Publication Number: **NIST Interagency Report (NISTIR) 8074 Volume 1**

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

Publication Date: **December 2015**

- Final Publication: http://dx.doi.org/10.6028/NIST.IR.8074v1 (which links to http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf)
- Related Information on CSRC: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-8074v1
- Information on other NIST cybersecurity publications and programs can be found at: http://csrc.nist.gov/

The following information was posted with the attached DRAFT document:

Aug. 10, 2015

NIST IR 8074

DRAFT Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (2 Volumes):
Volume 1: Report
Volume 2: Supplemental Information for the Report

NIST seeks public comments on Draft NIST Interagency Report (NISTIR) 8074, which comprises two volumes, "Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity" (Vol. 1) and "Supplemental Information" (Vol. 2).

The public comment period closed September 24, 2015.

NISTIR 8074 Volume 1 (Draft)

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

Editors:
Michael Hogan
Elaine Newton

NIST

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

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

Editors:
Michael Hogan
Elaine Newton
Office of the Director
Information Technology Laboratory

National Institute of Standards and Technology Interagency Report 8074 Volume 1

(Draft)

17 pages (August 2015)

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

Public comment period: *August 10, 2015* through *September 24, 2015*

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 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 Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* provides additional background on international cybersecurity standardization.

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

3
4 **Introduction**
5
6 This report, which was drafted by the NSC Cyber Interagency Policy Committee's International Cybersecurity
7 Standardization Working Group for the Administration, sets out proposed United States Government (USG)
8 strategic objectives for pursuing the development and use of international standards for cybersecurity, and makes
9 recommendations to achieve those objectives. Implementation of these recommendations — which cover
10 interagency coordination, collaboration with the U.S. private sector and international partners, agency
11 participation in international standards development, standards training and education, use of international
12 standards to achieve mission and policy objectives, and other issues – will enable the development and execution
13 of a comprehensive United States cybersecurity standardization strategy.
14
15 The Cybersecurity Enhancement Act of 2014 was signed into law by President Obama on December 18, 2014.
16 Section 502 of the Act requires the Director of the National Institute of Standards and Technology (NIST) to work
17 with relevant Federal agencies to ensure interagency coordination "in the development of international technical
18 standards related to information system security," and develop and transmit to Congress a plan for ensuring such
19 coordination within one year of enactment. This report will also serve as the basis of the required report to
20 Congress.
21
22 The Supplemental Information document provides additional background on the status of international
23 cybersecurity standardization.
24
25 **Strategic Objectives**
26
27 Given the increasingly global, complex, and interconnected nature of the world economy, characterized by rapid
28 advances in technology and use of commercial off the shelf products to assure cybersecurity and resiliency, the
29 use of international cybersecurity standards for information technologies (IT)[1] and industrial control systems
30 (ICS)[2] are necessary for the cybersecurity and resiliency of all U.S. information and communications systems and
31 supporting infrastructures.
32
33   •   Cybersecurity is the prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the
34   restoration of electronic information and communications systems and the information contained therein
35   to ensure confidentiality, integrity, and availability.[3]
36
37   •   Resilience is the ability of both the private sector and the government to reduce the magnitude and/or
38   duration of disruptive events to critical infrastructure. The effectiveness of a resilient infrastructure or
39   enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially
40   disruptive event.[4]
41
42 Cybersecurity relies upon a diverse set of standards including standards whose scopes are specific to one or more
43 attributes of cybersecurity and standards from other domains that are relevant to cybersecurity.
44

---

[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).

[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 Initial Public Draft, Guide to Industrial Control Systems (ICS) Security.

[3] Blueprint for a Secure Cyber Future, DHS, November 2011.

[4] Critical Infrastructure Resilience Final Report and Recommendations, National Infrastructure Advisory Council, September 8, 2009

45 The U.S. standardization community is comprised largely of non-governmental Standards Developing
46 Organizations (SDOs). These groups are primarily shaped by industry participation and are motivated by market
47 forces. USG participation is motivated by the need to achieve cost-efficient, timely and effective solutions for
48 mission and policy objectives. These diverse motivations are mutually beneficial.
49
50 The U.S. Government strategy is to leverage these motivations in the development and use of international
51 standards to promote cybersecurity and resiliency. Consistent with the goals of the USG to promote secure
52 cyberspace, there are four fundamental interrelated USG strategic objectives in actively participating in the
53 development and use of timely international standards for cybersecurity:

