Testimony of

James A. St. Pierre
Acting Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives
Committee on Oversight and Accountability
Subcommittee on Government Operations and the Federal Workforce

on

Login.gov Doesn't Meet the Standard

Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee, I am James St. Pierre, the Acting Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology – known as NIST. Thank you for the opportunity to testify today on behalf of NIST about how NIST develops guidance and about NIST's Digital Identity Guidelines (Special Publication 800-63).

NIST is home to five Nobel Prize winners, with programs focused on national priorities such as artificial intelligence, advanced manufacturing, the digital economy, precision metrology, quantum science, biosciences, and, of course, cybersecurity. The mission of NIST 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 Cybersecurity

In the area of cybersecurity, NIST has worked with federal agencies, industry, international partners, and academia since 1972, when it helped develop and published the Data Encryption Standard, which enabled efficiencies with security, like the electronic banking that we all enjoy today. NIST's role is to provide standards, guidance, tools, data references, and testing methods to protect information systems against threats to the confidentiality, integrity, and availability of information and services. This role 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.

Under the Federal Information Security Modernization Act (FISMA), NIST develops security standards and guidelines for non-national security federal agency systems, which may be made mandatory for federal agencies, as is the case for NIST Special Publication 800-63, Digital Identity Guidelines. NIST does not, however, oversee the adoption or implementation of its information security standards and guidelines by federal agencies, or ensure agency compliance where they are adopted.

In developing its guidelines, NIST prides itself on the strong partnerships we have developed, and relies on an open, transparent, and collaborative process that enlists broad expertise from government, industry, academia, and non-profit entities to develop and improve our cybersecurity resources. 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's Digital Identity Guidelines: Purpose and Process

NIST conducts research to better understand new and emerging technologies, their impact on existing standards, and the implementation of identity and access management solutions; leads in the development of national and international identity and access management standards, guidance, best practices, profiles, and frameworks; develops, issues, and improves identity and access management standards, guidelines, and resources; and produces example solutions that bring together the identity management and cybersecurity requirements needed to address specific challenges. Conducting research into emerging and applied methods of identity and access management is a priority for NIST, as is the maintenance of relevant standards and guidelines that can be implemented by organizations across government, industry, academia, and beyond.

As part of our program of research, NIST maintains and regularly updates its Digital Identity Guidelines (Special Publication [SP] 800-63). NIST first published its *Recommendation for Electronic Authentication (SP 800-63)* in 2004 in response to OMB Policy Memorandum 04-04, *E-Authentication Guidance for Federal Agencies*. This recommendation provided technical guidance to agencies implementing electronic authentication on how to allow an individual person to remotely authenticate their identity to a Federal Information Technology system. Since then, NIST has continued to follow an open and transparent process to update its guidance to reflect advances in technology, the evolving threat environment, new research, and implementation experiences.

The current final version of this guidance, SP 800-63 Revision 3, was published in June 2017. NIST SP 800-63 Revision 3 details a process for organizations' management of digital identity risk and use of digital identity products and services. These guidelines provide technical requirements for federal agencies implementing digital identity services. They can also be voluntarily adopted by non-federal organizations. The guidelines cover identity proofing and authentication – sometimes referred to as vetting or verifying the identities of individual users (such as employees, contractors, or private individuals) interacting with government information technology systems over open networks. It is important to note that the scope of the identities referenced in SP 800-63 is limited to individuals, and that the vetting of businesses or other organizations is out of scope for this publication.

The Guidelines detail a risk management process that seeks to achieve both interoperability and flexibility. SP 800-63 provides a common language and taxonomy to allow organizations to identify risks and select one of three defined groups of baseline controls, or "assurance levels," for identity proofing, authentication, and federation, depending on their assessment of their risk profile. Organizations that implement the guidance are allowed to select and implement compensating controls, provided they document their decision and offer a justification based on risk. In practice, this allows organizations implementing NIST's digital identity guidelines to review specific controls, such as remote biometric comparison or evidence requirements, and choose to document and implement comparable, alternative controls. In this way, the guidance is intended to maintain broad interoperability through the defined assurance levels, while allowing for modifications to meet organizational and mission-specific needs.

A draft of Revision 4 of SP 800-63 is out for public comment through April 14, 2023. NIST is following a robust engagement process to gain feedback from public and private-sector organizations, technology and professional services providers, academia, civil society, advocacy groups, and many others on how to improve the draft guidance and achieve a more secure identity ecosystem. These engagements include soliciting input through requests for information; hosting and participating in virtual and in-person conferences, workshops, and meetings; and seeking comment on public drafts of the guidelines.

Conclusion

NIST is proud of its role in establishing and improving cybersecurity solutions, standards, guidelines, and other resources, and of the longstanding and robust collaborations we've established with our federal government partners, private sector collaborators, and international colleagues.

Thank you for the opportunity to discuss NIST's activities related to our digital identity guidelines. I will be pleased to answer any questions you may have.

James St. Pierre

James A. St. Pierre is the Acting Director of the Information Technology Laboratory (ITL). ITL is one of six research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of approximately $160 million, nearly 400 employees, and about 200 guest researchers from industry, universities, and foreign laboratories.

As Acting ITL Director, St. Pierre oversees a research program designed to cultivate trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems. ITL supports the NIST mission of promoting 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. ITL also supports measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL seeks to enhance productivity and public safety, facilitate trade, and improve the quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is addressing the hard problems in IT Measurement Research. ITL's research results in fundamental and applied advances in Information Technology metrics, tests, guidance, and tools for a wide range of subjects including cybersecurity, quantum information science, artificial intelligence.

His work has been published in the NIST Journal of Research and in external publications. He has given hundreds of presentations on both technical and management topics, to both national and international audiences. Before joining NIST, in 1994, he worked as a technical project leader within Loral Space Systems semiconductor design group and worked for IBM on the development of hardware and software for Los Angeles-class submarines. In addition, he worked with several universities to develop their semiconductor design curricula.