From: **Abagail Lawson** <alawson@eastwest.ngo>
Date: Mon, Apr 10, 2017 at 2:16 PM
Subject: CSF Version 1.1 comments for submission
To: cyberframework@nist.gov
Cc: Bruce McConnell <bwm@eastwest.ngo>, Andreas Kuehn <akuehn@eastwest.ngo>, Anneleen Roggeman <aroggeman@eastwest.ngo>

Dear NIST Colleagues,

Please find attached a letter submitted on behalf of the EastWest Institute with comments on the draft Version 1.1 of the Cybersecurity Framework. Thank you for your consideration of our input, and we look forward to the release of the final Version 1.1 later this year.

Sincerely,
Abagail Lawson

Abagail Lawson
Program Coordinator

[Attachment Copied Below]

April 10, 2017

From: Bruce McConnell, Global Vice President, EastWest Institute, and Andreas Kuehn, Senior Program Associate, EastWest Institute, on behalf of the EastWest Institute (EWI)

To: NIST, Cybersecurity Framework Team

Subject: Comments on Developing a Framework to Improve Critical Infrastructure Cybersecurity (Cybersecurity Framework)

In response to the Request for Information (RFI) from the National Institute of Standards and Technology (NIST), regarding the Cybersecurity Framework (CSF) V1.1, the EastWest Institute (EWI) staff respectfully submits these comments, on behalf of the Breakthrough Group on Increasing the Global Availability and Use of Secure ICT Products and Services. EWI's Global Vice President, Bruce McConnell, served as the Acting Deputy Under Secretary for Cybersecurity for the U.S. Department of Homeland Security. In that role, he provided active support and guidance in the development of the initial CSF. Today, McConnell welcomes the opportunity to further contribute to the Framework's evolution in his current role.

EWI is pleased to see this draft of the CSF posted for comment and is encouraged to see the additions related to supply chain risk management. The CSF provides useful guidance and we encourage its broad use and adoption. Including supply chain risk management is timely and an important move forward for the CSF as it reflects a crucial source of risk.

EWI has been working on supply chain risk for several years as part of its Breakthrough Group on Increasing the Global Availability and Use of Secure ICT Products and Services under our Global Cooperation in Cyberspace Initiative. In September 2016, in cooperation with our partners, Huawei Technologies, Microsoft, and The Open Group, EWI released the EWI ICT *Buyers Guide* ("*Purchasing Secure ICT Products and Services: A Buyers Guide"*). The *Guide* is a resource that helps organizations begin a conversation with their suppliers on risk-informed security requirements that they might ask of, or require from, their suppliers to help them better understand and manage supply chain risk.

EWI has been active in raising awareness about supply chain risk and the importance of buyers using risk-informed, security-related procurement requirements to incentivize providers to raise the security assurance bar. We have organized and participated in domestic and international events, including an invitation-only workshop and a panel on supply chain risk at the 2016 ITU Telecom World in Bangkok, Thailand; participated in an ITU-D sponsored workshop on cybersecurity in January 2017 in Geneva, Switzerland; organized a webinar on supply chain risk on critical infrastructure for DOE contractors; and provided briefings on to the Software and Supply Chain Assurance Forum hosted by DoD, DHS, NIST and GSA.

Most recently, we conducted three workshops on supply chain risk and the EWI ICT *Buyers Guide* at our Global Cyberspace Cooperation Summit in Berkeley, CA March 14-16, 2017. In this setting, we explored ways to foster collaboration among organizations that work on supply chain risk. Invited experts included representatives from SAFECode, NIST, the Financial Service Roundtable/BITS, NERC, The Open Group, the Global Forum on Cyber Expertise, and former officials from the FCC (Homeland Security and Public Safety Bureau) and the Office of the U.S. Trade Representative.

As part of the EWI effort, we will promote awareness of the *Guide* and we solicit input to inform a revised version of the *Guide* to be released in 2017. In the revised guide, we hope to reflect changes in the NIST CSF and provide guidance on how to address supply chain risk consistent with the CSF.

EWI endorses the CSF as a useful document, encourages its broad use across the ecosystem, and references the CSF as such within the *Buyers Guide*. The value of the CSF stems from its ability to be used as a risk-analytic tool, global security baseline and collection of industry best practices, which can be applied broadly to many organizations of different sizes and sectors. Our detailed feedback below is consistent with our endorsement of these core principles of the CSF. As such, while recognizing the timeliness and importance of providing organizations with tools to improve supply chain security, it is equally important to do so in a manner that is aligned with the CSF's core principles of broad usability, cross-sector application and flexibility over a diverse set of stakeholders.

