Testimony of

Charles H. Romine, Ph.D.

Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives
Committee on Science, Space and Technology

Protecting the 2016 Elections from Cyber and Voting Machine Attacks

September 13, 2016

INTRODUCTION

Chairman Smith, Ranking Member Johnson, and members of the Committee, I am Dr. Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our key role in voting systems.

THE ROLE OF NIST IN VOTING SYSTEMS

With programs focused on national priorities from the Smart Grid and electronic health records to forensics, atomic clocks, advanced nanomaterials, computer chips and more, NIST's overall mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST's role in voting draws on our expertise in providing measurements, working with standards development organizations, and the development of testing and certification infrastructures necessary to support standards implementation.

Improving voting systems requires an interdisciplinary, collaborative approach. They must be accurate and reliable, yet cost-effective. They must be secure and usable. And, of course, they must be accessible to all voters, allowing them to vote independently and privately. Their design and the underlying standards must take into consideration the diversity of voting processes and ballots across the States. None of these can be considered in a vacuum. NIST expertise in testing and certification, information security, trusted networks, software quality, and usability and accessibility provides the technical foundation for our voting systems work, but our experience working in multi-stakeholder processes is also critical to this effort. We must bring together election officials, industry, technical experts, and advocacy groups to address this challenge. However, the NIST role is limited to the research to develop standards, tests, guidelines, best practices and assistance with laboratory accreditation that the Election Assistance Commission[1] (EAC), and state and local jurisdictions may use at their discretion. Further, neither the EAC nor NIST are empowered to regulate state and local electoral systems, and as NIST is a non-regulatory agency none of the guidelines and best practices offered by NIST are mandatory.

Historical Perspective

In 1974, the National Bureau of Standards (now the National Institute of Standards and Technology) began a research project funded by the Office of Federal Elections of the General Accounting Office. This project resulted in a 1975 report, later reprinted as NIST Special Publication (SP) 500-30, Effective Use of Computing Technology in Vote-Tallying. The report provided findings and conclusions about improving the accuracy and security of the vote-tallying process, improving the management of the election preparation process, and institutional factors affecting accuracy and security. The report also pointed out the lack of systematic research on election equipment and systems, and on human engineering of voting equipment, and it concluded that the setting of national minimum standards for federal election procedures would serve a valuable function.

[1] http://www.eac.gov/default.aspx.

Legislative Mandates

Since the signing of the Help America Vote Act of 2002[2] (HAVA) and reinforced by the Military and Overseas Voter Empowerment Act[3] (MOVE), the NIST Voting Program has partnered with the EAC to develop the science, tools, and standards necessary to improve the accuracy, reliability, usability, accessibility, and security of voting equipment used in federal elections for both domestic and overseas voters.

HAVA assigned three major items to NIST. First, NIST was assigned the development of a report to assess the areas of human factors research, which could be applied to voting products and systems design to ensure the usability and accuracy of voting products and systems. Second, NIST was tasked with chairing and providing technical support to the Technical Guidelines Development Committee (TGDC), Federal Advisory Committee to the EAC, in areas including (a) the security of computers, computer networks, and computer data storage used in voting systems, (b) methods to detect and prevent fraud, (c) the protection of voter privacy, and (d) the role of human factors in the design and application of voting systems, including assistive technologies for individuals with disabilities and varying levels of literacy. Third, NIST was to conduct an evaluation of independent, non-Federal laboratories and to submit to the EAC a list of those laboratories that NIST proposes to be accredited to carry out the testing.

The TGDC, first met in July 2004 to assist the EAC in the development of the voluntary voting system guidelines and established three subcommittees, focused on security and transparency; human factors and privacy; and core requirements and testing. The TGDC delivered its initial set of recommendations to the EAC in April 2005. Those recommendations, *Voluntary Voting System Guidance* (VVSG) 1.0, augmented the 2002 Voting System Standards by including security measures for auditability, wireless communications and software distribution and set up, and improvements for the accessibility guidelines and usability design guidelines for voting systems.

ACCOMPLISHMENTS

The NIST/EAC partnership is well over a decade old. Our joint accomplishments include:

- new voting system guidelines
- guidelines in support of MOVE and the Uniformed and Overseas Citizens Absentee Voting Act[4] (UOCAVA)
- the establishment of accredited testing laboratories for voting system equipment; and
- a testing and certification program upon which many states depend either in whole or in part.

