February 19, 2015

VIA EMAIL: cyberframework@nist.gov

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Views on the Framework for Improving Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt,

BSA | The Software Alliance ("BSA") appreciates the opportunity to respond to the National Institute of Standards and Technology's ("NIST") Request for Information about stakeholder views on the Framework for Improving Critical Infrastructure Cybersecurity ("Framework").[1] BSA is the leading advocate for the global software industry before governments and in the international marketplace.[2] BSA members are world class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life.

As providers of technology that is the backbone of the global IT infrastructure and of cybersecurity products and services, BSA members have extensive experience working with government and other stakeholders around the world on cybersecurity policy and standards. This experience has taught us the value of technology-neutral policies that provide guidance on managing cybersecurity risk while offering organizations the flexibility to deploy security measures that are tailored to the specific nature of the risks they face. BSA and its members are therefore very supportive of NIST's work to date in developing and overseeing the coordination of the Framework.

As NIST considers next steps, we urge you to remain mindful of the significant benefits to maintaining the Framework in a manner that will facilitate its adoption by organizations outside of the United States and enable it to serve as a model for international cooperation on strengthening critical infrastructure. With the profile of cybersecurity risks continuing to grow, governments around the world are examining potential domestic policy reforms to address these risks. Unless global norms emerge, there is a considerable risk that multinational companies will find themselves unable to comply with a patchwork of inconsistent international cybersecurity mandates.

Fortunately, we are seeing evidence that other countries are beginning to look to the Framework as a model to draw from as they develop their own cybersecurity policies. Use of the Framework

---

[1] National Institute of Standards and Technology, *Views on the Framework for Improving Critical Infrastructure Cybersecurity; Notice and Request for Information*, 80 Fed. Reg. 76935-36 (December 11, 2015).

[2] BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, Salesforce, SAS Institute, Siemens PLM Software, Symantec, Tekla, The MathWorks, Trend Micro and Workday.

20 F Street NW, Suite 800
Washington, DC 20011

P 202-872-5500
W bsa.org

to assess risk and recommend threat mitigation controls and remediation within the Financial, Electric Utilities, Water Utilities and Oil and Gas sectors is growing in Canada, Japan, Australia, the Middle East and Europe. To ensure that this momentum continues, we recommend that NIST not undertake major reforms to the structure or scope of the Framework at this time. Instead, we encourage NIST to focus on (1) helping to promote domestic and international adoption of the Framework and (2) updating, where necessary, the Framework's list of Informative References.

Encouraging Adoption of the Framework

We are appreciative of NIST's efforts to promote adoption of the Framework by enterprises through participation at workshops and public events and by offering resources on its website that provide practical guidance and tools for implementing the Framework. These efforts are having a material impact on the overall uptake of the Framework.[3] However, there is a risk that these educational outreach efforts may not be reaching less sophisticated audiences who could benefit from the Framework.

We therefore encourage NIST to continue working with its interagency partners to develop an outreach program that is targeted toward promoting adoption of the Framework by small- and medium-sized enterprises ("SMEs"). We recommend a two-prong approach. First, NIST should continue to develop use cases and best practices that illustrate how the Framework can be implemented to improve cybersecurity risk management across a range different business sizes and industries. We further recommend that NIST partner with the U.S. Small Business Administration and the Department of Homeland Security to host additional workshops focused on educating SMEs about the value proposition of implementing the Framework.

To promote international awareness of the Framework and encourage harmonization of international cybersecurity policies, we urge NIST to work closely with State Department's Office of the Coordinator for Cyber Issues ("S/CCI"). As the Administration's chief coordinator for global diplomatic engagement on cyber issues, the S/CCI is uniquely positioned to engage in norm building exercises with our international partners. As part of its capacity building exercises, the S/CCI should actively promote the Framework as a model for cybersecurity policy development. In addition, to further promote global awareness and adoption of the Framework, NIST should consider submitting the Framework as an international standard. Recognition by a standards organization would bolster the Framework's credibility among international constituencies and help to ensure that other countries considering cybersecurity regulations opt for a standards based approach.

Updating Informative References

While it would be premature to pursue major structural reforms to the Framework, NIST should consider adding to the list of Informative References where doing so would advance the Framework's objectives. As but one example, Section ID.AM-2 of the Framework Core relating to asset management of "software platforms and applications" would strongly benefit from the inclusion of a reference to ISO 19770-1. Although the referenced supporting material in Section ID.AM-2 is comprehensive with respect to overall implementation for security management systems and controls, there is a tendency in the existing Informative References to focus more on hardware and data assets than on the underlying software used to process and store such

[3] *See* Government Accountability Office, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, 25 (Dec. 2015) ("Respondents to our survey who indicated they had been promoted to by NIST noted that they were encouraged to use the framework as a result. Specifically, 102 responses out of 132 indicated that NIST promotional activities were "very" or "somewhat" effective in encouraging the use of the framework.")

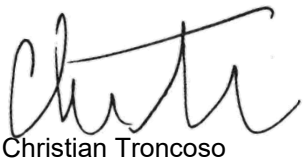
assets. The addition of ISO 19770-1, which focuses specifically on the management of software as a distinct asset, would fill this gap.

Managing software has become increasingly important in the cybersecurity control environment. Studies demonstrate that a significant portion of software in use around the globe is unlicensed. In 2013, the global rate of unlicensed software use was as much as 43%.[4] 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, which could contribute to cybersecurity incidents.[5] In addition, unlicensed software may not receive regular updates or security patches, further increasing potential vulnerability.

With a 2014 IDC study confirming that 57% of IT managers and CIOs either do not perform software audits at all, or perform them less frequently than once a year,[6] it is not surprising that fewer than half of all IT managers are confident that their company's software is properly licensed.[7] The addition of ISO 19770-1 to the Framework would therefore provide helpful guidance for organizations seeking to improve their cyber resilience through the implementation of voluntary and industry-led standards for software asset management practices.

Thank you again for the opportunity to share our views on this important topic.

Sincerely,



Christian Troncoso
Director, Policy

[4] BSA | The Software Alliance, "The Compliance Gap" Global Software Survey, June 2014, *available at* http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf.
[5] IDC, "Unlicensed Software and Cybersecurity Threats," January 2015, *available at* http://www.bsa.org/~/media/Files/Research%20Papers/IDCMalware/FinalIDCMalwareWPJan2015.pdf.
[6] BSA | The Software Alliance, "The Compliance Gap" Global Software Survey, June 2014, *available at* http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf
[7] *Id.*