The Software Alliance

BSA

January 19, 2018

Matthew Barrett
Cybersecurity and Privacy Applications Group
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity

Dear Mr. Barrett,

BSA | The Software Alliance[1] appreciates the opportunity to respond to the National Institute of Standards and Technology's ("NIST") Request for Information about stakeholder views on its revised draft of the Framework for Improving Critical Infrastructure Cybersecurity ("Framework"), Version 1.1. BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members provide cloud services, data analytics, cybersecurity solutions, and other cutting-edge products and services to governments and businesses of all sizes across all industries.

We commend NIST for the transparent, collaborative, stakeholder-driven approach it has taken to updating the NIST Framework. As with the initial development of the Framework, NIST has demonstrated that such an inclusive approach can not only yield highly impactful outcomes, but also generate consensus across industry and government stakeholders to act.

On April 10, 2017, BSA submitted comments in response to NIST's first draft of the Framework update. BSA noted its support for the update as a whole, and proposed modifications to two key areas addressed by the update: the proposed new section on "Measuring and Demonstrating Cybersecurity" and the addition of Supply Chain Risk Management ("SCRM") both as a new category in the Framework Core and as a standalone criterion in the Framework Implementation Tiers. BSA appreciates NIST's efforts to address each of these proposed modifications in Draft 2 of the update.

With regard to the "Measuring and Demonstrating Cybersecurity" section, BSA had expressed concern that the highly conceptual guidance in newly proposed Section 4 might be premature for inclusion in the Framework, suggesting that further work is needed to hone best practices for measuring cybersecurity before the topic is ripe for inclusion in the Framework. Helpfully, Draft 2 of the update re-frames the discussion around ""Self-

[1] BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, IBM, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

Assessing Cybersecurity Risk with the Framework" and moves much of the detailed discussion regarding processes and technical aspects of measuring cybersecurity to the Roadmap. We believe this approach better represents the current state of understanding around cybersecurity measurement best practices, and look forward to working with NIST and other stakeholders to further develop and refine tools to assess the effectiveness of cybersecurity strategies and guide finite investments to best strengthen organizations' cybersecurity.

BSA also proposed that the previous draft's discussion of SCRM should be modified to focus on providing SCRM guidance in the Framework Core, and to refrain from incorporating SCRM into the Framework Tiers, to avoid creating confusion about how Implementation Tiers should be used most effectively. We appreciate NIST accepting this recommendation, and believe the current draft will do much to advance stakeholder adoption of SCRM best practices.

As noted in our previous submission, BSA also commends NIST for its emphasis on identity management, authentication, and access control in Version 1.1 of the Framework. Given that the overwhelming majority of malicious cyberattacks take advantage of compromised identities and credentials, identity and access management is a critical element of strong cybersecurity, and its emphasis in Version 1.1 of the Framework will undoubtedly promote more sophisticated, holistic approaches to securing critical networks.

We would offer two suggestions to the "Identity Management, Authentication and Access Control (PR.AC)" category to further strengthen its impact. First, we recommend that Subcategory PR.AC-4 be modified to address permissions and authorizations of users with enhanced privileges, as follows: "Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties, *including permissions and authorizations for users with enhanced privileges (e.g., IT administrators, CIOs, or CISOs).*" Second, we recommend that Subcategory PR.AC-7 be modified to encourage use of analytics as one potential approach, as follows:"PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor*, and analytics*) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)." The modifications would ensure the PR.AC category reflects current best practices for identity and access management.

The current draft also includes a new subcategory within the Framework's "Respond" function, RS.AN-5: "Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)." BSA applauds this addition. Protecting critical networks against cyberattacks requires vigilant management of network and IT infrastructure to ensure that vulnerabilities are identified and mitigated. In particular, coordinated vulnerability disclosure (CVD) regimes have proven effective in helping to ensure well-intentioned security researchers can use their research to improve the security and integrity of networks and products, without inadvertently exposing these networks and products to greater risk of malicious attack.

BSA believes that encouraging more robust security research and the reporting of vulnerabilities through coordinated vulnerability disclosure can play a critical role in strengthening cybersecurity. Effective vulnerability reporting programs, such as CVD, involve collaboration, trusted communications mechanisms, risk analysis, thorough mitigation testing, and risk-based and user-focused disclosure decisions. In addition to including RS.AN-5 within the Framework Core, it may be helpful for NIST to address the complexities, best practices, and opportunities for further development associated with CVD programs, potentially in the Framework Roadmap.

As NIST looks toward future development of the Framework, the Roadmap offers an opportunity to identify "key areas for development, alignment, and collaboration." BSA would highlight software security, and particularly the encouragement of secure software development, as an important area for future development. While the NIST Framework is intended to focus on organizational risk management processes for owners and operators of critical infrastructure systems, software applications are increasingly integrated into those systems. Software is increasingly delivering greater efficiency, functionality, and security to the infrastructure upon which the United States economy is built. As the importance of software has increased, the way software is developed and deployed has also continued to evolve. New development methodologies offer means to increase the speed, precision, and integrity with which software is produced and deployed, as well as new approaches to testing software in development and identifying vulnerabilities before products reach the market. Use of such secure software development lifecycle processes should be encouraged, and how to encourage secure software development holds great relevance to the security of critical infrastructure.

There is no one-size-fits-all approach to software security; in fact, several variations of secure software development lifecycle processes have proven effective. Yet, despite differences, common practices and principles have been identified as key elements across these variations. BSA urges NIST to identify collaborative, stakeholder-driven development of guidance for encouraging the adoption of secure software development lifecycle processes for software components of critical infrastructure networks within the Framework Roadmap, emphasizing secure software outcomes while accounting for differing approaches to process. In future iterations of the Framework, it may be appropriate for NIST to include its Special Publication 800-160 as an "Informative Reference;" similarly, it may be useful to consider secure software development processes in the context of the Framework's discussion of supply chain risk management. As software increasingly drives the efficiency and functionality of critical infrastructure, ensuring that security is integrated into software development would add a robust new line of defense to secure the nation's critical infrastructure.

Thank you for the opportunity to comment on this important matter.

Sincerely,

Tommy Ross
Senior Director, Policy