

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
Subcommittee on Investigations & Oversight and
Subcommittee on Research & Technology

Election Security: Voting Technology Vulnerabilities

June 25, 2019

Introduction

Chairwoman Sherrill, Ranking Member Norman, Chairwoman Stevens, Ranking Member Baird and members of the Subcommittees, I am 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 role in what NIST is doing in election security.

NIST's Role in Cybersecurity

Home to five Nobel Prizes, with programs focused on national priorities such as advanced manufacturing, the digital economy, precision metrology, quantum science, and biosciences, NIST's 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.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, when it helped develop and published the data encryption standard, which enabled efficiencies like electronic banking that we all enjoy today. NIST's role, to research, develop, and deploy information security standards and technology to protect the federal government's information systems against threats to the confidentiality, integrity, and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347)¹ and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST develops guidelines in an open, transparent, and collaborative manner that enlists broad expertise from around the world. These resources are used by federal agencies and are frequently voluntarily used by other organizations, including businesses of all sizes, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective, state-of-art and widely accepted. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

The Role of NIST in Voting Systems

NIST's role in helping secure our Nation's voting systems draws on our expertise in providing measurements, working with standards development organizations, and the development of testing infrastructures necessary to support standards implementation.

Improving voting systems requires an interdisciplinary, collaborative approach. The systems must be accurate and reliable, yet cost-effective. They must be secure and usable. And, they

¹ FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347).

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, information security, trusted networks, software quality, and usability and accessibility provide the technical foundation for our voting systems work. Additionally, our experience working in multi-stakeholder processes is critical to success of NIST voting program.

For more than a decade, as directed by both the Help America Vote Act of 2002² (HAVA) and the Military and Overseas Voter Empowerment Act³ (MOVE), the NIST Voting Program has partnered with the Election Assistance Commission (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.

Under HAVA, NIST is tasked with providing technical support to the Technical Guidelines Development Committee, Federal Advisory Committee to the EAC to which the Director of NIST serves as Chair, in areas such as the security of computers, computer networks, and computer data storage used in voting systems, methods to detect and prevent fraud, protection of voter privacy, the role of human factors in the design and application of voting systems, and remote access voting, including voting through the Internet. This technical support includes intramural research and development in areas to support the development of a set of Voluntary Voting System Guidelines (VVSG or Guidelines), which upon recommendation by the Technical Guidelines Development Committee are forwarded to the EAC for further consideration prior to adoption via a quorum of EAC Commissioners. The Guidelines are used by accredited testing laboratories as part of both state and national certification processes; by 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.

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. Additionally, the Voluntary Voting System Guidelines tackles physical and systems-level security.

NIST Activities Related to Election Security

Voluntary Voting System Guidelines

The Guidelines is a set of specifications and requirements against which voting systems can be tested to determine if the systems meet required standards. On December 13, 2005, the EAC unanimously adopted the 2005 Guidelines, which significantly increased security requirements for voting systems and expanded access, including opportunities for individuals with disabilities to vote privately and independently. Version 1.1 of the Guidelines was unanimously approved by the Election Assistance Commissioners on March 31, 2015. Version 1.1 made the Guidelines

² Public Law 107-252, (Oct. 29, 2002), codified in relevant part at 52 U.S.C. 20901 *et seq.*

³ Public Law 111-84, div. A, title V, (Oct. 28, 2009), codified in relevant part at 52 U.S.C. § 20311.

more testable and improved portions of the guidelines without requiring massive programmatic changes.

Almost immediately following the adoption of Voluntary Voting System Guidelines 1.1, NIST, in consultation with the EAC, established a set of public working groups to gather input from a wide variety of stakeholders on the development of the next iteration of the Guidelines, entitled Voluntary Voting System Guidelines 2.0. This approach was consistent with NIST efforts in cloud and smart grid and served to address feedback from the Presidential Commission on Election Administration,⁴ the EAC Standards Board, and the National Association of State Election Directors,⁵ as well other subject matter experts across the Nation. There are currently 994 members across seven working groups, three of which are aimed at election process (pre-election, election and post-election), three groups focused on the technical underpinnings of the Guidelines (cybersecurity, usability and accessibility, and interoperability), and one that will address issues related to testing.