54
55 **1. Enhancing National and Economic Security and Public Safety**
56
57   o Ensuring that there is a sufficient inventory of international standards that can serve as a basis for
58   the cybersecurity and resiliency of U.S. organizations, particularly critical infrastructure.
59
60   o Using international standards as a key part of USG procurement policy to support secure and
61   resilient operations.
62
63   o Ensuring that international standards meet the cybersecurity interests of the USG including
64   protecting against illicit cyber activities or actions by terrorist groups and hostile nation-state
65   actors.
66
67 **2. Ensuring standards and assessment tools for the USG are Technically Sound**
68
69   o Supporting the development and use of new standards by taking into account: the scope of
70   standardization work of candidate SDOs, U.S. industry preferences, USG needs, and the recent
71   track record of candidate SDOs in particular areas of cybersecurity standardization.
72
73   o Developing technically sound and fit for purpose standards in open, transparent, and consensus-
74   based processes, and updating as often as necessary in collaboration with the private sector.
75
76   o Supporting coordination among SDOs to avoid duplication, promote interoperability, maximize
77   the utility of standards projects, and extend the field of application for existing standards.
78
79   o Supporting the development and use of associated assessment tools (e.g., reference
80   implementations, conformance and interoperability test suites) to complement timely, technically-
81   sound standards development.
82
83 **3. Facilitating International Trade**
84
85   o Supporting the development and use of international standards and associated assessment
86   schemes for cybersecurity (where relevant, effective, and appropriate), which can promote
87   international trade and provide a level playing field for U.S. companies.
88
89   o Ensuring market relevance by developing standards in response to industry, government and
90   consumer requirements and timelines.
91
92 **4. Promoting Innovation and Competitiveness**
93
94   o Supporting the development and use of international standards in collaboration with U.S.
95   industry, to foster open and fair competition.
96

2

97   o   Promoting the inclusion of existing and emerging technologies in international standards that
98   boost U.S. competitiveness and ensuring that USG equities are well represented in those
99   standards.
100
101   o   Encouraging the development and use of performance standards for cybersecurity, where
102   appropriate. Performance standards generally are more likely to encourage innovation and enable
103   competition than prescriptive design standards. Prescriptive design standards are sometimes
104   necessary, however, particularly for describing test methods or procedures.
105
106 **Relevant Background on Standardization and Assessment**
107
108 *Background on standardization*
109
110 For purposes of this exercise, a standard is a document, established by consensus and approved by a recognized
111 body, which provides for common and repeated use, rules, guidelines or characteristics for activities or their
112 results, aimed at the achievement of the optimum degree of order in a given context.[5] A standards developer is
113 any organization that develops and approves standards using various methods to establish consensus among its
114 participants. The use of such documentary consensus standards is voluntary.
115
116 Pursuant to U.S. law and policy,[6] Federal agencies are required to use voluntary consensus standards in their
117 procurement and regulatory activities, except where inconsistent with law or otherwise impractical. Many SDOs
118 operate through a process that is characterized by all or some of the following attributes: openness, balance, due
119 process, ability to appeal, and consensus. Openness means that the procedures or processes used are open to
120 interested parties. Such parties are provided meaningful opportunities to participate in standards development on
121 a non-discriminatory basis. The procedures or processes for participating in standards development and for
122 developing the standard are transparent. The standards development process should also be balanced.
123 Specifically, there should be meaningful involvement from a broad range of parties, with no single interest
124 dominating the decision-making. Due process shall include documented and publically available policies and
125 procedures, adequate notice of meetings and standards development, sufficient time to review drafts and prepare
126 views and objections, access to views and objections of other participants and a fair and impartial process for
127 resolving conflicting views. An appeals process shall be available for the impartial handling of procedural
128 appeals. Consensus is defined as general agreement, but not necessarily unanimity. During the development of
129 consensus, comments and objections are considered using fair, impartial, open, and transparent processes. These
130 process attributes contribute to the technical soundness and market relevance of the published standards of an
131 SDO.
132
133 The U.S. standards system differs significantly from the government-driven, centrally-coordinated standards
134 systems common in many other countries. Within the United States, there are hundreds of SDOs, which are
135 overwhelmingly private sector organizations, providing the infrastructure for the preparation of standards
136 documents. USG personnel participate in SDO activities along with representatives from industry, academia, and
137 other organizations and consumers. In many other countries' standards systems, the government plays a larger
138 role in standards development-related activities, which provides those governments the ability to use standards to
139 support domestic industrial and innovation policy, rather than to advance technical solutions in support of public
140 policy goals. While Federal agencies possess certain responsibilities related to standards, such as in their own use
141 of standards or in their development of technical regulations, there is a much greater reliance in the United States
142 on the private sector, including companies and industry groups, consumers, and other interested parties, in
143 standards development. The United States Standards Strategy, elaborated through a private and public sector
144 partnership in 2000, and revised most recently in 2010, outlines the contribution of private-sector led standards
145 development to overall competition and innovation in the U.S. economy and the imperative of public and private
146 sector participation that is a central tenet of the U.S. approach to standardization.

