NISTIR 8074
Volume 1

Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity

Prepared by the International Cybersecurity Standardization Working Group
of the National Security Council's
Cyber Interagency Policy Committee

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8074v1

National Institute of
Standards and Technology
U.S. Department of Commerce

This page left intentionally blank

NISTIR 8074
Volume 1

Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity

Prepared by the International Cybersecurity Standardization Working Group
of the National Security Council's
Cyber Interagency Policy Committee

NIST Editors:
Michael Hogan
Elaine Newton
Information Technology Laboratory

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8074v1

December 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Interagency Report 8074 Volume 1
22 pages (December 2015)

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8074v1

DISCLAIMER

Certain commercial entities may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities are necessarily the best available for the purpose.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

This interagency report sets out proposed United States Government (USG) strategic objectives for pursuing the development and use of international standards for cybersecurity and makes recommendations to achieve those objectives. The recommendations cover interagency coordination, collaboration with the U.S. private sector and international partners, agency participation in international standards development, standards training and education, use of international standards to achieve mission and policy objectives, and other issues. NISTIR 8074 Volume 2, *Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, provides additional background on international cybersecurity standardization.

Keywords

conformity assessment; coordination; cybersecurity; ICS; Industrial Control Systems; international standards; IT; information technology; privacy; standards education; strategy; SDO; standards developing organizations; standards development

This page left intentionally blank

Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity

Introduction

This report, which was drafted by the National Security Council (NSC) Cyber Interagency Policy Committee's International Cybersecurity Standardization Working Group for the Administration, sets out proposed United States Government (USG) strategic objectives for pursuing the development and use of international standards for cybersecurity, and makes recommendations to achieve those objectives. Implementation of these recommendations—which cover interagency coordination, collaboration with the U.S. private sector and international partners, agency participation in international standards development, standards training and education, use of international standards to achieve mission and policy objectives, and other topics–will enable the development and execution of a wide-ranging United States Government cybersecurity standardization strategy.

The Cybersecurity Enhancement Act of 2014 was signed into law by President Obama on December 18, 2014. Section 502 of the Act requires the Director of the National Institute of Standards and Technology (NIST) to work with relevant federal agencies to ensure interagency coordination "in the development of international technical standards related to information system security," and develop and transmit to Congress a plan for ensuring such coordination within one year of enactment. Further, the Act instructs NIST to ensure consultation with "appropriate private sector stakeholders." This report will also serve as the basis of the required report to Congress.

The Supplemental Information document (NISTIR 8074 Volume 2) provides additional background on the overall importance of standards and conformity assessment for global commerce and the status of international cybersecurity standardization.

Strategic Objectives

Given the increasingly global, complex, and interconnected nature of the world economy, characterized by rapid advances in technology and use of commercial off the shelf products to assure cybersecurity and resilience, the use of international cybersecurity standards for information technologies (IT)[1] and industrial control systems (ICS)[2] are necessary for the cybersecurity and resilience of all U.S. information and communications systems and supporting infrastructures.

- Cybersecurity is "the prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability."[3]

- Resilience is the ability of both the private sector and the government "to reduce the magnitude and/or duration of disruptive events [to critical infrastructure]. The effectiveness of a resilient infrastructure or

---

[1] *Information technology* (IT) means: "The art and applied sciences that deal with data and information. Examples are capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage, and retrieval of data and information." (*American National Standard Dictionary of Information Technology (ANSDIT)*, available at http://www.incits.org/standards-information/ [accessed 11/20/2015].)

[2] "*Industrial control system* (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures." (NIST Special Publication 800-82 Revision 2 *Guide to Industrial Control Systems (ICS) Security*, May 2015, p. 2-1. http://dx.doi.org/10.6028/NIST.SP.800-82r2.)

[3] U.S. Department of Homeland Security, *Blueprint for a Secure Cyber Future: the Cybersecurity Strategy for the Homeland Security Enterprise*, November 2011, p. D-2. Available at: http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf [accessed 11/20/2015].

enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event."[4]

Cybersecurity relies upon a diverse set of standards including standards whose scopes are specific to one or more attributes of cybersecurity and standards from other domains that are relevant to cybersecurity.

The U.S. standardization community is comprised largely of non-governmental Standards Developing Organizations (SDOs). These groups are primarily shaped by industry (both U.S. and foreign), academic institutions, professional societies, consumer groups, and nonprofits and are motivated by market forces, public interest, and consumer protection. USG participation is motivated by the need to achieve economic, timely and effective solutions for mission and policy objectives. These diverse motivations are mutually beneficial.

The U.S. Government strategy is to leverage these motivations in the development and use of international standards to promote cybersecurity and resilience. Consistent with the goals of the USG to promote secure cyberspace, there are four fundamental interrelated USG strategic objectives in actively participating in the development and use of timely international standards for cybersecurity:

1. **Enhancing National and Economic Security and Public Safety**

    - Ensuring that there is a sufficient inventory of international standards that can serve as a basis for the cybersecurity and resilience of U.S. organizations, particularly critical infrastructure. This includes both cybersecurity standards and standards from other domains that are relevant to cybersecurity.

