Comments of Huawei Technologies

Framework for Improving Critical Infrastructure Cybersecurity
Version 1.1 Draft 2

National Institute of Standards and Technology

January 19, 2018

In general, there are a number of positive changes proposed in this draft relative to the CSF version currently in effect, which explicitly add supply chain risk management to the Framework Core, the Framework Profile, and the Framework Implementation Tiers.

First, as we suggested in our most recent comments, inclusion of an addition to the Framework Core of a Category for Supply Chain Risk Management (SCRM) is very important. Previously the CSF consideration of product suppliers and others providing third-party services (often involved in the delivery chain; e.g. cloud suppliers, third-party data center, managed services, etc…) were buried deep in the other Categories or were implicit in the scope of risk analysis. It is also worth considering whether language should be added to emphasize that SCRM includes third-party services, as well as providers of technology and other products. The addition of SCRM to the Sub-Categories is also helpful.

Following up on the discussion in our most recent Comment regarding whether Supply Chain Risk Management should be largely confined to the Identify Function, upon further reflection and consideration of other NIST and industry materials, we believe that the Protect function should be modified to explicitly state that supply chain risks that were not adequately addressed by the supplying organization as part of the SCRM process (pursuant to the SCRM Category in Identify) before the product or service was acquired/used by the acquiring organization, need to be addressed/mitigated as part of the acquiring organizations activities in the Protect Function. Similarly, if the third-party service provider is found to be introducing risk into the acquiring organization, then not only is the Protect Function implicated, so is the Response Function, and possibly even the Recovery Function.

Second, the clarified and improved revisions to the guidance on Framework Tiers with respect to SCRM and external stakeholders is definitely helpful.

Third, the proposed addition of section 4.0, Measuring and Demonstrating Cybersecurity, is a positive step, although it may still be too generic. Use of the CSF could be supported with tools that assist in measuring outcomes without becoming overly specific.

We recommend closely studying some repeated wording of Subcategory outcomes for the reason of apparent overlap because there are important differences in context that can have a dramatic effect on outcomes. Because the wording of Sub-Category outcomes may be similar during an assessment this sometimes creates confusion for assessed organizations when responding to questions. While we understand the reasoning that is generally due to the different context

(Category) it may create situations where we appear to be asking the same questions (i.e. looking for similar outcomes). See, for example, PR.AC-4 and PR.PT-3, PR.AC-5 and PR.PT-4

Fourth, the Informative References should be closely reviewed for accuracy of applicability and placement within the CSF References and should be expanded to be more inclusive of the references that are helpful in particular industry sectors and subsectors. For example, some of the original Informative References had what appeared to be errors in mapping as they had very little to do with the referenced Category/Sub-category and accordingly caused confusion with respect to the intended outcome. Additional Informative References from other standards may help provide clarity on the expected outcomes of each Sub-Category. An example of references that need to be reviewed for accuracy in references are the references to the Center for Internet Security Cyber Security Controls.

Fifth, although the revised draft gives greater emphasis to privacy (for example, including "people") it is somewhat limited in the extent to which it covers privacy and security of Personally Identifiable Information (PII). While the relevant wording is in the document section (3.6) but is largely missing from the actual Sub-Category outcomes. It might be worth considering the approach of the EU GDPR to security relative to privacy. While it is technically a European regulation, the discussion regarding approaches to security of PII in Article 32 are worth considering for inclusion into the Framework.

Six, while the Framework is primarily geared toward operational environments and, other than a few Subcategories referencing other parts of the development lifecycle there appear to be gaps in addressing risk in development organizations. The new wording adds some clarity but outcomes are still largely lacking.

Regarding specific question asked by NIST

Do the revisions in Version 1.1 Draft 2 reflect the changes in the current cybersecurity ecosystem (threats, vulnerabilities, risks, practices, technological approaches), including those developments in the Roadmap items?

Yes, these changes better cover typical environments. Specifically, the addition of Supply Chain Risk Management is important because this is a critical factor in almost all service delivery chains today.

For those using Version 1.0, would the proposed changes affect their current use of the Framework? If so, how?

Yes, it helps to enhance the ability to work with the Framework. The new version has minimal negative impact on our current implementation of the Framework.

For those not currently using Version 1.0, would the proposed changes affect their decision about using the Framework? If so, how?

Yes, it helps to promote the Framework as more accessible and its continued evolution is helpful for gaining management buy-in to extend the use of the Framework across the organization