---

[5] See ISO/IEC Guide 2:2004, Standardization and related activities - General Vocabulary.
[6] See the National Technology Transfer and Advancement Act (NTTAA), as amended, and OMB Circular A-119 Revised (Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities).

147
148   *Background on conformity assessment*
149
150   Conformity assessment determines whether a product, process or service has fulfilled the specified requirements
151   of a standard. Conformance testing captures the technical description of the requirements in a standard and
152   measures whether an implementation (product, process or service) faithfully fulfills these requirements.
153   Conformance testing alone does not completely ensure the interoperability or performance of conforming
154   products, processes, or services. Therefore, interoperability and performance testing are also important aspects
155   for procurements. Interoperability testing tests one implementation with another to establish that they can work
156   together properly. Performance testing measures the performance characteristics of an implementation, such as its
157   throughput[7] or response time,[8] under various conditions.
158
159   Testing and attestation of products, processes, and services against established cybersecurity standards help
160   provide a level of assurance that a product, process, or service's stated security claim is valid.   An example is the
161   USG requirement for using cloud products that meet Federal cloud security requirements. Commercial
162   assessment organizations, which are accredited for assessing cloud security, determine if a cloud product
163   conforms to the requirements. This can be more cost-effective for Federal agencies than developing in-house
164   USG testing expertise.
165
166   *Other relevant legal and policy instruments*
167
168   •   The World Trade Organization (WTO) Agreement on Technical Barriers to Trade (TBT Agreement) –
169   which has been implemented in U.S. law by the Trade Agreements Act of 1979, as amended (TAA) —
170   highlights the important role that international standards can play in facilitating trade and requires the use
171   of relevant international standards, where effective and appropriate, in a Member's technical regulations.
172   Although the TBT Agreement does not identify specific international standardizing bodies, the WTO
173   Committee on Technical Barriers to Trade has identified several principles that functionally define
174   international standards (i.e., standards developed in processes characterized by transparency, openness,
175   impartiality and consensus, relevance and effectiveness, coherence and accounting for developing country
176   interests).[9]
177
178   •   The International Strategy for Cyberspace lays out an approach to unify USG engagement with
179   international partners on a full range of cyber issues. The International Strategy highlights the need to
180   develop and use international cybersecurity standards and conformity assessment schemes, and the
181   importance of public-private sector collaboration. The Strategy establishes the goal that "[t]he United
182   States will work internationally to promote an open, interoperable, secure, and reliable information and
183   communications infrastructure that supports international trade and commerce, strengthens international
184   security, and fosters free expression and innovation." The strategy contains policy priorities for the
185   economy; protecting our networks; law enforcement; military; internet governance; international
186   development; and internet freedom. This includes steps to enhance confidence in cyberspace and pursue
187   those who would exploit online systems, and a commitment from the USG to participate actively in
188   discussions about how international norms and measures on cybercrime are developed bilaterally and
189   multilaterally, in fora with proven expertise and a history of promoting effective cybercrime policies.
190   This also includes promoting processes to permit states to investigate, apprehend, and prosecute those
191   who intrude or disrupt networks.
192
193   •   The National Cooperative Research Act of 1984 first allowed organizations to collaborate to carry out
194   joint research and development ventures and not be deemed illegal per se under Federal antitrust laws or
195   similar State laws. One result has been a rapid growth in IT consortia developing standards. In

---

[7]Throughput is a measure of how much work the system can do in a given period of time.

[8]Response time is a measure of how quickly the system responds to a request for it to do something.

[9] 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.