    - Using international standards as a key part of USG procurement policy to support secure and resilient operations.

    - Ensuring that international standards meet the cybersecurity interests of the USG including protecting against illicit cyber activities or actions by terrorist groups, cybercriminals, and hostile nation-state actors.

2. **Ensuring standards and assessment tools for the USG are Technically Sound**

    - Supporting the development and use of new standards by taking into account: the scope of standardization work of candidate SDOs, U.S. industry preferences, USG needs, and the recent track record of candidate SDOs in particular areas of cybersecurity standardization.

    - Developing technically sound, reasonably available[5], and fit for purpose standards in open, transparent, and consensus-based processes, and updating as often as necessary in collaboration with the private sector.

    - Supporting coordination among SDOs to ensure consistency, avoid conflicting standards, promote interoperability, maximize the utility of standards projects, and extend the field of application for existing standards.

---

[4] National Infrastructure Advisory Council, *Critical Infrastructure Resilience Final Report and Recommendations*, September 8, 2009, p. 8. Available at: http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf [accessed 11/20/2015].

[5] The proposed revision to OMB Circular A-119 provides guidance on criteria for "reasonably available" under: **How should my agency determine whether a voluntary standard is "reasonably available" in a regulatory or non-regulatory context?**" (Office of Management and Budget, [*Proposed revision to OMB Circular A-119*], [February 10, 2014], p. 34. Available at: https://www.whitehouse.gov/sites/default/files/omb/inforeg/revisions-to-a-119-for-public-comments.pdf [accessed 11/20/2015].)

- Supporting the development and use of associated assessment tools (e.g., reference implementations, conformance and interoperability test suites) to complement timely, technically-sound standards development.

3. Facilitating International Trade

- Supporting the development and use of international standards and associated assessment schemes for cybersecurity (where relevant, effective, and appropriate), which can promote international trade and provide a level playing field for U.S. companies.

- Ensuring market relevance by developing standards in response to industry, government and consumer requirements and timelines.

4. Promoting Innovation and Competitiveness

- Supporting the development and use of international standards in collaboration with U.S. industry, to foster open and fair competition.

- Promoting the inclusion of existing and emerging technologies in international standards that boost U.S. competitiveness and ensuring that USG equities are well represented in those standards.

- Encouraging the development and use of performance-based standards for cybersecurity, where appropriate. Cybersecurity standards with performance-based requirements are more likely to encourage innovation and enable competition than standards based upon prescriptive design requirements. Prescriptive design standards are sometimes necessary, however, particularly for describing test methods or procedures.

Relevant Background on Standardization and Assessment

Background on standardization

For purposes of this report, a standard is a document, established by consensus and approved by a recognized body, which provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.[6] A standards developer is any organization that develops and approves standards using various methods to establish consensus among its participants. The use of such documentary consensus standards is voluntary.

Pursuant to U.S. laws and policy,[7] federal agencies are required to use voluntary consensus standards in their procurement and regulatory activities, giving preference to international standards, except where inconsistent with law or otherwise impractical. Many SDOs operate through a process that is characterized by all or some of the following attributes: openness, balance, due process, ability to appeal, and consensus. Openness means that the procedures or processes used are open to interested parties. Such parties are provided meaningful opportunities to participate in standards development on a non-discriminatory basis. The procedures or processes for participating in standards development and for developing the standard are transparent. The standards development process should also be balanced. Specifically, there should be meaningful involvement from a broad range of parties,

[6] See ISO/IEC Guide 2:2004, *Standardization and related activities - General Vocabulary*, November 1, 2004.
[7] See the National Technology Transfer and Advancement Act (NTTAA), as amended; OMB Circular A-119 Revised (Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities); and the Trade Agreements Act of 1979, as amended (TAA), July 26, 1979/December 8, 1994.

with no single interest dominating the decision-making. Due process should include documented and publicly available policies and procedures, adequate notice of meetings and standards development, sufficient time to review drafts and prepare views and objections, access to views and objections of other participants and a fair and impartial process for resolving conflicting views. An appeals process should be available for the impartial handling of procedural appeals. Consensus is defined as general agreement, but not necessarily unanimity. During the development of consensus, comments and objections are considered using fair, impartial, open, and transparent processes. These process attributes contribute to the technical soundness and market relevance of the published standards of an SDO.

The U.S. standards system differs significantly from the government-driven, centrally-coordinated standards systems common in many other countries. Within the United States, there are hundreds of SDOs, which are overwhelmingly private sector organizations, providing the infrastructure for the preparation of standards documents. USG personnel participate in SDO activities along with representatives from industry, academia, and other organizations and consumers. In many other countries' standards systems, the government plays a larger role in standards development-related activities, which provides those governments the ability to use standards to support domestic industrial and innovation policy, rather than to advance technical solutions in support of public policy goals. While Federal agencies possess certain responsibilities related to standards, such as in their own use of standards or in their development of technical regulations, there is a much greater reliance in the U.S. on the private sector, including companies and industry groups, academic institutions, professional societies, consumer groups, and other interested parties, in standards development. The United States Standards Strategy[8], elaborated through a private and public sector partnership in 2000, and revised most recently in 2010, outlines the contribution of private-sector led standards development to overall competition and innovation in the U.S. economy and the imperative of public and private sector participation that is a central tenet of the U.S. approach to standardization.

