonly tested to these same standards; therefore auditing the testing already done by the manufacturer, or using Federal test results, can reduce hardware testing costs





State Examples

New York *(requires testing to federal standards)*

Leveraged available testing done for federal certification

- Reviewed source code review and documentation review reports to ensure the configuration and versions were of the same being used in NY and that the method for verifying the VVSG requirements was suitable
- Reviewed reported discrepancies and ensured the resolution was acceptable
- Conducted a sample code review and documentation review on an agreed upon percentage of the code
- Performed focused code review and documentation review against NY specific requirements.



State Examples

Oklahoma (no federal requirement)

Leveraged testing done by the vendor

- Performed an audit of the vendor's documentation and functional test results to verify compliance to Oklahoma's requirements
- Conducted readiness test and additional functional tests as deemed necessary by Oklahoma
- Compared source code from another version of code that had been previously reviewed and identified differences. Conducted a source code review focused on the modified code
- Reviewed hardware test reports from the hardware lab used by the vendor for VVSG compliance
- Conducted accuracy and security testing based on Oklahoma's requirements



State Examples

California (requires federal certification)

Oversaw testing conducted during federal certification

- VSTL test witnessing by a California representative:
 - Witnessed testing that was conducted by SLI to eliminate the need for additional testing to be done at the state

New Mexico (requires testing by a federally accredited lab) & **New Jersey** (no federal requirement)

Leveraged testing executed for another state

- Conducted source code review, identified areas of documentation review and hardware testing to the states requirements.
- Documented efforts that were previously preformed on the same system in the areas of documentation review, security and functional testing in the state's test report



What Testing is Appropriate for Re-use?

- Consider the configuration that was tested, and whether or not it's the same as what's being offered
- Is the documentation and source code of the same version? If not what are the differences?
- If you plan on using another entity's test results, make certain that they are a reliable source. A VSTL has not only been accredited by NIST/NVLAP but also by the EAC to do voting system certification testing
- If you use testing that has been done by another entity, make sure they are a qualified resource with experience in testing voting systems, and various voting configurations



Summary

- While each state is unique in their own laws and requirements, a large percentage of what is required in an electronic voting system is common to all jurisdictions
- This provides the opportunity to leverage the efforts of others that have already traveled down the certification path
- The effectiveness of a test and certification program does not need to be at odds with fiscal prudence and schedule needs



Managing technology risk

Questions and Answers