196   developing their standards, many of these consortia follow the WTO TBT Committee Decision principles.
197   However, consortia are also formed that are not open, with membership by invitation. Consortia range
198   from unincorporated affiliations of companies to incorporated entities with budgets, offices and paid staff.
199   A consortium may exist to complete a specific standard, but others have a broader mission and develop
200   multiple standards necessary to enable the evolution of a category of business services and products. An
201   oft-cited advantage of IT consortia is speed in developing a standard, but speed is sometimes obtained due
202   to a greater alignment in the technical interests of the participating entities. However, the narrow
203   alignment of the interests of the participating entities may not represent a broad need, and this may slow
204   uptake of the developed standard. At the same time, rapid innovation in emerging technologies has been
205   accompanied by competition among SDOs to undertake new work areas in emerging fields of
206   standardization that are perceived to be of great market relevance (e.g., smart grid, cloud computing,
207   cybersecurity). This competitive environment has encouraged most SDOs to streamline their consensus
208   building processes in order to develop and approve technically sound standards that meet current market
209   needs in an effective manner.
210
211   • Memorandum M-12-08 on "Principles for Federal Engagement in Standards Activities to Address
212   National Priorities" provides guidance to agencies with respect to their engagement in standards activities
213   that have been identified as national priorities either through executive branch or Congressional actions.
214   For example, "[a]gencies considering a convening or active engagement role in private sector standards
215   developing organizations in order to address a national priority area should state their reasons plainly
216   (including why private sector leadership alone is insufficient). Further, agencies should accept and act on
217   feedback on their rationales before assuming this convening or active-engagement role in a private sector
218   standards developing organization. In all cases, agencies should ensure effective intra- and inter-agency
219   coordination of engagement in standards development activities. When an agency commits to a
220   cooperative standards development effort with industry, that commitment should be maintained, as
221   resources permit, and the resulting standards should be used where feasible. Agencies should use existing
222   processes and, where necessary, establish new processes for open, transparent, and effective two-way
223   communication with private sector interests, ensuring that concerns from private sector entities are given
224   thorough and objective consideration. To the extent feasible and appropriate, agencies should also provide
225   continuous support for their technical experts' participation and leadership activities in mission-critical
226   standards-setting activities and standards organizations, including standards organization-specific training
227   and mentoring. Agencies should periodically review their standards activities to identify gaps in
228   representation for mission-critical areas as part of their long-range planning and adopt policies that value
229   and reward participation in standardization activities."
230

231 **Present State of International Cybersecurity Standardization**
232

233 This section sets out core areas of cybersecurity that broadly influence the overall cybersecurity of products,
234 processes, services, and organizations. USG technical experts have been participating in many core areas of
235 cybersecurity standardization for decades. The resulting standards are largely being developed for the global
236 marketplace generally and not just for Federal networks and applications.[10] Such standards provide the
237 requirements for cybersecurity standards-based products, processes or services. As a consequence of participating
238 in this standards work, the USG has acquired and accumulated competency in core areas of cybersecurity
239 standardization, but the depth and breadth of this USG competency can rise and fall with time.

---

[10] 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. 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
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.

240
241   Core areas of cybersecurity standardization include: cryptographic techniques; cyber incident management;
242   identity management; IT system security evaluation; information security management systems; network security;
243   security automation and continuous monitoring; supply chain risk management; software assurance; and system
244   security engineering. These areas, which are relevant for numerous applications, are discussed in detail in the
245   Supplemental Information document. Based upon legislative and policy mandates, there are a growing number of
246   national priority applications for which the USG participates in the development of standards relevant to
247   cybersecurity, including: cloud computing; emergency management; industrial control systems; health IT; smart
248   grid; and voting. Such applications utilize cybersecurity standards in each of the listed core areas.
249
250   Worldwide, there are over 200 SDOs developing IT and ICS standards. Among those, there are dozens of SDOs
251   developing cybersecurity standards, yet fewer SDOs may develop international cybersecurity standards. Some of
252   the key SDOs directly involved in cybersecurity that may develop international standards are: the 3rd Generation
253   Partnership Project (3GPP); the 3rd Generation Partnership Project 2 (3GPP2); the Alliance for
254   Telecommunications Industry Solutions (ATIS); the International Electrotechnical Commission (IEC); the
255   Institute of Electrical and Electronic Engineers (IEEE); the Internet Engineering Task Force (IETF); the
256   International Society of Automation (ISA); the International Organization for Standardization/International
257   Electrotechnical Commission Joint Technical Committee 1 (ISO/IEC JTC 1), Information Technology; the
258   International Organization for Standardization Technical Committee 68 (ISO TC 68), Financial Services; the
259   International Telecommunication Union Radiocommunication Sector (ITU-R); the OpenID Foundation (OIDF);
260   the Organization for the Advancement of Structured Information Standards (OASIS); the Payment Card Industry
261   Security Standards Council (PCI SSC); the Trusted Computing Group (TCG); the World Wide Web Consortium
262   (W3C); and the WiMAX Forum. Collectively, these SDOs have many hundreds of cybersecurity standards
263   projects under maintenance or development. Being able to influence cybersecurity standards development
264   requires developing and maintaining effective liaisons within and among these SDOs.
265
266   Table 1 below provides an abbreviated, high-level snapshot of where standards are being developed and the
267   present status of cybersecurity standards for some priority cybersecurity applications. This status information in
268   Table 1 represents a high-level standards gap analysis. **"Standards Mostly Available"** indicates that SDO-
269   approved cybersecurity standards are for the most part available and standards-based implementations are
270   available. However, the availability of standards means that such standards require continuous maintenance and
271   updating/replacing based upon feedback from testing and deployments of standards-based products, processes,
272   and services, as well as improvements in technology and the exploitation of those improvements by those
273   engaging in cybercrime and cyberespionage. **"Standards Being Developed"** indicates that needed SDO-
274   approved cybersecurity standards are still under development and that needed standards-based implementations
275   are not yet available. **"New Standards Needed"** indicates that many necessary cybersecurity standards are either
276   not yet being developed or are at the beginning stages of development within SDOs and therefore standards-based
277   implementations are not yet available.
278
279   Two observations can be made on the overall status of ongoing cybersecurity standardization. First, robust
280   standardization activities in the listed core areas of cybersecurity standardization are undoubtedly necessary for
281   ensuring interoperability, security, usability, and resiliency. Second, as illustrated by the listed applications in
282   Table 1, there is a mix of ongoing standardization and maintenance of existing standards that is necessary to
283   sustain deployments of standards-based products, processes and services.
284

