September 24, 2015

Michael Hogan
Elaine Newton
National Institute of Standards and Technology
Attn: Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Via e-mail: nistir8074@nist.gov

Dear Mr. Hogan and Ms. Newtown,

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

BSA | The Software Alliance (BSA)[1] welcomes the opportunity to comment on the Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity published by the National Institute of Standards and Technology (Draft Report) on August 10, 2015.

We commend NIST's work to coordinate efforts with relevant Federal agencies for the development of international technical standards related to information system security as required by Section 502 of the Cybersecurity Act of 2014. BSA shares the goals and interests of NIST on this issue because robust cybersecurity practices can only be achieved by leveraging international, consensus-based, voluntary, and market-driven standards in order to maximize protection of IT infrastructures and defend them against cyber-attacks.

As providers of technology that is the backbone of IT infrastructure globally and of cybersecurity products and services, our members have extensive experience working with governments and other stakeholders around the world on cybersecurity policy and standards. This will better enhance the security and privacy of our customers' information. We are committed to supporting NIST in this regard and offer these comments to assist with your efforts.

[1] BSA | The Software Alliance (*www.bsa.org*) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Altium, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks, and Trend Micro.

Comments

1. Coordinated and International Approach to Cybersecurity

No individual government agency, country or government can address cybersecurity risk in isolation. Inter-agency coordination and collaboration among governments and private sectors from around the globe are key elements to achieving an effective approach to cybersecurity.

It is important that coordination within the United States government (USG) is maintained because cybersecurity standards are developed by many groups and for a variety of different technology areas and processes. To ensure that the efforts of various engaged agencies are complementary and best enable the USG to achieve its goals in this dispersed space, regular coordination and centralized oversight will be important.

It is equally important to maintain an international approach to cybersecurity because cyber threats are global in nature. Leveraging international, voluntary, market-driven standards in order to increase cybersecurity is key.

We are pleased, therefore, to see these priorities reflected throughout the Draft Report. In particular recommendations 1 through 5 focus on these issues, and we support the implementation of such recommendations.

2. Standards Training

The Draft Report states that the USG should support standards education in technical and graduate educational programs to ensure the development of capacity building in this area. The Draft Report also recommends the expansion of cybersecurity standards training for Federal agency staff. Building cybersecurity capacity is critical to enabling USG officials to play meaningful roles in standards development organizations and to improving cyber resilience and, therefore, BSA supports this effort and the implementation of Recommendation # 6.

Relatedly, BSA encourages the USG to commit to long-term resources for cybersecurity standards development. Both sufficient training, which should be ongoing, and regular travel to standards development organization meetings around the world will require significant funding. Moreover, if USG officials are expected to play meaningful roles—especially leadership roles—in standards development organizations, consistent budgetary support will be required.

3. Use of Standards from Other Domains Relevant to Cybersecurity

BSA applauds NIST’s recognition that the use of international standards is key to enhancing national and economic security and public safety. It is important to focus not only on cybersecurity-specific standards but also on other relevant international, voluntary, and market-driven technology standards to achieve this goal.

For example, eliminating the use of unlicensed software could help reduce the risk of cybersecurity incidents. A recent study by IDC found that there is a strong positive correlation (0.79) between the presence of unlicensed software and the likelihood of malware encounters[2], which could contribute to cybersecurity incidents. In addition, unlicensed software may not be updated with all the security patches that are often released by software publishers increasing vulnerability.

The lack of proper software asset management practices often contributes to the use of unlicensed software. For instance, a recent report by the Government Accountability Office confirmed that the Federal Agencies do not have adequate polices for managing software licenses and this contributes to agencies' use of software that is not properly licensed. Implementing sound software asset management aligned with international standards (e.g. ISO 19770-1:2012) could contribute to increasing cybersecurity resilience. In fact, this practice is aligned with the requirements set forth by the Cybersecurity Act of 2014 that requires NIST to identify information security measures and controls that may be voluntarily adopted by owners and operator of critical infrastructure to help them manage cyber risks (S. 1353, Title I).