Background on conformity assessment

Conformity assessment is activity that provides demonstration that specified requirements relating to a product, process, system, person or body are fulfilled. Conformity assessment activities can be performed by many types of organizations or individuals. Conformity assessment can be conducted by: (1) a first party, which is generally the supplier or manufacturer; (2) a second party, which is generally the purchaser or user of the product; (3) a third party, which is an independent entity that is generally distinct from the first or second party and has no interest in transactions between the two parties; and (4) the government, which has a unique role in conformity assessment activities related to regulatory requirements.

For example, conformance testing captures the technical description of the requirements in a standard and measures whether an implementation (product, process or service) faithfully fulfills these requirements. Conformance testing alone does not completely ensure the interoperability or performance of conforming products, processes, or services. Therefore, interoperability and performance testing are also important aspects for procurements. Interoperability testing tests one implementation with another to establish that they can work together properly. Performance testing measures the performance characteristics of an implementation, such as its throughput[9] or response time,[10] under various conditions.

In some instances, testing and attestation of products, processes, and services against established cybersecurity standards may help provide a level of assurance that a product, process, or service's stated security claim is valid. An example is the USG requirement for using cloud products that meet Federal cloud security requirements. Commercial assessment organizations, which are accredited for assessing cloud security, determine if a cloud

[8] http://www.ansi.org/standards_activities/nss/usss.aspx
[9] Throughput is a measure of how much work the system can do in a given period of time.
[10] Response time is a measure of how quickly the system responds to a request for it to do something.

product conforms to the requirements. This can be more cost-effective for Federal agencies than developing in-house USG testing expertise.

Consistent with OMB Circular A-119, agencies retain the flexibility of choosing the appropriate conformity assessment programs—whether private, public, or some combination thereof—and tools to best achieve their objectives.

Other relevant legal and policy instruments

- The World Trade Organization (WTO) Agreement on Technical Barriers to Trade (TBT Agreement) – which has been implemented in U.S. law by the Trade Agreements Act of 1979, as amended (TAA)[11] – highlights the important role that international standards can play in facilitating trade and requires the use of relevant international standards, where effective and appropriate, in a Member's technical regulations. Although the TBT Agreement does not identify specific international standardizing bodies, the WTO Committee on Technical Barriers to Trade has identified several principles that functionally define international standards (i.e., standards developed in processes characterized by transparency, openness, impartiality and consensus, relevance and effectiveness, coherence and accounting for developing country interests).[12]

- The International Strategy for Cyberspace[13] lays out an approach to unify USG engagement with international partners on a full range of cyber issues. The International Strategy highlights the need to develop and use international cybersecurity standards and conformity assessment schemes, and the importance of public-private sector collaboration. The Strategy establishes the goal that "[t]he United States will work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation." The strategy contains policy priorities for the economy; protecting our networks; law enforcement; military; internet governance; international development; and internet freedom. This includes steps to enhance confidence in cyberspace and pursue those who would exploit online systems, and a commitment from the USG to participate actively in discussions about how international norms and measures on cybercrime are developed bilaterally and multilaterally, in fora with proven expertise and a history of promoting effective cybercrime policies. This also includes promoting processes to permit states to investigate, apprehend, and prosecute those who intrude or disrupt networks.

- The National Cooperative Research Act of 1984[14] first allowed organizations to collaborate to carry out joint research and development ventures and not be deemed illegal per se under federal antitrust laws or similar State laws. One result has been a rapid growth in IT consortia developing standards. In developing their standards, many of these consortia follow the WTO TBT Committee Decision principles. However, consortia are also formed that are not open, with membership by invitation. Consortia range from unincorporated affiliations of companies to incorporated entities with budgets, offices and paid staff. A consortium may exist to complete a specific standard, but others have a broader mission and develop multiple standards necessary to enable the evolution of a category of business services and products. An oft-cited advantage of IT consortia is speed in developing a standard, but speed is sometimes obtained due to a greater alignment in the technical interests of the participating entities. However, the narrow

[11] 19 U.S.C. § 2501 *et seq.*; http://uscode.house.gov
[12] WTO G/TBT/1/Rev.10, 9 June 2011, DECISIONS AND RECOMMENDATIONS ADOPTED BY THE WTO COMMITTEE ON TECHNICAL BARRIERS TO TRADE SINCE 1 JANUARY 1995.
[13] https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
[14] http://thomas.loc.gov/cgi-bin/bdquery/z?d098:SN01841:@@@L&summ2=m&

alignment of the interests of the participating entities may not represent a broad need, and this may slow uptake of the developed standard. At the same time, rapid innovation in emerging technologies has been accompanied by competition among SDOs to undertake new work areas in emerging fields of standardization that are perceived to be of great market relevance (e.g., smart grid, cloud computing, cybersecurity). This competitive environment has encouraged most SDOs to streamline their consensus building processes in order to develop and approve technically sound standards that meet current market needs in an effective manner.