Core Areas of Cybersecurity Standardization	Examples of Relevant SDOs	Examples of Some Key IT 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	Standards Being Developed	Standards Being Developed	Standards Being Developed	Standards Being Developed	Standards Being Developed
Cyber Incident Management	ISO/IEC JTC 1; ITU-T; PCI	Standards Being Developed	New Standards Needed	Standards Being Developed	Standards Being Developed	Standards Being Developed	New Standards Needed
Identity 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; OASIS; PCI SSC; ISO TC 223	Standards Being Developed	New Standards Needed	Standards Being Developed	Standards Being Developed	New Standards Needed	New Standards Needed
IT System Security Evaluation	ISO/IEC JTC 1	Standards Being Developed	Standards Mostly Available	Standards Being Developed	Standards Being Developed	Standards Being Developed	Standards Mostly Available
Network Security	3GPP; IEC; IETF; IEEE; ISO/IEC JTC 1; ITU-R; ITU-T; WiMAX Forum	New Standards Needed	Standards Being Developed	Standards Being Developed	Standards Being Developed	Standards Being Developed	Standards Mostly Available

Core Areas of Cybersecurity Standardization	**Examples of Relevant SDOs**	**Examples of Some Key IT Applications**					
		Cloud Computing	**Emergency Management**	**Industrial Control Systems**	**Health IT**	**Smart Grid**	**Voting**
Security Automation & Continuous Monitoring	**IETF; ISO/IEC JTC 1; TCG**	**Standards Being Developed**	**Standards Being Developed**	**New Standards Needed**	**Standards Being Developed**	**New Standards Needed**	**New Standards Needed**
Software Assurance	**IEEE; ISO/IEC JTC 1; TCG**	**New Standards Needed**	**Standards Being Developed**	**Standards Being Developed**	**Standards Being Developed**	**Standards Being Developed**	**Standards Being Developed**
Supply Chain Risk	**ISO/IEC JTC 1**	**Standards Being**	**New Standards**	**Standards Being**	**New Standards**	**New Standards**	**New Standards**
System Security Engineering	**IEC; ISA; ISO/IEC JTC 1**	**New Standards Needed**	**Standards Mostly Available**	**Standards Being Developed**	**Standards Being Developed**	**New Standards Needed**	**Standards Being Developed**

