From: **Dennis Amari**
Date: Mon, Apr 10, 2017 at 3:12 PM
Subject: Comments on Draft Update of Cybersecurity Framework
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: Donald PurdyJr

Please see the attached comments submitted by Huawei Technologies on the Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity.

If you have any questions/concerns regarding these comments, please feel free to contact either myself or:

Donald A. Purdy, Jr., CSO
Huawei Technologies, Inc. (USA)

Thank you,
Dennis J. Amari

Dennis J. Amari | Dir., Federal & Regulatory Affairs
Huawei Technologies, Inc. (USA)

[Attachment Copied Below]

April 10, 2017

From: Huawei Technologies

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

To: NIST, Cybersecurity Framework Team

In response to the Request for Information (RFI) from the National Institute of Standards and Technology (NIST), regarding the Cybersecurity Framework V1.1, Huawei Technologies USA respectfully submits these comments.

In general, Huawei is supportive of the intent behind the draft revised version (1.1) of the Cyber Security Framework (CSF) made available for comment. Having participated in five of the initial workshops for Version 1.0 of the CSF and opportunities to participate in public-private discussion about the CSF, and to provide formal and informal comment submissions, we applaud the thoughtful, collaborative approach that has been used throughout the development of v1.0 and draft v1.1.

In addition, we know that supply chain risk was highlighted in the Cybersecurity Framework Roadmap, and we are supportive of the ongoing effort to raise awareness of the importance for organizations to understand, consider, and address supply chain risk, and to consider supply chain risk in procurement/buying decisions of both government and private organizations.

We have organized our comments in three sections:

I. Executive messaging;

II. Promoting understanding on how to use the CSF to understand and address risk, including supply chain risk; and

III. Comments on the revisions proposed in v 1.1.

I. Executive Messaging

We recommend that in the U.S. NIST work with DHS, and other lead agencies for the U.S. critical infrastructure sectors, through the public-private partnership model, to promote understanding among leaders of government and private organizations of their due care and due diligence responsibilities (and fiduciary for private company leadership) to address risk to their organizations -- including cyber security and privacy risk relative. And communicate the fact that corporate boards and C-level executives "own" risk to their organizations and need to act accordingly. The CSF provides a risk-analytic tool that will help them do that.

Our premise is that an important and appropriate starting point for discussions and communication strategies related to cyber risk is to begin at the top, not just at the tactical level focusing on the criticality of the roles of CISO, CIO, Risk office, and the importance of a cyber expert having regular face-time with the Board, or even with how to persuade or incentivize Boards to care about cyber. We believe that we can strategize about how to communicate about – and, in fact – impact the due care requirements for Boards of Directors and C-level and other senior executives.

In our view, it is important for NIST, in collaboration with others, to communicate the following messages in connection with v 1.0 and in the impending release of v 1.1, later in 2017:

(1) there are fiduciary/due care/due diligence responsibilities of the leaders of private organizations (Board and C-suite) and government organizations, which essentially require them to consider implementing the measures recommended below (*in some shape or form*);

(2) the Board, and senior leaders, own the risk to the organization and, accordingly, must have a handle on what the organization needs to worry about from a risk perspective, what they need to do about it, and how they are progressing.

(3) there should be an enterprise-wide risk management program that addresses security and privacy risk [this concept is referenced in the recent Internet Security Alliance/NACD publication: https://www.nacdonline.org/AboutUs/PressRelease.cfm?ItemNumber=39211https://www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=10687.] We believe that due care requires an organization to use a risk-analytic approach – like the NIST Cybersecurity Framework (CSF) – to determine the organization's risk posture and enable the organization to chart a course toward a more appropriate risk posture, customized to the organization's business objectives, risk environment, and risk tolerance of the particular organization.

A key message NIST could communicate is that due care requires that third-party risk be part of the overall risk equation of the organization, and that third-party risk includes risks related to all third-party products and services, including the technology development and supply chain risk of the ICT (information and communication technologies) products. Too many organizations do not seem to understand this; they seem to think supply chain risk is a "bridge too far." Accordingly, it is important to message that due care requires that

organizations address supply chain risk and that procurement practices of the organization should take into account this risk.