VVSG: The Guidelines address many aspects of voting systems including determining system readiness, ballot preparation and election definition, voting and ballot counting operations, safeguards against system failure and protections against tampering, ensuring the integrity of voted ballots, protecting data during transmission, and auditing. The VVSG also address physical and systems level security. The Guidelines are used by accredited testing laboratories as part of both

[2] Pub. L. No. 107-252, (Oct. 29, 2002) 116 Stat. 1666, codified in relevant part at 52 U.S.C. 20901 et seq.
[3] Pub. L. No. 111-84, div. A, title V, (Oct. 28, 2009) 123 Stat. 2319, codified in relevant part at 52 U.S.C. § 20311.
[4] Pub.L.No. 99-410, title I, § 102, (Aug. 28, 1986), 100 Stat. 925.

state and national certification processes, state and local election officials who are evaluating voting systems for potential use in their jurisdictions, and by manufacturers who need to ensure that their products fulfill the requirements so they can be certified.

VVSG 1.0 also provided a set of specifications and requirements against which voting systems can be tested to determine if they possess the requisite functionality, accessibility and security capabilities. In addition, the guidelines established evaluation criteria for the national certification of voting systems. The VVSG and the related testing efforts, although voluntary for states, are in use in whole or in part by 47 out of 50 states. Work began on a new set of guidelines after the adoption of the VVSG 1.0. A draft of these guidelines was released for public comment in 2007 and, after much debate, many of the proposed guidelines were included the VVSG 1.1 This addressed new requirements for human factors, audit and election logging, quality assurance and configuration management, as well as new security requirements on access control, physical security, auditing, cryptography, software quality, and software integrity. In January 2015, the newly appointed EAC approved the latest version, deemed VVSG 1.1, or VVSG 2015.

UOCAVA: To support the Federal Voting Assistance Program's (FVAP) mission to help overseas and military voters exercise their right to vote, NIST has conducted research on the use of electronic technologies in the absentee voting process, including casting ballots over the Internet. To identify the potential risks, NIST produced NISTIR 7551, A Threat Analysis on UOCAVA Voting Systems, which analyzed the use of several electronic technologies for different aspects of the absentee voting process. This research concluded that widely-deployed security technologies and procedures could mitigate many of the risks associated with electronic blank ballot delivery, but that the risks associated with casting ballots over the Internet were more serious and challenging to overcome. Based on that research, NIST developed two additional documents covering security best practices for UOCAVA voting, NISTIR 7711, Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters and NISTIR 7682, Information System Security Best Practices for UOCAVA-Supporting Systems. These two documents serve as companion documents to one another. NISTIR 7711 provides security best practices and considerations for election officials on the use of electronic mail or Web sites to expedite transmission of voter registration materials and blank ballots. NISTIR 7682 provides best practices for those configuring and administering IT systems used to support UOCAVA voting. In early 2011, NIST released NISTIR 7770, Security Considerations for Remote Electronic UOCAVA Voting which studied Internet voting in more detail. This report identified and analyzed current and emerging technologies that may mitigate risks to Internet voting. It also identified several areas where additional research and technological improvements are needed to ensure the security, usability and accessibility of Internet voting. Many of these challenges are not unique to Internet voting, such as strong identity management, protection against malware, and the resiliency of Internet-connected systems. The unique challenges of Internet voting are the requirements and expectations – notably, ensuring the integrity of the voting process while also protecting voters' privacy.

Accredited Laboratories and Testing and Certification Program: Section 231 of HAVA requires EAC and NIST to develop a national program for accrediting Voting System Test Laboratories (VSTL) to conduct testing of voting systems and components, providing a measure of confidence that such laboratories are capable of performing testing to meet the requirements. A laboratory

achieving National Voluntary Laboratory Accreditation Program (NVLAP) accreditation is recommended by NIST to the EAC for designation as EAC-accredited VSTL. The EAC maintains a list of accredited VSTLs to help vendors and elections officials identify resources to fulfill system testing requirements. EAC-accredited VSTLs test voting systems for conformance with the voluntary voting system standards. Laboratory test reports are reviewed by the EAC for compliance with certification requirements. At this time, 47 states either require national certification or utilize the national standards when certifying voting systems.

In addition to national certification, state certification tests are performed to confirm that the voting system presented is the same as the one certified under the Guidelines.

- Acceptance tests are performed at the state or local jurisdiction level upon system delivery by the manufacturer to confirm that the system delivered is the specific system certified by the EAC and, when applicable, certified by the state.
- Election personnel conduct voting equipment and voting system readiness tests prior to the start of an election to ensure that the voting system functions properly, to confirm that voting equipment has been properly integrated, and to obtain equipment status reports.
- Election officials also perform verification at the polling place and any central locations used for vote counting to ensure that all voting systems and voting equipment function properly before, during, and after an election.