We are convinced of the importance of providing guidance in the revised CSF about how organizations need to assess their risk posture in a way that includes supply chain risk.

Please find our comments below. Thank you for your consideration in addressing them in the new CSF.

Sincerely,

Bruce McConnell
Global Vice President, EastWest Institute

Andreas Kuehn
Senior Program Associate, EastWest Institute

Attachments:
EWI ICT *Buyers Guide* (version 1.0)

Comments:

We would like to bring the following issues to NIST's consideration:

(1) Update Informative References to include a more Comprehensive Set of Standards Relevant to Supply Chain Risk.

The proposed update prominently addresses supply chain risk in two out of three main parts of the CSF; namely, the *Framework Core* (as in category ID.SC and subsequent subcategories, and in subcategory ID.BE-1) and in the *Framework Implementation Tiers* ("Tiers").

The proposed revisions to the CSF (pages 30-31, Table 3: Framework Core) include only a minimal set of standards in the informative references under the proposed new category, Supply Chain Risk Management (ID.SC).

Therefore, we would like to encourage NIST to extend the set of standards and suggest NIST to consider *adding* the following references to the list of *informative references to all of the ID.SC sub-categories*:

- ISO/IEC 20243
- ISO 27036
- NIST SP161

Adding ISO/IEC 20243, ISO 27036 and NIST SP161 as informative references would increase awareness of the threats that should be of concern to business partners. These references would also increase awareness of the technology development and supply chain processes that governments, critical infrastructure owners and operators, and other organizations should be asking of, or requiring from, their suppliers in their procurements as part of their cybersecurity risk management processes relative to supply chain.

In particular, we suggest adding the following to the informative reference sections in ID.SC:

- **ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
    - **ISO/IEC 20243** 4.1 – 4.2.1.12

- **ID.SC-2:** Identify, prioritize and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment process
    - **ISO/IEC 20243** 4.1 – 4.2.1.12, Assessment Procedures for 20243 4.11- 4.22

- **ID.SC-3:** Suppliers and partners are required by contract to implement appropriate measures, ***based on global standards or other global guidelines,*** designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan. **NOTE**: Suggest a change to this subcategory, which includes "*based on global standards or other guidelines"* per bolded text above.
    - **ISO/IEC 20243** 4.2.1.4, 4.2.1.5

- **ID.SC-4:** Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted
  - **ISO/IEC 20243** 4.1 – 4.2.1.12, Assessment for 20243 4.11-4.22

- **ID.SC-5:** Response and recovery planning and testing are conducted with critical suppliers/providers
  - **ISO/IEC 20243** 4.1.2.4 – 4.1.2.6

In addition, a more detailed discussion of the standards and how they enable users of the CSF to implement supply chain risk management may provide useful guidance.

Therefore, we suggest adding references to the EWI ICT *Buyers Guide*, including the questions in appendix B "Cybersecurity Perspectives: 100 Requirements When Considering End-To-End Cybersecurity With your Technology Vendors" to the updated CSF.

The EWI ICT *Buyers Guide* also provides a mapping of relevant standards, including a discussion regarding the specific areas of application, third-party certification, product development requirements, and supply chain risk requirements. We suggest the revised NIST CSF to include a description and mapping of these standards based on the EWI ICT *Buyers Guide*.

The CSF V1.1 seems to avoid addressing the issue of what questions owners/operators should be asking their providers from a product integrity and supply chain security perspective.
The EWI *Buyers Guide* identifies those questions and, equally as important from a scalability perspective, points to several standards and certification programs that implicitly address many of those questions related to product and supply chain security.

We believe it would be beneficial to add the EWI *Buyers Guide* either as an Appendix to the CSF or as an informative reference, which may fit well in the category ID.SC-3.

(2) Strengthening the usability of the CSF

To improve the usability of the CSF and the new parts on Supply Chain Risk Management, we suggest providing references to other materials, such as the EWI ICT *Buyers Guide* and resources NIST has developed (e.g., profiles for the CSF). Such resources can be used to explain how the new additions of Supply Chain Risk in CSF V1.1 are used in practice.

In addition, the maintenance of the CSF's broad usability across a diverse set of stakeholders is key in the Framework's success and adoption in the U.S. and internationally. Additions of new topical areas, such as supply chain risk management, should reflect needs of the cybersecurity ecosystem and be done in a way that is both scalable and flexible to accommodate the differing risk management needs and resources of the highly varied set of Framework users. By focusing on processes and outcomes generally and highlighting specific standards and guidelines that explicitly and comprehensively address software and hardware integrity and supply chain security practices in the informative reference sections, users are able to select those aligned with their profiles. Subsequently, the key message that supply chain security is an integral component of cybersecurity risk management is strengthened.