Part of the message should be that the buyers of ICT should develop risk-informed procurement requirements and partner with like-minded buyers to leverage their purchasing power to incentivize the availability and use of more secure products and services. In September 2016, the EastWest Institute issued an *ICT Buyers Guide* to help organizations start a conversation with their suppliers to begin to include security requirements in their procurements (https://www.eastwest.ngo/idea/purchasing-secure-ict-products-and-services-buyers-guide). Providing a more detailed approach regarding acquisition of software, SAFECode (www.safecode.org) is working to update a similar type of buyers guide to give guidance on security questions the buyers might began to ask of their suppliers, or impose as requirements for the procurement.

It would also be helpful if NIST would work with DHS, and other lead agencies for priority critical infrastructure sectors, again, through the public-private partnership model, to develop voluntary, sector-focused risk-informed security-related requirements for ICT procurements. Leveraging the purchasing power of ICT buyers will undoubtedly incentivize suppliers to raise the bar and help to reduce sector risk. One example is the Communications Sector that could build on the exemplary work of the FCC advisory group, CSRIC, to voluntarily identify cyber security best practices for the sector and to provide guidance to the sector (and its five major sub-sectors) about the use of the CSF to understand and address supply chain risk. It is a logical step to encourage them to create voluntary, sector-focused risk-informed security-related requirements for ICT procurements.

For an organization to understand and address risk, there should be an organization-wide committee/task force/working group (or its equivalent) that oversees the risk management program that includes representatives of each key element of the organization (business groups, department, HR (e.g., all employee training and testing; specialized training for specialized roles), IT, legal, CIO, security, risk officer, audit/compliance), which provides visibility to enable the Board to meet its responsibility

The committee/working group can ensure that internal requirements are identified, set, monitored, and updated as needed, for each key element of cyber security and privacy risk (HR, legal, service delivery, etc.). It would also be helpful if organizations can be encouraged to develop and implement an internal compliance program to track and ensure compliance selected requirements, and, from time to time, to engage outside independent experts to verify the status of the effort, for the same reason that independent accounting firms are used for financial audits.

II. Promoting understanding on how to use the CSF to understand and address risk, including supply chain risk.

NIST's efforts to promote awareness and understanding about the use of CSF have been commendable and valuable for the many organizations that are using or considering using the CSF. As consideration is given to whether, how, how much, and when to revise v1.0, though, it important to keep in mind that many organizations are just beginning to use 1.0. For them, this is a work in progress, just as the CSF is a body of work that is likely to be

periodically revised over time, whether or not the CSF 1.1 is finalized and released in 2017 as planned.

NIST's most recent efforts, including the widely viewed webinar (with two valuable presentations about the use of 1.0 and about 1.1, respectively, available on the NIST website) have provided very constructive and specific guidance about how an organization develops its risk profile. Significantly, the manufacturing sector conceptual profile referenced in the first of the two decks presented on the webinar, is backed up by a very lengthy and instructive document about the process, that is also on the website. Unfortunately, it is not clear whether and how the conceptual profile includes the risk from the suppliers of the sectors. Nor is it clear how the risk profile (illustrated by the manufacturing sector example) should be depicted to show supply chain risk (and the impact of that risk on the organization's overall risk (profile)).

It would be extraordinarily helpful if NIST could work with a few companies, perhaps in different sectors, to create at least notional risk profiles that include and depict supply chain risk. If they could be created prior to the May 16, 17 workshop, perhaps they could be circulated in advance and be the subject of a session of the workshop dedicated to the issue. This could not only help attendees and others better understand how supply chain risk is supposed to be included (whether using v 1.0 or v1.1), but it could also help shine light on whether and how the CSF could best be modified at this time to provide appropriate guidance.

It may be that it may take more experience with the CSF over time to generate broader consensus on possible revisions related to supply chain risk. It is important to strike the right balance between waiting for more information that can only be gleaned from experience and providing guidance to help organizations in the meantime.

III. Comments on the revisions proposed in v 1.1.

Part of the need to promote greater awareness of the importance of using the CSF and how to use it, and about the need to include supply chain risk, can be accomplished by executive messaging and greater awareness as suggested above.

