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 Research and Technology and
Subcommittee on Oversight

"Is the OPM Data Breach the Tip of the Iceberg?"

July 8, 2015

Introduction

Chairwoman Comstock, Chairman Loudermilk, Ranking Member Lipinski, Ranking Member Beyer, and members of the Subcommittees, 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 one of our key roles in cybersecurity. Specifically, today I will testify about our responsibilities for assisting federal agencies with cybersecurity.

The Role of NIST in Cybersecurity

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.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, starting with the development of the Data Encryption Standard, when the potential commercial benefit of this technology became clear. Our role, to research, develop, and deploy information security standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services, was strengthened through the Computer Security Act of 1987, broadened through the Federal Information Security Management Act of 2002 (FISMA) and reaffirmed in the Federal Information Security Modernization Act of 2014.

Our Role under FISMA

At the time of the original FISMA bill, *House Report 107-787* stated the importance of NIST's approach to developing successful standards, guidelines and practices:

> ". . . open, transparent standards activities undertaken by NIST, such as the development and publication of the Advanced Encryption Standard, promote flexibility by permitting alternative hardware and software solutions to provide equivalent levels of protection and enable vendors to offer a variety of solutions to meet customer needs. By contrast, when standards development has not been open and the resulting NIST standard is not published and flexibly implementable, the standard has failed to gain broad acceptance and use."

NIST carries out its responsibilities under FISMA through the creation of a series of Federal Information Processing Standards (FIPS) and associated guidelines and practices. Under FISMA, federal agencies are required to implement these FIPS. NIST provides management, operational, and technical security guidelines for Federal agencies covering a broad range of topics, such as protecting the confidentiality of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations, BIOS management and measurement, key management and derivation, media sanitization, electronic authentication, security automation, Bluetooth and wireless protocols, incident handling and intrusion detection, malware, cloud computing, public key infrastructure, risk assessments, supply chain risk management, authentication, access control, security automation and continuous monitoring.

Beyond these documents - which are peer-reviewed throughout industry, government, and academia - NIST conducts workshops, awareness briefings, and outreach to ensure comprehension of standards and guidelines, to share ongoing and planned activities, and to aid in scoping guidelines in a collaborative, open, and transparent manner.

NIST has a series of very specific responsibilities called for in both the Federal Information Security Management and Modernization Acts, including the development of:

- A standard for categorizing information to be used by all federal agencies. The categories are based on the potential impact of harm to the organization if the information or information systems are compromised; and
- Minimum security requirements (*i.e.*, management, operational, and technical controls), for each information category.

In support of FISMA implementation, in recent years NIST has strengthened its collaboration with the Department of Defense, the Intelligence Community, and the Committee on National Security Systems, through the Joint Task Force Transformation Initiative, which continues to develop key cybersecurity guidelines for protecting federal information and information systems.

This collaboration allows for a broad-based and comprehensive set of safeguards and countermeasures for information systems. This unified framework provides a standardized method for expressing security at all levels, from operational implementation to compliance reporting. It allows for an environment of information sharing and interconnections among these communities and significantly reduces costs, time, and resources needed for finite sets of systems and administrators to report on cybersecurity to multiple authorities.

Federal Information Processing Standards and Mandatory Baselines

Of particular relevance to today's hearing are two FIPS developed by NIST to meet the specific requirements under FISMA:

- FIPS 199, the standard for security categorization of federal information and information systems; and

- FIPS 200, which sets minimum security requirements based on those categorization.

The minimum security requirements of FIPS 200 comprise a set of security controls that vary in breadth and depth depending on the importance of the information and information system to the mission of the agency.

NIST created three baselines for these minimum security requirements based on three categorization levels determined in accordance with FIPS 199: low, moderate, and high. These baselines are specified in our guideline documents and available tools. For example, at a "high" categorization, FIPS 199 states that "[t]he loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals."[1]

Examples of controls included in the associated baselines then cover a range of requirements for a lifecycle of security for any agency. Some specific examples include: security awareness and training; contingency planning; access controls; incident identification; incident response; and system disposal. Some controls call for specific technical implementations as well, such as the use of encryption, Domain Network Security Protocols, port locking, and white listing. Through an open and transparent process, these baselines are developed and updated collaboratively with our partners in government and industry.

Once a baseline is established, NIST provides guidance to agencies to assist them in determining that the baseline is adequate to meet their risk-based requirements. An agency may need to enhance a given baseline to address local risks and take into account that agency's mission and technical infrastructure. This enhancement might require that an agency substitute a specific control for another appropriate security mechanism.

For example, an agency with a real time monitoring system such as workstations in Air Traffic Control, pipe line pressure monitoring or critical patient monitoring systems might not want to use a timed, password locked screen saver to mitigate security issues for unattended workstations. Instead, use of a guard or site surveillance systems might be more appropriate to support the mission, and would allow that agency to meet the intent of the requirement in the baseline. In other words, while a

[1] The standard further amplifies this definition for agencies as follows: "A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries."

specific step recommended in the baseline may not fit an agency's needs, a complementary and compensating step can achieve the desired security outcome.

Establishing a sound security baseline is not the end of security for an agency, just as developing an IT system is not the end of an IT project. NIST provides standards, guidelines and tools for agencies to test and assess their security and then to continuously monitor their implementation and new risks. This process is essential to ensure the baseline is initially implemented correctly and remains appropriate as technologies, threats, and missions evolve. We stress that the authorization of a system by a management official is an important quality control under FISMA. By authorizing processing in a system, the manager accepts the associated risk. This causes that official to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.

Complying with FISMA

Under FISMA, NIST does not assess, audit, or test agency security implementations. Similarly, Congress has not accorded NIST with oversight authority. Congress recognized that placing such responsibilities on NIST would impede and ultimately defeat its ability to work with federal agency and private sector stakeholders to develop standards, guidelines and practices in the open, transparent, and collaborative manner Congress intended, as noted above in my testimony.

Accordingly, compliance and oversight authority resides with other agencies, such as OMB. Federal agency heads, in coordination with their Chief Information Officers and Senior Agency Information Security Officers, report the security status of their information systems to OMB in accordance with annual FISMA reporting guidance. In addition, agency Inspectors General provide an independent assessment of the security status of federal information systems, also reporting results to OMB annually.

NIST's statutory role as the developer – but not the enforcer – of standards and guidelines under FISMA has ensured NIST's ongoing ability to engage freely and positively with federal agencies on the implementation challenges and issues they experience in using these standards and guidelines. We meet frequently with agencies and hold regular Federal Security Manager Forums to discuss these issues, our standards and guidance, share lessons learned, and gain insights into methods and means to continually improve our standards, guidelines, and practices.

Conclusion

NIST is committed to continue to help agency officials address their responsibilities under FISMA to understand and mitigate risks to their information and information systems that could adversely affect their missions. We recognize that we have an essential responsibility in cybersecurity and in helping industry, consumers, and government to counter cybersecurity threats. Our work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of organizations, and is leveraged 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 federal cybersecurity. I would be happy to answer any questions you may have.

Charles H. Romine

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL is one of seven research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $150 million, more than 440 employees, and about 150 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program designed to promote U.S. innovation and industrial competitiveness 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.