- Memorandum M-12-08[15] on "Principles for Federal Engagement in Standards Activities to Address National Priorities" provides guidance to agencies with respect to their engagement in standards activities that have been identified as national priorities either through executive branch or Congressional actions. For example, "Agencies considering a convening or active engagement role in private sector standards developing organizations in order to address a national priority area should state their reasons plainly (including why private sector leadership alone is insufficient). Further, agencies should accept and act on feedback on their rationales before assuming this convening or active-engagement role in a private sector standards developing organization. In all cases, agencies should ensure effective intra- and inter-agency coordination of engagement in standards development activities. When an agency commits to a cooperative standards development effort with industry, that commitment should be maintained, as resources permit, and the resulting standards should be used where feasible. Agencies should use existing processes and, where necessary, establish new processes for open, transparent, and effective two-way communication with private sector interests, ensuring that concerns from private sector entities are given thorough and objective consideration. To the extent feasible and appropriate, agencies should also provide continuous support for their technical experts' participation and leadership activities in mission-critical standards-setting activities and standards organizations, including standards organization-specific training and mentoring. Agencies should periodically review their standards activities to identify gaps in representation for mission-critical areas as part of their long-range planning and adopt policies that value and reward participation in standardization activities."

Present State of International Cybersecurity Standardization

This section sets out core areas of cybersecurity that broadly influence the overall cybersecurity of products, processes, services, and organizations. USG technical experts have been participating in many core areas of cybersecurity standardization for decades. The resulting standards are largely being developed for the global marketplace generally and not just for federal networks and applications.[16] Such standards provide the requirements for cybersecurity standards-based products, processes or services. As a consequence of participating in this standards work, the USG has acquired and accumulated competency in core areas of cybersecurity standardization, but the depth and breadth of this USG competency can rise and fall with time.

Core areas of cybersecurity standardization include: cryptographic techniques; cyber incident management; identity and access management; IT system security evaluation; information security management systems; network security; security automation and continuous monitoring; supply chain risk management; software

[15] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08.pdf

[16] That said, the national and economic security of the United States depends on the reliable functioning of critical infrastructure, which is largely owned and operated by the private sector. Recognizing this, the President issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, in February 2013 (http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf). It directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices — for reducing cyber risks to critical infrastructure. NIST released the first version of the *Framework for Improving Critical Infrastructure Cybersecurity* (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf) on February 12, 2014. The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure by helping owners and operators of critical infrastructure to manage cyber security related risk.

assurance; and system security engineering. These areas, which are relevant for numerous applications, are discussed in detail in the Supplemental Information document (NISTIR 8074 Volume 2). Based upon legislative and policy mandates, there are a growing number of national priority applications for which the USG participates in the development of standards relevant to cybersecurity, including: cloud computing; emergency management; industrial control systems; health IT; smart grid; and voting. Such applications utilize cybersecurity standards in each of the listed core areas.

Worldwide, there are over 200 SDOs developing IT and ICS standards. Among those, there are dozens of SDOs developing cybersecurity standards, yet fewer SDOs may develop international cybersecurity standards. Some of the key SDOs directly involved in cybersecurity that may develop international standards are: the 3rd Generation Partnership Project (3GPP); the 3rd Generation Partnership Project 2 (3GPP2); the Alliance for Telecommunications Industry Solutions (ATIS); the Cloud Security Alliance (CSA); the European Telecommunications Standards Institute (ETSI); the International Electrotechnical Commission (IEC); the Institute of Electrical and Electronics Engineers (IEEE); the Internet Engineering Task Force (IETF); the International Society of Automation (ISA); the International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 (ISO/IEC JTC 1), Information Technology; the International Organization for Standardization Technical Committee 68 (ISO TC 68), Financial Services; the International Telecommunication Union Radiocommunication Sector (ITU-R); the Object Management Group (OMG); the OpenID Foundation (OIDF); the Organization for the Advancement of Structured Information Standards (OASIS); the Payment Card Industry Security Standards Council (PCI SSC); SAE International; The Open Group; the Trusted Computing Group (TCG); the World Wide Web Consortium (W3C); and the WiMAX Forum. Collectively, these SDOs have many hundreds of cybersecurity standards projects under maintenance or development. Being able to influence cybersecurity standards development requires developing and maintaining effective liaisons and active engagements within and among these SDOs.

Table 1 below provides an abbreviated, high-level snapshot of where standards are being developed and the present status of cybersecurity standards for some priority cybersecurity applications. This status information in Table 1 represents a high-level standards gap analysis. **"Standards Mostly Available"** indicates that SDO-approved cybersecurity standards are for the most part available and standards-based implementations are available. However, the availability of standards means that such standards require continuous maintenance and updating/replacing based upon feedback from testing and deployments of standards-based products, processes, and services, as well as improvements in technology and the exploitation of those improvements by those engaging in cybercrime and cyberespionage. **"Some Standards Available"** indicates that some standards exist and have standards-based implementations, but there may be a need for additional standards and/or revisions to existing standards in this area. **"Standards Being Developed"** indicates that needed SDO-approved cybersecurity standards are still under development and that needed standards-based implementations are not yet available. **"New Standards Needed"** indicates that new cybersecurity standards development projects are starting to be considered by various SDOs.