There is no one right answer to what the correct balance is between waiting for more information that can only be gleaned from experience and providing guidance in the CSF to help organizations in the meantime. I recommend using a light touch in proposing revisions, centered around revisions that can provide high-priority guidance to help in use of the CSF, recognizing that additional changes can be made in the future.

The issue of whether to include the supply-chain related guidance for the demarcations for the four Tiers is not without controversy. However, the proposed supply chain revisions to the Tiers are quite consistent with the existing general guidance (which some have criticized as too vague), are not prescriptive, and will help put organizations on notice that supply chain risk is officially part of the equation.

The next level of proposed revisions has to do with the proposed addition(s) to the Core of the CSF; specifically, by adding references to supply chain risk management in the Identify

Function at the Category level (and some sub-categories). No additional categories are proposed to be added to any of the other four functions.

It is by no means essential to add the supply chain references at the Category level, but is it logical to do it ONLY in the Identify Function and not others; would it be helpful?

It is not clear that it is the right decision to add supply chain risk ONLY to the Identify Function and not in one or more other Functions, such as Detect and Protect. But it is not a clear matter. Isn't there an aspect of supply chain risk related to the importance of the acquiring company being able to detect vulnerabilities, incidents, or other problems in the supplier company(ies) technology development or supply chain risk? Isn't there a similar aspect related to the ability to implement Protect measures at the supplier level? There may be Response and Recover aspects also.

There has been some discussion about whether the approach of the CSF is "operational" in construct so that supply chain activities do not run across all of the Functions. If that is the approach, it is not immediately clear why it would be proposed for inclusion as a Category in the Identify Function.

If it doesn't make sense to add supply chain risk to the Category level only in the Identify Function, would it make more sense to make supply chain risk an overlay of the CSF, generally, rather than add it to just one Function?

There is an argument that by including supply chain risk at the Category level in the Identify Function it promotes awareness of the importance of addressing supply chain risk as part of the CSF risk analytic model, but doesn't complicate the use of the CSF by interjecting it at a similar level of other Functions. But will including it in the Identify Function suggest that there is no connection between supply chain risk and the Functions of Detect, Protect, Respond, and Recover?

On balance, while it is not essential that it be included in the Identify Function at the Category level, it promotes the supply chain risk awareness priority in a non-prescriptive manner.

It is important to keep in mind, as the FCC Advisory Group, CSRIC, demonstrated in their March 2016 report giving guidance to the sector on using the CSF to address supply chain risk, it is arguably possible to use CSF 1.0 to consider supply chain risk without any changes to the Core.

Finally, because a new category has been proposed to be added to the Identity Function for supply chain risk (Supply Chain Risk Management (ID.SC)), along with several sub-categories within that category (ID.SC1-ID.SC5), I recommend that the informative references that were added for these new subcategories be further revised to add relevant supply chain security standards.

One of the major drivers for the addition of supply chain risk is to make sure organizations take into account and address risk from products and services they obtain from others. Accordingly, it is logical and important to suggest that they evaluate their suppliers using the analytic approach of the CSF, which includes normative references to applicable

international standards and best practices to reduce that risk. Just as the CSF provides normative references for operators to consider as bench-marks for addressing their risks, so it should provide normative references that are relevant to the risk of products and services they obtain from others.

The proposed revisions to the CSF (pages 30-31, Table 3: Framework Core) include only a minimal set of standards in the normative references under the proposed new category, Supply Chain Risk Management (ID.SC), undoubtedly because of the strict criteria used in the selection of what would be included, which includes the requirement that the standard be “widely adopted.” We think that this element of the criteria should be stricken so that otherwise qualifying and appropriate – and helpful -- standards can be included. This is particularly the case because “widely adopted” is a subjective term – for example, many relevant cyber and supply chain standards are based on best practices that are already adopted by some of the most mature vendors in the industry (e.g., ISO/IEC 20243 and ISO 27036). The CSF should not use a criterion that at least implicitly discourages the creation of internationally recognized standards that fill gaps, or represent significant improvement, relative to existing standards. Given that premise, we would suggest adding ISO/IEC 20243 and ISO 27036 to the informative references in the supply-chain subcategories.

Thank you for your consideration of these comments and recommendations.