285
286   **Table 1 Status of Cybersecurity Standardization in Core Areas (Illustrative Examples)**
287
288   **Key Challenges in Cybersecurity Standardization**
289
290   *Interagency and Private Sector Engagement*
291
292   There are at least three active USG groups that provide for interagency coordination on standards-related matters.
293   The Interagency Committee on Standards Policy (ICSP) provides advice and recommendations to the Secretary of
294   Commerce and other Executive Branch agencies on matters related to standards policy that could impact Federal
295   agencies' participation in, and use of, standards. The Technical Barriers to Trade (TBT) Subcommittee of the
296   Trade Policy Staff Committee (TPSC), which is led by the Office of the United States Trade Representative
297   (USTR), coordinates the development and implementation of USG positions relating to technical regulations,
298   standards and conformity assessment procedures around the world. The JESC (Joint Enterprise Standards
299   Committee) serves as the Department of Defense information technology standards and Intelligence Community
300   (IC) enterprise standards governance body. This forum collaborates and recommends common enterprise
301   standards, profiles, and specifications for the respective DoD and IC information environments. Interagency
302   coordination on standards-related matters also occurs in some subcommittees and working groups within the
303   National Science and Technology Council (NSTC). Given the critical importance of cybersecurity
304   standardization and its cross-cutting nature —which involves security, standards, innovation, competition, trade,
305   privacy, law enforcement and national security, and other policy considerations –a higher-level interagency
306   coordination mechanism is needed. Coordination by senior Federal cybersecurity officials under the auspices of
307   the Executive Office of the President (EOP) would provide the necessary focus and resources to develop and
308   implement a comprehensive strategy for cybersecurity-related standardization, as well as ensure that the USG can
309   respond to specific priority issues as they arise.

310
311   In addition to coordination among Federal agencies, the USG needs to engage effectively with U.S. industry.
312   There are several methods agencies use to engage and coordinate with external stakeholders. Agencies may
313   choose to establish external advisory committees per the Federal Advisory Committee Act (FACA), seek input
314   using Federal Register Notice solicitations, use specific statutory or regulatory authority to create a forum — such
315   as a private sector coordinating council — for obtaining input, or use some other method that provides all
316   potential stakeholders an equal opportunity to provide input and share their perspectives. As an example of
317   FACA committees, the U.S. Department of Health and Human Services (HHS) created Health IT Policy and
318   Standards committees that make recommendations to the National Coordinator on policy and standards topics,
319   including cybersecurity. In addition, in developing the Framework for Improving Critical Infrastructure
320   Cybersecurity under Executive Order 13636, NIST provided stakeholders with an equal opportunity to share their
321   views and make contributions through a series of workshops and public comment periods on drafts.
322
323   For SDOs that use a national body member process, such as the International Organization for Standardization
324   (ISO), there is already built-in U.S. coordination through U.S. mirror groups (e.g., U.S. Technical Advisory
325   Groups (TAGs) for ISO technical committees and subcommittees). The State Department administers a FACA-
326   based process for developing U.S. positions relating to standardization in the International Telecommunication
327   Union's Telecommunication Standardization Sector (ITU-T), a treaty-based United Nations organization. For
328   SDOs that are based on an individual membership model, public-private sector coordination prior to technical
329   committee meetings is not built-in, so this may be a particular area that could benefit from enhanced focus by the
330   USG.
331
332   In carrying out these activities, it is important to prioritize resources and engagement to achieve maximum impact
333   with various SDOs. The number of cybersecurity standards projects is substantial. Therefore, the USG needs to
334   develop an engagement model to ensure that it is able to participate dynamically at the right level when necessary.
335   The following four categories characterize possible levels of engagement and related resource planning needs:
336
337   • **Participating in limited specific activities** is following, contributing to, and/or leading a specific
338   standards effort for a select activity(s) specific to unique needs or interests.
339
340   • **Monitoring** focuses on broader programs of work and emerging and evolving standards produced by the
341   SDOs. It includes developing an understanding of, and relationships with, the key players.
342
343   • **Influencing**, in addition to the requirements of monitoring, involves commenting on, and providing
344   contributions to, strategically important standards, working with industry and international players, and
345   exerting influence through formal and informal discussions and provision of expertise.
346
347   • **Leading** involves the activities associated with monitoring and influencing and, additionally, providing
348   leadership through roles such as convening or administering consensus groups, serving as the standards
349   project editor, and serving as the liaison representative between standards groups.
350
351   All of these options require having qualified USG participants (whether USG employees or contractors) function
352   in these capacities, based on their expertise, relationships, and knowledge of specific SDO processes and best
353   practices.
354
355   *Privacy*
356
357   The protection of individual privacy promotes U.S. interests by facilitating improved trust in online and offline
358   transactions and helping U.S. products and services compete in global markets. Cybersecurity is an important
359   component of protecting privacy, and many privacy standards address the protection of personal data by cross-
360   referencing standards in the area of information security management systems. Nonetheless, cybersecurity
361   measures also can create privacy risks. Executive Order 13636 recognized this concern by requiring the National
362   Institute of Standards and Technology (NIST) to include a methodology to protect privacy and civil liberties in