Four observations can be made on the overall status of ongoing cybersecurity standardization. First, robust standardization activities in the listed core areas of cybersecurity standardization are undoubtedly necessary for ensuring interoperability, security, usability, and resilience. Second, as illustrated by the listed applications in Table 1, there is a mix of ongoing standardization and maintenance of existing standards that is necessary to sustain deployments of standards-based products, processes and services. Third, the standards produced by SDOs represent a point in time. They often need to evolve in a way that meets the challenges of the ever-changing threat landscape. Finally, while Table 1 is structured by applications, there are some cybersecurity standards that apply across the applications to the development and manufacturing of IT products (hardware and software), products that most if not all of these applications depend on.

Notes on Table 1: Status of Cybersecurity Standardization

The ten listed core areas of cybersecurity standardization are important areas but are not all inclusive. An augmented taxonomy for core areas of cybersecurity standardization could be an area for further work. The six examples of key applications that depend upon cybersecurity are also not all inclusive. Many other applications could be added, such as automotive, financial services, mobile, and Internet of Things (IoT). However, the listed ten core areas and six examples of key applications are considered sufficient for the purposes of capturing a snapshot of the status of cybersecurity standardization.

Table 1: Status of Cybersecurity Standardization

Core Areas of Cybersecurity Standardization	Examples of Relevant SDOs	Examples of Some Key Applications					
		Cloud Computing	Emergency Management	Industrial Control Systems	Health IT	Smart Grid	Voting
Cryptographic Techniques	IEEE ISO TC 68 ISO/IEC JTC 1 W3C	Standards Mostly Available	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available
Cyber Incident Management	ISO/IEC JTC 1 ITU-T PCI	Some Standards Available	New Standards Needed	Some Standards Available	Some Standards Available	Some Standards Available	New Standards Needed
Identity and Access Management	FIDO Alliance IETF; OASIS OIDF ISO/IEC JTC 1 ITU-T; W3C	Standards Mostly Available	Standards Being Developed	New Standards Needed	Standards Being Developed	New Standards Needed	New Standards Needed
Information Security Management Systems	ATIS; IEC; ISA ISO/IEC JTC 1 ISO TC 223 OASIS The Open Group	Some Standards Available	New Standards Needed	Some Standards Available	Some Standards Available	New Standards Needed	New Standards Needed
IT System Security Evaluation	ISO/IEC JTC 1 The Open Group	Some Standards Available	Standards Mostly Available	Some Standards Available	Some Standards Available	Some Standards Available	Standards Mostly Available
Network Security	3GPP; 3GPP; IEC IETF; IEEE ISO/IEC JTC 1 ITU-T The Open Group WiMAX Forum	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available	Standards Mostly Available
Security Automation & Continuous Monitoring	IEEE; IETF ISO/IEC JTC 1 TCG The Open Group	Some Standards Available	Some Standards Available	New Standards Needed	Some Standards Available	New Standards Needed	New Standards Needed
Software Assurance	IEEE ISO/IEC JTC 1 OMG TCG The Open Group	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available
Supply Chain Risk Management	IEEE ISO/IEC JTC 1 IEC TC 65 The Open Group	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available
System Security Engineering	IEC IEEE ISA ISO/IEC JTC 1 SAE International The Open Group	Some Standards Available	Standards Mostly Available	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available

Key Challenges in Cybersecurity Standardization

Interagency and Private Sector Engagement

There are at least three active USG groups that provide for interagency coordination on standards-related matters. The Interagency Committee on Standards Policy (ICSP) provides advice and recommendations to the Secretary of Commerce and other Executive Branch agencies on matters related to standards policy that could impact Federal agencies' participation in, and use of, standards. The Technical Barriers to Trade (TBT) Subcommittee of the Trade Policy Staff Committee (TPSC), which is led by the Office of the United States Trade Representative (USTR), coordinates the development and implementation of USG positions relating to technical regulations, standards and conformity assessment procedures around the world. The JESC (Joint Enterprise Standards Committee) serves as the Department of Defense (DoD) information technology standards and Intelligence Community (IC) enterprise standards governance body. This forum collaborates and recommends common enterprise standards, profiles, and specifications for the respective DoD and IC information environments. Interagency coordination on standards-related matters also occurs in some subcommittees and working groups within the National Science and Technology Council (NSTC). Given the critical importance of cybersecurity standardization and its cross-cutting nature —which involves security, standards, innovation, competition, trade, privacy, law enforcement and national security, and other policy considerations –a higher-level interagency coordination mechanism is needed. Coordination by senior Federal cybersecurity officials under the auspices of the Executive Office of the President (EOP) would provide the necessary focus and resources to develop and implement a strategy for cybersecurity-related standardization, as well as ensure that the USG can respond to specific priority issues as they arise.