Election Security

The cybersecurity working group has grown to 175 members and engages in discussions regarding the security of U.S. elections. From the early 1900s, election administrators were primarily concerned with breaches of physical security, natural disasters, accidental errors, and events affecting public trust.

As U.S. election infrastructure has evolved, so have its security concerns, which today range from unauthorized attempts to access the voter registration systems of multiple states to errors or malicious software attacks. Guidelines 2.0 addresses these evolving concerns. It includes support for advanced auditing methods (such as risk-limiting audits) as well as enhanced authentication requirements. It mandates two-factor authentication for certain critical voting operations, including accessing administrative accounts, updating voting system software, performing aggregation of tabulation of ballots, enabling networking functions, and deleting or modifying the audit trail. Voting systems often use commercial off-the-shelf hardware and software. The system integrity section in Guidelines 2.0 ensures that security protections developed by industry over the past decade are built into the voting system.

Other security issues to be resolved, beyond those mentioned in the Guidelines, include the need for regular and timely software update and security patches. Networked communication is another important security issue currently under discussion. Many election jurisdictions rely on public telecommunications networks for certain election functions, such as reporting results to state agencies and media outlets the night of an election. These connections, however brief, are a significant expansion of threat surface and their security requires further study.

In January 2017, the Secretary of Homeland Security designated the Nation's election infrastructure as a critical infrastructure subsector of the Government Facilities Sector. Shortly thereafter, DHS established an Election Task Force to coordinate federal support to state and local governments regarding election security. NIST participates in the Election Task Force, recently recast as the Election Security Initiative Federal Partner Roundtable and is as an Ex

⁴ <https://www.supportthevoter.gov/>

⁵ <https://www.nased.org/>

Officio member of the Election Infrastructure Subsector (EIS) Government Coordinating Council, alongside our federal, state, and local partners. In support of these efforts, NIST is providing technical leadership in the creation of an Election Profile of the Cybersecurity Framework.

With our partners at DHS, NIST kicked off the Election Profile of the Cybersecurity Framework effort in March 2019 by establishing a joint subcommittee of the EIS Government Coordinating Council and the Sector Coordinating Committee (SCC). NIST co-leads this effort alongside DHS and the private sector chair of the Sector Coordinating Committee. To orient the efforts of the joint committee, NIST provided training on the NIST Cybersecurity Framework and profile development. In addition to the groundwork discussions occurring through bi-weekly meetings of the joint subcommittee, NIST will hold face-to-face workshops in July and August to identify election processes and assets that need protection; threats from foreign control of technology vendors; available safeguards; techniques that can detect incidents; and methods to respond and recover. The Election Profile will serve as a one-stop cybersecurity playbook that matches cybersecurity requirements with operational methodologies across all election processes, from voter registration through election reporting and auditing. The profile can be used by Secretaries of State, state and local election officials to identify and prioritize opportunities to improve their cybersecurity posture. NIST expects that an initial draft of the Election Profile of the Cybersecurity Framework will be available in the Fall of 2019.

Testing

NIST is responsible, under HAVA, for conducting evaluations of independent, non-federal laboratories and submitting to the EAC a list of the laboratories that NIST proposes to be accredited to carry out testing, certification, decertification, and recertification of voting systems.

NIST developed “test assertions” for critical security, usability, accessibility and functional requirements under Voluntary Voting System Guidelines 1.0 and 1.1. It is anticipated that accredited voting systems laboratories will use these NIST-developed test assertions to achieve uniformity in testing among laboratories.

Conclusion

NIST is addressing election security by strengthening the Voluntary Voting System Guidelines for voting systems, such as vote capture and tabulation, and by working with our government partners, including the EAC, to provide guidance to state and local election officials on how to secure their election systems including voter registration and election reporting systems.

Thank you for the opportunity to testify on NIST’s work regarding election security. I will be pleased to answer any questions you may have.