363 the Framework for Improving Critical Infrastructure Cybersecurity.[11] The NIST Roadmap for Improving Critical
364 Infrastructure Cybersecurity referred to how few technical standards or best practices exist to mitigate the impact
365 of cybersecurity activities on individual privacy and civil liberties. It is in the best interests of the USG to support
366 the development and use of cybersecurity standards that minimize risks to privacy, promote information-sharing
367 relating to cybersecurity, and allow the USG to combat cyber-enabled threats. Greater understanding of how to
368 identify privacy risks and integrate mitigations into cybersecurity standards or their deployment in information
369 systems will require further research.
370
371 *Participation/Training/Education*
372
373 Maintaining and, where needed, augmenting USG competency in the core areas of cybersecurity standardization
374 require continuous education, participation and training. Obtaining a consensus to approve standards among
375 participants in various SDOs usually requires more than a simple majority but less than unanimity. Effective
376 negotiation in standards development requires not just technical expertise by Federal agency participants, but a
377 thorough knowledge of an SDO's standards development process and policies, as well as soft skills in negotiating
378 with stakeholders with a range of often diverse and conflicting positions. In addition, awareness of the relevant
379 market and associated market politics that drive the motivations of the other participants is essential. For
380 international fora, understanding the culture of the participants is also important. Accordingly, continuity in
381 participation is crucial to success. Participants must regularly attend the meetings, have established relationships
382 with the other participants, and ensure that the draft standards are technically sound and meet USG needs.
383 Effective leadership in SDOs promotes timely development of technically sound standards.
384
385 It is in the best interests of Federal agencies to support qualified Federal representatives (including contracted
386 technical experts) in SDO leadership positions. Candidates for such leadership positions should be both
387 technically knowledgeable and thoroughly familiar with the SDO's development processes and policies, and have
388 a good understanding of USG and U.S. industry priorities and perspectives. Further, long-term participation of
389 the same USG representatives within an SDO establishes trust and builds the credibility of those representatives.
390 This is critical for effective communication and information-sharing and ultimately will assist in advancing the
391 USG's strategic objectives in each SDO. In addition to effective participation and leadership by Federal agency
392 representatives, Federal agencies, consistent with agency missions, need to coordinate their positions.
393
394 Lastly, leveraging strong government/private sector/university cooperation is needed to ensure the availability of
395 USG expertise. Policies should be put in place to educate Federal agencies' management and technical staff on
396 the need for continuity, cooperation, and effective participation in standards development. The USG should also
397 support standards education in technical and graduate educational programs, especially in engineering, business,
398 sciences, and technology to ensure the development of future generations of U.S. cybersecurity standards
399 participants. Some initiatives that could be built upon include:
400
401   • The National Initiative for Cybersecurity Education (NICE): The goal of NICE is to establish an
402   operational, sustainable and continually improving national cybersecurity education program that will
403   develop sound cyber practices to enhance the nation's security.   The scope of this program includes the
404   Federal workplace, civilians, and students in kindergarten through post-graduate school.
405

---

[11] EO 13636 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.

406   •   The NIST Standards Services Curricula Development Cooperative Agreement Program provides financial
407   assistance to support curriculum development for the undergraduate and/or graduate level. This Program
408   supports the integration of documentary and measurement standards and standardization information and
409   content into seminars, courses, and learning resources.
410

411   •   Many U.S. based private sector entities also run relevant standards education activities and welcome USG
412   participation and collaboration. These include, but are not limited to, the American National Standards
413   Institute (ANSI), which has programs and content to raise awareness of the importance of standards and
414   conformity assessment among university faculty in engineering, technology, business, public policy and
415   law schools (StandardsLearn.org). Similarly, the Institute of Electrical and Electronics Engineers (IEEE)
416   runs a broad Standards Education program to promote knowledge of standards and the importance of
417   standardization among students. Other unique standards education-related resources are available from
418   the International Organization for Standardization (ISO) at Education about standards.
419

420   •   The Framework for Improving Critical Infrastructure Cybersecurity developed under Executive Order
421   13636 provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to
422   manage cybersecurity risk for those processes, information, and systems directly involved in the delivery
423   of critical infrastructure services. The Framework relies on standards for its use, with "Informative
424   References" containing specific sections of standards, guidelines, and practices common among critical
425   infrastructure sectors. The Framework can be used to identify opportunities for new or revised standards,
426   guidelines, or practices that would help organizations address emerging needs.
427

428 **Recommendations**
429

430 Maintaining USG competency to participate effectively in the development of new or revised core cybersecurity
431 standards areas provides the foundation to respond to ever-evolving USG priorities. The development of
432 international standards for cybersecurity promotes U.S. interests by facilitating interoperability, security, usability
433 and resiliency; improving trust in online and offline transactions; promoting innovation and competitiveness; and
434 helping U.S. products and services compete in global markets. Increased and more strategic and coordinated U.S.
435 engagement in cybersecurity standardization will help promote U.S. interests by ensuring that standards-based
436 requirements for cybersecurity products, processes, and services meet U.S. objectives. Ensuring effective U.S.
437 leadership in the relevant standards developing bodies for cybersecurity requires awareness of specific SDO
438 environments, coordination of USG interests with U.S. industry and organization interests to prioritize and
439 achieve U.S. objectives, and a robust focus on education and training.
440

441 The following recommendations, which are intended to help achieve USG strategic objectives in cybersecurity,
442 could provide the basis for guidance from White House leadership (e.g., the White House Cybersecurity
443 Coordinator) to Federal agencies.
444

445 **Recommendation 1: Ensuring USG Coordination**
446

447   •   The USG should institute a high-level interagency coordination process for cybersecurity standardization.
448

449   o   An Executive Office of the President (EOP) interagency policymaking body would provide the
450   proper level of authority to oversee such a coordination process.
451

452   o   The U.S. Department of Commerce would host a subordinate interagency working group -- the
453   International Cybersecurity Standardization Working Group –on behalf of the EOP interagency
454   policymaking body. Such a group would be comprised of senior Federal cybersecurity officials
455   with the expertise and bandwidth to develop and implement a comprehensive set of objectives
456   and strategies, and to coordinate on major issues in standardization before and as they
457   arise. Major policy decisions and areas of significant disagreement could then be brought to the
458   EOP body.

459
460   o   Such a mechanism would help to ensure that both internal agency and overall USG efforts are
461   coordinated and support U.S. objectives when working with relevant private sector actors,
462   including SDOs, industry, NGOs, and international partners.
463
464   o   Agencies participating in the work of specific SDOs would have an established interagency venue
465   for developing objectives and strategies in concert with interagency colleagues, as well as raising,
466   and where possible coordinating on, major issues.
467

Recommendation 2: Promoting USG Participation in Cybersecurity Standards Development

468
469
470 •   Federal agencies should regularly highlight within their agencies the need to participate in standards
471   development for cybersecurity, which is a USG priority.
472
473 •   Federal agencies should support a long-term commitment of resources and participants with specialized
474   knowledge, skills and abilities for international cybersecurity standardization.
475
476 •   The USG should maintain and, where needed, augment its competency in core areas of cybersecurity
477   standardization. As part of their long-range planning, Federal agencies should periodically review their
478   standards participation to identify gaps in representation for mission-critical activities.
479
480 •   Federal agencies should value and reward staff participation in standardization activities, encourage
481   junior staff members to be involved in standardization activities, and provide mechanisms for recognition
482   of effective participation by their technical experts.
483

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

484
485
486
487 •   To help make standards projects more focused and timely, Federal agencies participating in the work of
488   SDOs should make clear and comprehensive contributions with regard to the scope of cybersecurity
489   standardization projects, as well as target dates to complete those projects.
490
491 •   Federal agencies should make timely technical contributions to draft standards for cybersecurity to ensure
492   that the resulting standards are technically sound.
493
494 •   Federal agencies should support and coordinate the timely development of conformity and
495   interoperability assessment schemes for cybersecurity, whether by private or public sector bodies, to
496   accelerate the development and use of technically sound standards and standards-based products,
497   processes and services (e.g., the Federal Risk and Authorization Management Program (FedRAMP)).
498

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

499
500
501
502 •   Federal agencies should regularly promote close collaboration with the private sector in standards
503   development for cybersecurity. This means that agencies should seek to build consensus rather than
504   impose a preferred solution.
505
506 •   Leveraging U.S. public and private sector collaboration in standards development for cybersecurity
507   requires making maximum use of existing processes and, where necessary, establishing additional
508   processes for effective communication on substance, strategy, and tactics between the USG and U.S.
509   private sector standardization participants.
510
511

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.

  - It would also 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.

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 utilizing 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 Achieve Mission and Policy Objectives

- Federal agencies should use relevant international standards for cybersecurity, where effective and appropriate, in their mission and policymaking activities.

- 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, 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.