In addition to coordination among federal agencies, the USG needs to engage effectively with U.S. industry. There are several methods agencies use to engage and coordinate with external stakeholders. Agencies may choose to establish external advisory committees per the Federal Advisory Committee Act (FACA), seek input using Federal Register Notice solicitations, use specific statutory or regulatory authority to create a forum — such as a private sector coordinating council — for obtaining input, establish a public-private partnership, or use some other method that provides all potential stakeholders an equal opportunity to provide input and share their perspectives. As an example of FACA committees, the U.S. Department of Health and Human Services (HHS) created Health IT Policy and Standards committees that make recommendations to the National Coordinator on policy and standards topics, including cybersecurity. In addition, in developing the Framework for Improving Critical Infrastructure Cybersecurity under Executive Order 13636, NIST provided stakeholders with an equal opportunity to share their views and make contributions through a series of workshops and public comment periods on drafts.

For SDOs that use a national body member process, such as the International Organization for Standardization (ISO), there is already built-in U.S. coordination through U.S. mirror groups (e.g., U.S. Technical Advisory Groups (TAGs) for ISO technical committees and subcommittees). The State Department administers a FACA-based process for developing U.S. positions relating to standardization in the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T), a treaty-based United Nations organization. For SDOs that are based on an individual membership model, public-private sector coordination prior to technical committee meetings is not built-in, so this may be a particular area that could benefit from enhanced focus by the USG.

In carrying out these activities, it is important to prioritize resources and engagement to achieve maximum impact with various SDOs. The number of cybersecurity standards projects is substantial. Therefore, the USG needs to develop an engagement model to ensure that it is able to participate dynamically at the right level when necessary. The following four categories characterize possible levels of engagement and related resource planning needs:

- **Participating in limited specific activities** is following, contributing to, and/or leading a specific standards effort for a select activity(s) specific to unique needs or interests.

- **Monitoring** focuses on broader programs of work and emerging and evolving standards produced by the SDOs. It includes developing an understanding of, and relationships with, the key players.

- **Influencing**, in addition to the requirements of monitoring, involves commenting on, and providing contributions to, strategically important standards, working with industry and international players, and exerting influence through formal and informal discussions and provision of expertise.

- **Leading** involves the activities associated with monitoring and influencing and, additionally, providing leadership through roles such as convening or administering consensus groups, serving as the standards project editor, and serving as the liaison representative between standards groups. Such leadership roles require that the official act in accordance with the duties assigned by the SDO and not advocate on behalf of his or her agency or country.

All of these options require having qualified USG participants (whether USG employees or contractors) function in these capacities, based on their expertise, relationships, and knowledge of specific SDO processes and best practices.

Privacy

The protection of individual privacy promotes U.S. interests by facilitating improved trust in online and offline transactions and helping U.S. products and services compete in global markets. Cybersecurity is an important component of protecting privacy, and many privacy standards address the protection of personal data by cross-referencing standards in the area of information security management systems. Nonetheless, cybersecurity measures also can create privacy risks. Executive Order (E.O.) 13636[17] recognized this concern by requiring the National Institute of Standards and Technology (NIST) to include a methodology to protect privacy and civil liberties in the Framework for Improving Critical Infrastructure Cybersecurity.[18] The NIST Roadmap for Improving Critical Infrastructure Cybersecurity[19] referred to how few technical standards or best practices exist to mitigate the impact of cybersecurity activities on individual privacy and civil liberties. It is in the best interests of the USG to support the development and use of cybersecurity standards that minimize risks to privacy, promote information-sharing relating to cybersecurity, and allow the USG to combat cyber-enabled threats. Greater understanding of how to identify privacy risks and integrate mitigations into cybersecurity standards or their deployment in information systems will require further research.

Participation/Training/Education

[17] E.O. 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013 notes:
"Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards." (Section 1) http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[18] *Framework for Improving Critical Infrastructure Cybersecurity*, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[19] *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

Maintaining and, where needed, augmenting USG competency in the core areas of cybersecurity standardization require continuous education, participation and training. Obtaining a consensus to approve standards among participants in various SDOs usually requires more than a simple majority but less than unanimity. Effective negotiation in standards development requires not just technical expertise by Federal agency participants, but a thorough knowledge of an SDO's standards development process and policies, as well as soft skills in negotiating with stakeholders with a range of often diverse and conflicting positions. In addition, awareness of the relevant market and associated market politics that drive the motivations of the other participants is essential. For international fora, understanding the culture of the participants is also important. Accordingly, continuity in participation is crucial to success. Participants must regularly attend the meetings, have established relationships with the other participants, and ensure that the draft standards are technically sound and meet USG needs. Effective leadership in SDOs promotes timely development of technically sound standards.

Other countries are making sustained efforts to fund national participants in leadership positions, which could ultimately put U.S. industry at a disadvantage and/or limit the influence of the USG, to the extent that such participants are not acting in a neutral and unbiased manner with respect to governance issues and standards development. Therefore, it is in U.S. industry's interest to have competent and fair-minded USG representatives in SDO leadership roles.

