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 Senate
Committee on Rules and Administration

"*Election Security Preparations: Federal and Vendor Perspectives*"

July 11, 2018

Introduction

Chairman Blunt, Ranking Member Klobuchar, and members of the Committee, 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.

The Role of NIST 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 also coordinates with numerous other federal agencies, as well as its sister bureaus within the Department of Commerce. For example, as the executive branch agency principally responsible for advising the President on telecommunications and information policies, the Commerce Department's National Telecommunications and Information Administration, collaborates with NIST to ensure that the equities of innovation, economic growth, and an open Internet are factored into cybersecurity policy decisions within both domestic and international fora.

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 as well as 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.

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

NIST Cybersecurity Framework

I would like to highlight some changes to a document that the Committee may be familiar with: the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"), which many organizations—including many state governments—use to manage their cybersecurity risk. Beginning in 2013, NIST created, promoted, and continues to enhance the Framework in collaboration with industry, academia, and other government agencies. The Framework consists of voluntary standards, guidelines, and practices to promote the protection of critical infrastructure. The Framework's voluntary, risk-based, flexible, repeatable, and cost-effective approach helps users manage their cybersecurity risk. The Framework was originally designed for owners and operators of critical infrastructure, but organizations of all sizes and from many economic sectors now use the Framework to manage their cybersecurity risks, including risks to their supply chains. While use is both voluntary and widespread in the private sector, the Executive Order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," formally requires agencies to use the Framework to manage their cybersecurity risk – something many agencies did prior to its issuance.

In response to stakeholder requests, NIST began the public engagement process to update the Framework. This process included NIST examining lessons learned from use of the Framework, collecting written comments, hosting multiple workshops, incorporating comments and feedback, and issuing multiple drafts before publishing the final updated version 1.1 in April 2018. The Framework continues to be a living document which draws strength from active and voluntary private-sector contributors.

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 stakeholder communities, 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 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 the success of NIST's voting program.

For more than a decade, as directed by both the Help America Vote Act of 2002[2] (HAVA) and the Military and Overseas Voter Empowerment Act[3] (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.

[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.

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. This support includes 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 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 a 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, where NIST convened groups of stakeholders to gather input, 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 963 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.

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

Election Security

The cybersecurity working group has grown to 162 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 voting systems have evolved, so have their security concerns. Guidelines 2.0 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, and enabling networking functions. 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 critical infrastructure, making it a subsector of the Government Facilities Sector. NIST participates as an ex officio member of the Election Infrastructure Subsector Government Coordinating Council, alongside our federal, state, and local partners. In support of this effort, NIST is providing technical leadership in the creation of an Election Profile of the Cybersecurity Framework. This profile is another tool NIST is developing to help election officials identify and prioritize opportunities to improve their cybersecurity posture.

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 functionality 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.

Charles H. Romine

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL, one of seven research Laboratories within the National Institute of Standards and Technology (NIST), has an annual budget of $150 million, nearly 400 employees, and approximately 200 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission, 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.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the Nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology.

Education:
Ph.D. in Applied Mathematics from the University of Virginia.
B.A. in Mathematics from the University of Virginia.