We, therefore, suggest that the section that refers to "Enhancing National and Economic Security and Public Security" (line 55) be amended to clearly recommend the use of non-cybersecurity specific standards that can contribute to increasing cybersecurity resilience. Therefore, we suggest that the second recommendation (line 60) is amended as follows:

> *Using international standards as a key part of USG procurement and technology management policy to support secure and resilient operations. In addition to standards focused specifically on cybersecurity, other relevant international, industry-led, and voluntary standards that can contribute to increased cybersecurity should also be used to achieve this goal.*

In addition, we recommend amending Recommendation 8 (line 551) as follows:

> *Recommendation 8: Using ~~Relevant~~ Cybersecurity and Other Relevant International, Voluntary, Industry-Led Cybersecurity and Related Standards ~~for Cybersecurity~~ to Achieve Mission and Policy Objectives*
>
> - *Federal agencies should use cybersecurity and other relevant international, voluntary, industry-led cybersecurity and related standards, where effective and appropriate, in their mission and policymaking activities.*

4. Use of Voluntary Standards in Procurement and Regulatory Activities

The background information section of the Draft Report correctly highlights that Federal Agencies are required to use voluntary standards in their procurement and regulatory activities whenever possible and consistent with the law, according to the National Technology Transfer and Advancement Act (NTAA) and OMB Circular A-119.

This obligation should be emphasized again in the recommendation section. BSA recommends, therefore, adding a new item to Recommendation 8, as follows:

[2] BSA Global Software Survey: The Compliance Gap available at http://globalstudy.bsa.org/2013/index.html

- *Federal agencies must use voluntary standards in their procurement and regulatory activities whenever possible, according to the requirements set forth by the National Technology Transfer and Advancement Act and OMB Circular A-119.*

5. Conformity Assessments

BSA recognizes the value of conformity assessments for some cybersecurity standards. However, BSA encourages NIST to recognize that conformance testing and certification schemes are not appropriate for all cybersecurity standards. The vast majority of standards instead rely upon self-attestation, which is an effective means of assurance. BSA thus suggests that NIST incorporate reference to self-attestation into the Draft Report.

6. Supply Chain Security

Supply chain security is a very important priority for BSA members. Like most cybersecurity issues, supply chain security is incredibly complicated. We commend the Draft Report for seeking ways to improve and streamline standards for supply chain risk management. Currently, the U.S. government has numerous and overlapping supply chain risk management initiatives. We believe that NIST has the unique opportunity to play a key role in bringing order to a currently chaotic landscape.

7. Technology Neutrality

It is important that global standards maintain a technology neutral approach to the products and tools to be used to protect IT systems.

Procurement practices that mandate the use of specific technologies tend to freeze innovation and force users to procure products that might not suit their security needs, jeopardizing cybersecurity.

We recommend that the draft report reinforces the importance of the USG support to international standards that are technology neutral.

8. Ensuring Technically Sound Standards

The requirement for “reasonable availability” of the underlying specifications necessary to implement standards is very important and should be taken into account.

The section of the Draft Report that discusses support for development and use of technically sound standards (page 2, line 67 through 81) should highlight this requirement.

9. Private Sector Engagement

Although the views of the private sector are often times represented through the USG participation in the standard development process, this is not always the case. It is important to ensure that treaty-based international agreements include a mechanism for private sector to provide advice and input given that sometimes the USG is blocked from expressing a view based on disagreements by affected industries.

In addition, when the USG is formulating its position, there needs to be a clear mechanism for soliciting input from affected industries.

The Draft Report recommendations should, therefore, include language that clearly reflects these two mechanisms for private sector engagement.

Conclusion

In light of our shared interests and commitment in the area of cybersecurity, BSA and its members appreciate the opportunity to submit these comments and we look forward to continuing to work with you.

Sincerely,

Lewis

Leticia S. Lewis
Director, Policy
BSA | The Software Alliance