It may be in the best interest of U.S. industry for the USG to take such leadership roles, especially when solicited by private sector participants. Federal agencies should support qualified Federal representatives (including contracted technical experts) in SDO leadership positions. Candidates for such leadership positions should be both technically knowledgeable and thoroughly familiar with the SDO's development processes and policies, and have a good understanding of USG and U.S. industry priorities and perspectives. Further, long-term participation of the same USG representatives within an SDO establishes trust and builds the credibility of those representatives. This is critical for effective communication and information-sharing and ultimately will assist in advancing the USG's strategic objectives in each SDO. In addition to effective participation and leadership by Federal agency representatives, Federal agencies, consistent with agency missions, need to coordinate their positions.

Lastly, leveraging strong government/private sector/university/professional society cooperation is needed to ensure the availability of USG expertise. Policies should be put in place to educate Federal agencies' management and technical staff on the need for continuity, cooperation, and effective participation in standards development. The USG should also support standards education in technical undergraduate and graduate educational programs, especially in computing, engineering, business, sciences, and technology to ensure the development of future generations of U.S. cybersecurity standards participants. Some initiatives that could be built upon include:

- The National Initiative for Cybersecurity Education (NICE)[20]: The goal of NICE is to establish an operational, sustainable and continually improving national cybersecurity education program that will develop sound cyber practices to enhance the nation's security. The scope of this program includes the Federal workplace, civilians, and students in kindergarten through post-graduate school.

- The NIST Standards Services Curricula Development Cooperative Agreement Program provides financial assistance to support curriculum development for the undergraduate and/or graduate level. This Program supports the integration of documentary and measurement standards and standardization information and content into seminars, courses, and learning resources.

[20] http://csrc.nist.gov/nice

- Many U.S. based private sector entities also run relevant standards education and curricular development activities and welcome USG participation and collaboration. These include, but are not limited to, the American National Standards Institute (ANSI), which has programs and content to raise awareness of the importance of standards and conformity assessment among university faculty in engineering, technology, business, public policy and law schools[21]. Similarly, the Institute of Electrical and Electronics Engineers (IEEE) runs a broad Standards Education program[22] to promote knowledge of standards and the importance of standardization among students. Other unique standards education-related resources are available from the International Organization for Standardization (ISO) at Education about standards[23]. The NIST Standards.gov web pages include standards training resources of agencies, SDOs, universities, etc.

- The *Framework for Improving Critical Infrastructure Cybersecurity*[24] developed under Executive Order 13636 provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services. The Framework relies on standards for its use, with "Informative References" containing specific sections of standards, guidelines, and practices common among critical infrastructure sectors. The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices that would help organizations address emerging needs.

Recommendations

Maintaining USG competency to participate effectively in the development of new or revised core cybersecurity standards areas provides the foundation to respond to ever-evolving USG priorities. The development of international standards for cybersecurity promotes U.S. interests by facilitating interoperability, security, usability and resilience; improving trust in online and offline transactions; promoting innovation and competitiveness; and helping U.S. products and services compete in global markets. Increased and more strategic and coordinated U.S. engagement in cybersecurity standardization will help promote U.S. interests by ensuring that standards-based requirements for cybersecurity products, processes, and services meet U.S. objectives. Ensuring effective U.S. leadership in the relevant standards developing bodies for cybersecurity requires awareness of specific SDO environments, coordination of USG interests with U.S. industry and organization interests to prioritize and achieve U.S. objectives, and a robust focus on education and training.

The following recommendations provide the basis for achieving overall USG strategic objectives in cybersecurity, which are derived from each agency's mission and objectives. They are representative of interagency consensus, achieved through the Presidential Policy Directive (PPD)-1 policy and provide the basis for guidance from White House leadership to Federal agencies.

Recommendation 1: Ensuring USG Coordination

- The USG should strengthen its high-level interagency coordination process for cybersecurity standardization.

    - Through the process established by PPD-1 (or its successors), the National Security Council should provide the forum for coordinating policy development related to cybersecurity standardization.

[21] http://www.StandardsLearn.org
[22] http://www.ieee.org/education_careers/education/standards/index.html
[23] http://www.iso.org/iso/home/standards/standards-in-education.htm
[24] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

- The U.S. Department of Commerce should host a subordinate interagency working group -- the International Cybersecurity Standardization Working Group –on behalf of the NSC interagency policymaking body. Such a group would comprise senior Federal cybersecurity officials with the expertise and bandwidth to develop and implement a set of objectives and strategies pursuant to USG agencies' missions, and to coordinate on major issues in standardization before and as they arise. Major policy decisions and areas of significant disagreement could then be addressed through the National Security Council process (namely the Cyber Interagency Policy Council).

- Such a mechanism should help to ensure that both internal agency and overall USG efforts are well coordinated, both within the USG and with relevant private sector stakeholders.

- Agencies participating in the work of specific SDOs would have an established interagency venue for developing objectives and strategies in concert with interagency colleagues, as well as raising, and where possible coordinating on, major issues.

