

Draft Report on Strategic USG Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (DRAFT NISTIR 8074)

Presentation to the Software and Supply Chain Assurance
Forum – Fall 2015

Jeff Weiss

Senior Advisor for Standards and Global Regulatory Policy
Office of Policy & Strategic Planning, Office of the Secretary
United States Department of Commerce

September 1, 2015

Items we'll cover in the presentation

- Statutory basis for the draft report
- Importance of the report
- Process for developing the report
- Main elements of the draft report
- Challenges and opportunities
- Key questions to consider

Relevant provisions of the Cybersecurity Enhancement Act of 2014

TITLE V – Advancement of cybersecurity technical standards

SEC. 502. International cybersecurity technical standards.

(a) In general.—The Director [of NIST], in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) *not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.*

(b) Consultation with the private sector.—In carrying out the activities specified in subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

Importance of the report

- In an area that is critical to U.S. economic and national security, we are not creating a top-down approach to standardization
- Rather, the approach we've put together is consistent with existing USG law and policy on standards and, in fact, is an application of existing law and policy to cybersecurity standardization
- We have a set of higher level objectives in developing this approach, along with meeting the statutory requirements:
 - Improving awareness, information-sharing, and coordination among federal agencies on cybersecurity standardization
 - Laying out for the private sector a clear articulation of USG objectives and approaches in standardization in this area
 - Developing a document that can be used as a basis for the USG and U.S. stakeholders to engage with foreign governments
 - Further strengthening the existing U.S. public-private partnership on standards

Process for developing the report

- The Cyber Interagency Policy Committee (IPC) established the International Cybersecurity Standardization Working Group, which is led by Commerce/NIST and reports to the IPC
- The WG developed this draft report, which will serve as the basis for the report to Congress by the NIST Director called for in the Act
- Numerous agencies are participating in the WG, including: CFTC, Commerce (NIST, ITA, and NTIA), DHS, DOD, DOE, DOJ, GSA, State, Treasury, and USTR
- Participants include experts in: cybersecurity, standards, law enforcement, trade, information technology, supply chain, internet governance, international organizations, regulation, procurement, and specific types of products and services

Process for developing the report (continued)

- We requested public comment on the draft report on August 10th, with comments due by September 24th
- As of August 30th, the draft report has been downloaded more than 1,100 times, the supporting analysis more than 500 times
 - Approximately 25 percent of the downloads have been from outside the United States
 - Most of the downloads outside the United States have come from: Europe (at least 63), Canada (51), China (47), Japan (29), India (25), and Israel (16)

Process for developing the report (continued)

- The WG will review comments and revise the draft report
- WG representatives have been briefing individual agency advisory committees and coordinating councils
- The WG remains open to holding additional meetings with stakeholders and will consider other avenues for soliciting feedback depending on the comments
- The WG will report periodically to the IPC on progress
- NISTIR 8074 will serve as the basis for the NIST Director's Report to Congress – due December 18, 2015

Proposed strategic objectives

- To ensure cybersecurity and resiliency of U.S. information and communications systems and supporting infrastructures, we must develop and use robust cybersecurity standards and assessment schemes
- Four key (and interrelated) objectives for standards and assessment:
 - Enhancing national and economic security and public safety
 - Ensuring standards and assessment tools are technically sound
 - Facilitating international trade
 - Promoting innovation and competitiveness
- The Act focuses on interagency coordination on international standards
 - Standards developing bodies that develop standards through open, transparent, impartial, and consensus-based processes and are globally relevant are strongly preferred

Proposed elements of the report

- 1) Establishing a process for internal USG coordination
- 2) Incentivizing USG participation in cybersecurity standards development in core areas
- 3) Developing timely and technically sound standards and assessment schemes
- 4) Better leveraging the U.S. public-private sector partnership in standards development
- 5) Coordinating and sharing information with trusted international partners
- 6) Supporting and expanding standards education for agency officials
- 7) Minimizing privacy risk/building confidence and trust
- 8) Using relevant international cybersecurity standards to achieve mission and policy objectives

Challenges and opportunities

- **CHALLENGE:** Wide breadth of ongoing work streams and dozens of venues of all different types
 - No single agency can follow everything or has all of the expertise
 - There may be linkages/trends among various work streams that are not necessarily obvious if you are not monitoring the entire ecosystem
- **OPPORTUNITY:** The WG's focus on collaboration and information-sharing among agencies will enable it to:
 - Implement a comprehensive USG strategy;
 - Assist individual agencies in achieving their cybersecurity-related mission and policy objectives through standardization and assessment, where appropriate; and
 - Help formulate USG cybersecurity and cybersecurity-related policy

Core Areas of Cybersecurity Standardization	Examples of Relevant Standards Developers	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
Security Automation & Continuous Monitoring	IETF ISO/IEC JTC 1	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 Management	ISO/IEC JTC 1 The Open Group IEC TC 65	Standards Being Developed	New Standards Needed	Standards Being Developed	New Standards Needed	New Standards Needed	New Standards Needed
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

Challenges and opportunities (continued)

- **CHALLENGE:** Ensuring sufficient agency participation can be difficult in tight budgetary times
- **OPPORTUNITY:** Developing a public plan and establishing a WG under the Cyber IPC helps elevate this as a priority within individual agencies

Key questions for consideration

- 1) The draft report sets out an illustrative list of high priority areas for cybersecurity-related standardization. What are your high priority areas?
- 2) How can we most effectively influence governments that take a top-down approach to standardization to encourage their officials and stakeholders to participate in the development of international cybersecurity standards and use those standards to meet their agencies' mission and policy objectives, rather than develop and use national or regional standards as their default option?
- 3) Are existing agency-specific and interagency mechanisms for consulting with the public on cybersecurity standards-related issues sufficient or are new mechanisms needed?
- 4) Are there emerging commercial norms and industry best practices that should be incentivized through international cybersecurity standardization?