NIST works actively with the election community to support the development of tests used by the VSTLs for certification. Test assertions are measurable expressions that must be tested to evaluate conformance of an implementation (in this case a voting system) to a requirement. The goal of creating these test assertions is to make clear to testing laboratories and manufacturers of voting systems the specific conditions of each VVSG requirement that must tested to be certified by the EAC. Different testing laboratories, using this set of test assertions, should arrive at the same pass/fail results for each requirement in the VVSG, thus helping to ensure uniformity in testing among testing laboratories. These test assertions were developed by NIST and distributed to EAC and testing laboratories for their comments. For VVSG 1.0, NIST developed and updated, based on public comments, 1138 test assertions covering usability, accessibility and security requirements. For VVSG 1.1, there are an additional 597 test assertions, covering security and quality and configuration management in the review process.

RECENT ACTIVITIES

The VVSG development has been focused on developing guidelines for voting systems that are used on election day, for casting and counting ballots. After voters are checked in, they mark their ballots using one of three methods – electronic machines, ballot marking devices that produce a paper ballot, or directly on paper. New technologies are entering the marketplace, including those that support online voter registration systems, electronic pollbooks (e-pollbooks), electronic ballot marking, ballot on demand, ballot delivery, election reporting and auditing. These systems replace paper-based equivalents with electronic methods, with an increased use of tablets and connected or online options.

There is much debate over whether these election systems should be addressed in the VVSG and thus require federal testing and certification. It is clear that additional guidance is necessary to secure increasingly connected or online systems. The move towards tablets provides superior

usability and accessibility features, but requires new guidelines to allow all voters to vote independently and privately using these new devices, new interfaces, and new modes of interaction. Interconnected systems must also be able to communicate among components using standard protocols.

Open and Transparent Process

In February 2015, NIST and the EAC cosponsored the second of two symposiums aimed at ensuring that the technology and standards for voting systems support verifiable, fair elections, an essential element of our U.S. democracy. The first symposium, in February 2013, brought together election officials, voting system manufacturers, test labs, standards developers, researchers, and advocates to discuss standards and conformance testing processes that are needed to best accommodate future voting systems and the needs of election officials and voters. The theme of the second Symposium was "The People, The Process, The Technology". The purpose was to ensure we are responding appropriately to the many recent changes in voting technology and are prepared to respond to future updates. More than 540 government, industry, and academic representatives attended the workshop, and/or participated via live webcast.

NIST and the EAC organized public working groups that provide an open and transparent development process and gives the EAC and state election officials the opportunity to work directly with academic, industry, and federal government experts. The working groups help inform NIST, the EAC and the TGDC in creating a new version of the VVSG. The creation of the working groups was done as a direct response to feedback received from the Presidential Commission on Election Administration[5], EAC Standards Board as well as from the National Association of State Election Directors[6]. Each of these groups expressed interest in being involved in the process throughout the development, rather than only after the draft standard is released for public comment. This new process allows the working groups to take advantage of the expertise of the many election officials and other subject matter experts across the country who are willing to volunteer their time and offer their input.

There are three election working groups (pre-election, election and post-election) that are providing insight on election processes via the development of models and assessing the impact of integrating electronic equivalents into their processes. These groups are supported by four technical groups covering cybersecurity; human factors, including accessibility and usability; interoperability; and testing. The election working groups take input from the technical groups to inform requirements development for consideration by the TGDC. There are currently more than 400 members across the seven public working groups.

Our common goal, of course, is to ensure that the next generation of technology and standards for voting systems support verifiable, fair elections. Through the election working groups, we've already made progress in:

- creating a detailed understanding of elections through the creation of process models,
- identifying what well-established procedures are already in place, and
- documenting how technology is playing an increasing role in the election processes.

[5] https://www.supportthevoter.gov/
[6] https://www.nased.org/

Using the election models as input, the TGDC has discussed the increased use of digital systems and has identified several areas for additional investigation. These areas include: voter registration databases, e-pollbooks, ballot delivery, ballot on demand, ballot marking, election-night reporting, and auditing. NIST developed a set of use cases that further explored possible scenarios within these areas. The technical working groups are now reviewing the VVSG with a focus on these use cases, performing a gap analysis, and providing work plans for the development of new guidelines.

NIST has designed a new approach to developing standards for emerging voting system technologies based on a structure of high level principles and guidelines that is more responsive to rapidly changing technology and the needs of election officials. This structure is useful in identifying gaps in the existing requirements and also provides a design for the next generation VVSG document that will provide a more intuitive way for election officials as well as advocates, developers, and test labs to find, understand, and navigate the guidelines, requirements, and test assertions.

Usability and Accessibility

In 2015, NIST funded development of a roadmap for improving the usability and accessibility of next generation elections, with input from a cross-section of election officials, advocacy groups, academics, and the EAC. Following this roadmap, the human factors technical working group is addressing accessibility and usability issues and requirements that pertain to where voters, poll workers, and election officials interact with the electronic voting system at the polling place. The working group developed a set of five human factors voting principles with supporting guidelines and are using these to guide the their discussions about requirements for new voting system technologies. This structure has proven particularly useful in identifying gaps in the existing usability and accessibility requirements.

NIST also has worked with the election community to develop draft guidance in two other areas: (1) a protocol for testing the usability of e-pollbooks and a checklist for ease-of-use considerations that election officials can turn to when acquiring e-pollbooks and (2) usability, accessibility and security guidance for remote ballot marking to enable voters with disabilities to mark their ballots independently at home using their own assistive technology that can then be mailed or delivered to the polling place for casting.

Interoperability

The goal of the interoperability technical working group is to enable voting systems to become interoperable and thus assist election officials in having more choice in the market. A critical element to voting system interoperability, the Common Data Format (CDF) for election data, was initiated within the IEEE and is now being developed within the interoperability technical working group. Its first output, NIST SP 1500-100, constitutes an interoperable CDF for the election data commonly processed by election management systems, which includes election setup data (e.g., contest/candidate info, ballot preparation, political geography configuration) and election results data. This CDF was used by Ohio and the Associated Press for publishing and receiving its 2014 and 2016 primary and general election results and adopted by Google and Pew Research for use in their voting information projects; several other States and manufacturers have expressed their desire to use and support this format in products. The next CDF Specification, Draft NIST SP 1500-101 Election Log Export, addresses election system logging

and auditing and is being readied for publication. The group is working currently on three other CDF specifications:

- Voter Registration Data: for registration-related data imported and exported from voter registration systems and other sources such as the DMV.
- Cast Vote Records: for voted ballot data exported from voting devices and used for tabulation and election audits.
- E-Pollbooks: for data used in check-in at the polls and updates to voter records.

Cybersecurity

Ensuring that voting systems are secure and auditable is critical to providing trust and confidence in the voting process. To provide a firm foundation for next-generation security guidelines, NIST staff are researching threats and vulnerabilities to voting systems, and the security best practices and technologies that can mitigate those risks.

Software Vulnerabilities and Weaknesses: As part of that research, NIST has cataloged published vulnerabilities and weaknesses in voting system software using the Common Weakness Enumeration (CWE). The overarching goal of the work is to understand the types of vulnerabilities in voting systems by looking at historical evidence and creating a voting-specific list of vulnerabilities. CWE provides a common language for describing software security weaknesses in architecture, design, or code and is used worldwide in industry, government, and academia as a common method to communicate software vulnerabilities. Use of the CWE definitions can provide a common baseline for weakness identification, mitigation, and prevention efforts and can serve as a measurement for software security tools targeting those weaknesses. This research has identified over 250 weaknesses in the areas of authentication, cryptography, input validation, and privilege management. Further, NIST mapped these weaknesses to software security requirements in the VVSG 1.0 and VVSG 1.1. This work will provide valuable input to the VVSG development process, and has identified issues that should be addressed in future security requirements and test methods and by voting system manufacturers.

The *cybersecurity technical working group* is developing guidelines and best practices to secure voting systems, with the primary objective of contributing to the development of the next VVSG. The work of this group is intended to inform the decisions and activities of the TGDC and the election working groups. The group is currently focused on election security best practices, including physical security, auditing, and contingency planning. These discussions will inform future activities by NIST and the EAC. To support the development of the next version of the VVSG, the group is identifying security principles that will drive the development of new security requirements and test assertions. These principles are being derived from past versions of the VVSG, augmented by other cybersecurity guidelines and working group discussions. In the near-term, the group will also investigate a number of election use cases that were identified as priorities by NIST and the EAC working in collaboration with election officials. The group will consider security issues associated with each use case and identify gaps in the existing guidelines. This information will be used to scope and prioritize the next VVSG.

CONCLUSION

NIST is committed to continue collaborating with the EAC, the FVAP, election officials and others to fulfill our role defined in HAVA, MOVE and UOCAVA. We leverage our work in the areas of testing and certification, information security, trusted networks, usability, and software quality, which are applicable to a wide variety of organizations, and are used by industry and governments throughout the world. Active collaboration within the public sector, and between the public and private sectors, is the only way to effectively meet this challenge, leveraging each participant's roles, responsibilities, and capabilities.

Thank you for the opportunity to testify today on NIST's work in voting systems. I would be happy to answer any questions you may have.