Recommendation 2: Promoting USG Participation in Cybersecurity Standards Development

- Federal agencies should regularly highlight within their agencies the need to participate in standards development for cybersecurity in pursuit of their agency's mission and objectives.

- Federal agencies should support a long-term commitment of resources and participants with specialized knowledge, skills and abilities for international cybersecurity standardization.

- The USG should maintain and, where needed, augment its competency in core areas of cybersecurity standardization. As part of their long-range planning, Federal agencies should periodically review their standards participation to identify gaps in representation for mission-critical activities.

- Federal agencies should value and reward staff participation in standardization activities, encourage junior staff members to be involved in standardization activities, and provide mechanisms for recognition of effective participation by their technical experts.

Recommendation 3: Developing Timely and Technically Sound Standards and Assessment Schemes for Cybersecurity

- To help make standards projects more focused and timely, Federal agencies participating in the work of SDOs should make clear and comprehensive contributions with regard to the scope of cybersecurity standardization projects, as well as target dates to complete those projects.

- Federal agencies should make timely technical contributions to draft standards for cybersecurity to ensure that the resulting standards are technically sound.

- Federal agencies should support and coordinate on the timely development of conformity and interoperability assessment schemes for cybersecurity (including international schemes), whether by private or public sector bodies, to accelerate the development and use of technically sound standards and standards-based products, processes and services (e.g., the Federal Risk and Authorization Management Program (FedRAMP)[25], and where appropriate show preference in procurement for those suppliers that demonstrate conformance to such standards.

[25] http://www.gsa.gov/portal/category/102371

Recommendation 4: Leveraging U.S. Public and Private Sector Collaboration in Standards Development for Cybersecurity

- Federal agencies should regularly promote close collaboration with the private sector in standards development for cybersecurity. This means that agencies should seek to build consensus rather than impose a preferred solution.

- Leveraging U.S. public and private sector collaboration in standards development for cybersecurity requires making maximum use of existing processes and, where necessary, establishing additional processes for effective communication on substance, strategy, and tactics between the USG and U.S. private sector standardization participants.

Recommendation 5: Enhancing International Coordination and Information Sharing

- The USG should ensure dialogue and information exchange takes place between senior Federal cybersecurity officials and their counterparts in key partner countries on cybersecurity standards development activities.

- The USG should also facilitate periodic reviews of coordination efforts between Federal agency staff and their foreign government counterparts on cybersecurity standards activities, focusing on lessons learned, highlighting useful collaborative mechanisms, and suggesting opportunities for improvement.

Recommendation 6: Supporting and Expanding Standards Training for Federal Agency Staff

- The USG should encourage and support expanded standards training for Federal agency staff. Such training should cover: the impacts and benefits of cybersecurity standardization; the potential costs of failing to participate in cybersecurity standards development, revise standards when needed, and use such standards in their programmatic activities; and understanding the processes of various SDOs and how to influence successfully the content of standards to meet U.S. objectives.

    - Standards training would help to ensure that Federal agency participants in cybersecurity standardization are aware of policy and technical developments impacting cybersecurity standardization, and are current on other skills and competencies needed for successful participation in cybersecurity standardization.

    - Educating senior leadership of agencies regarding the value of standards work and the need for long-term consistency of investment would encourage Federal agencies to provide: (i) continuous support for their technical experts' participation and leadership activities in mission critical SDOs, including SDO-specific training and mentoring; and (ii) generalized standards training to enhance their participants' effectiveness in international standards development. Many SDOs offer training on their processes and on standards in general, which Federal agencies may be able to use.

Recommendation 7: Developing Technically Sound International Standards for Cybersecurity that Minimize Privacy Risk

- The USG should encourage privacy research and development to support standards and best practices that contribute to the improved identification of privacy risk and mitigation methods.

- Federal agencies participating in the work of SDOs should make technical contributions to draft standards to ensure that the resulting cybersecurity standards minimize privacy risks using a privacy risk

management framework, while enabling information-sharing relating to cybersecurity and allowing the USG to combat cyber-enabled threats.

Recommendation 8: Using Relevant International Standards for Cybersecurity to Promote Global Acceptance and Achieve Mission and Policy Objectives

- Federal agencies should use relevant international standards for cybersecurity, where effective and appropriate, in their mission and policymaking activities. This includes both cybersecurity standards and standards from other domains that are relevant to cybersecurity.

- In accordance with U.S. laws and policy[26], Federal agencies should use relevant international standards in their procurement and regulatory activities whenever possible.

- Where international standards are either not relevant, effective, and appropriate or do not exist, agencies should seek to work with the private sector to develop them through an SDO to promote global acceptance and then use them for achieving mission and policy objectives.

- To the extent that agencies believe that it is necessary to use U.S.-specific approaches, they should develop such approaches through open and transparent processes (e.g., notice-and-comment rulemaking) and seek to promote their adoption into the international standards ecosystem, where appropriate, to promote their use globally.

[26] See: the National Technology Transfer and Advancement Act (NTTAA), as amended; the Trade Agreements Act of 1979, as amended (TAA), July 26, 1979/December 8, 1994; and OMB Circular A-119 Revised (Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities).