January 19, 2018

VIA EMAIL: cyberframework@nist.gov

Edwin Games
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899

Re: McAfee's comments in response to NIST's Solicitation for Comments on "Draft 2 of Cybersecurity Framework Version 1.1"

McAfee LLC appreciates the opportunity to respond to the National Institute of Standards and Technology (NIST) request for comments on the *Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity*, posted on December 5, 2017. McAfee has been an active participant alongside NIST during the initial development of the Cybersecurity Framework and hopes NIST finds our comments useful.

McAfee, an independent cybersecurity company, is focused on accelerating ubiquitous protection against security risks for people, businesses and governments worldwide. We are responding today to comment on the proposed Draft 2 changes to the Framework. McAfee is committed to improving the global security ecosystem and has been demonstrating that support by our global outreach in support of the Framework. McAfee has long shared the sentiment with governments worldwide that we cannot delay in collectively addressing the evolving cybersecurity threats facing us all. McAfee continues to lead efforts to improve cybersecurity across the compute continuum.

Our response includes answers to the specific questions asked in the "Notes to Reviewers" section of the draft, as well as our comments on the proposed changes in the Framework draft.

Before beginning our comments, we want to express how extremely pleased we are to see that NIST has demonstrated once again that it listened to industry, took industry's recommendations and made Draft 2 a more useful enhancement to the Framework. Thank you.

Notes to Reviewers

In the *Notes to Reviewers* section, NIST requested public comment specifically regarding the following questions. We have provided answers to each.

- ***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?***

While there is always room for improvement, as reflected in some of our comments, we believe the Framework Version 1.1 Draft 2 has included much of what is needed to improve an organization's cyber risk management program. Additional areas included and refined in this version, such as coordinated vulnerability disclosure and a focus on incorporating how to deal with the evolving threat landscape, are vital for organizations to understand and incorporate into their cyber risk management processes. Please refer to our recommendation on the security considerations for internally developed tools below.

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

  The current changes should not have any negative effect on implementing this version (v1.1 Draft 2) as compared to implementing the 1.0 version of the Framework. The fundamentals are the same with enhanced considerations and subcategories to self-assess against.

- ***For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?***

  We cannot answer this question directly but we know Draft 2 will be much easier and more cost effective than had Draft 1 been approved as the final 1.1 version.

Our Comments

The Framework needs to continue to be as widely applicable as possible

We are pleased to see items specific to the U.S. government, added in the V1.1 Draft 1, have been removed from this version. This document continues to have global influence and the authors should continue to keep that perspective in mind in all future enhancements and versions.

Treating the Framework as a framework

The Framework is not a recipe book. It is a bit surprising that more focused text is not included that states this. In our use of the Cybersecurity Framework, we treat it like the risk management framework that it is. As such, we believe tailoring the Framework to meet our business needs is a net positive. Tailoring of areas such as Tier definitions, Categories and Subcategories was intended during the initial development of the Framework. Sadly today, the only reference to tailoring any part of the Framework comes in section 3.3 when discussing using a sector established Target profile and sector constituents using that to build their organization's "tailored Target Profiles."

We believe organizations implementing the Framework should be encouraged to tailor the Framework to better fit their individual business priorities and processes in order to gain the most value from it. We would like to see this more clearly called out in the Framework itself.

Documentation explaining the Tiers needs to be expanded and clarified

As the original version did, the Framework uses the verbiage in the Tiers to describe itself, making the definition self-referencing. There needs to be a clearer explanation of the Tiers and their value to the overall evaluation process.

The Implementation Tiers would benefit from more explanation before jumping into the Tier Definitions. Tiers have a very important dual purpose in the Framework process. Tiers are foundational to both establishing an organizational target for what is an acceptable level of risk (Target) and in the assessed organizational cyber posture outcome (Current).

Tiers need to be reasonably understood on various levels. Explaining a definition with a definition is typically not a good way to convey information effectively. We would like to see more clarifying information up front so as not to rely solely on the definitions to describe themselves. This is one area we are consistently asked about. More distinct descriptions need to be given for each of the Tier definitions and what constitutes the differences between the Tiers. Expanded descriptions of each Tier would be helpful in clarifying the latter.

Additionally, a more logical flow would be to place the Framework Profile (section 2.3) before Implementation Tiers (section 2.2). It would create a better flow in describing the value of the dual use of the Tiers. Currently the draft talks about Profiles in the Tier section without having described them. Reversing the two sections would make it easier to expand and explain the Implementation Tiers in a more coherent fashion.

Metrics and Measurements - Changing directions on measuring implementation success of the Framework

McAfee is happy to see NIST listened to the chorus from industry and McAfee, who felt the v1.1 wording and approach to Metrics and Measurements was a violation of the intent of the Framework. The purpose of the Framework is to provide an organization with a means to improve its security program, not to be a means for external comparison with others in a specific sector or geographic region. It is not intended to give regulators the ability to enforce any arbitrary level of security. The Framework is a tool that organizations should be using to help guide them in incorporating better cyber risk management capabilities at all levels of their business. While measurement is important, the initial wording in version 1.1 Draft 1 focused too much on external audits and assessments. The focus on "Self-Assessing Cybersecurity Risk with the Framework" is much more aligned with what we believe is the proper direction for overall cyber risk management improvements.

That said, the following text is confusing and needs to be expanded with examples to help the implementer better understand what is meant by lagging and leading measurements:

> *For example, tracking both security measures and business outcomes may provide meaningful insight as to how changes in granular security controls affect the completion of organizational objectives. While it is sometimes important to determine whether or not an organizational objective was achieved through lagging measurement, leading measurements*

of whether a cybersecurity risk may occur, and the impact it might have, are typically more important to determining likelihood of accomplishing an organizational objective.

Supply Chain Risk Management Changes

While we agree, the inclusion of Cyber Supply Chain Risk Management (SCRM) is a critical component to any organizational Cyber Risk Management process, we believe there is a great deal of work needed to properly integrate this into the Framework. NIST needs to assure it is a positive addition to the Framework, not a costly one, and one that does not have a negative impact on adoption and use of the Framework.

The above is what was included in our comments for v1.1 Draft 1. The focus on SCRM was too heavy a lift for most organizations to actively support. McAfee is pleased to see NIST listened and removed the C-SCRM sections from the Tier definitions while appropriately including supply chain considerations into the External Participation components of the Tier levels. The "Communicating Cybersecurity Requirements with Stakeholders" section is much improved and is a welcomed addition in its educational tone and content.

Coordinated vulnerability disclosure and handling processes included (RS.AN-5)

McAfee is pleased to see NIST has added the RS.AN-5 sub-category and associated Informative References to Draft 2. Any reasonable security program should have processes established to effectively work with those, both internally and externally, who have discovered vulnerabilities within the organizations products, services or support infrastructure.

The Informative References for RS.AN-5, however, are incomplete, as they do not include ISO/IEC 29147 and ISO/IEC 30111 references despite being mentioned in the Roadmap. For clarity and to reduce potential confusion with other incident management efforts, we believe adding these standards as Informative References for RS.AN-5 in the Core will clarify that the subcategory focuses on coordinated vulnerability disclosure.

Additionally, we appreciated seeing the discussion of coordinated vulnerability disclosure in the draft Roadmap version 1.1.1.

Improving the "How to Use the Framework" section

There should be more discussion within the "How to Use the Framework" section. This section is extremely important, and at the time of its original writing, there were no real lessons learned that could be included. Now that industry has experience using the Framework, this area would benefit from their inclusion.

We have and continue to encourage NIST to either have a track in a future workshop or to convene a group for those who have actively implemented the Framework with the purpose of sharing successful practices and challenges they have experienced. This would provide valuable

[1] Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, Dec. 5, 2017, pg. 5, https://www.nist.gov/sites/default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf.

input for creating a secondary deliverable documenting an improved process that leverages the lessons learned, pitfalls avoided and emerging best practices in integrating the Framework into an organizational security program.

Integrity of the assessment process

When performing evaluations, we intentionally separate those individuals who created the Target Profile from the actual Assessment team. We do this so as not to bias the Assessment SMEs with what we were targeting to achieve. The Assessment team is not aware of the target profile until the assessed results are compiled. We believe this approach is essential to the integrity of the overall process and should be mentioned in the Framework process itself. We believe this should be called out in section 3.2, Establishing or Improving a Cybersecurity Program. This separation should be continued in subsequent years as the organization reviews and updates their Target Profile to accurately reflect their current organizational level of acceptable risk.

Inconsistency in Framework Naming

Version 1.1 Draft 2 has various ways of naming the Framework. The title lists it as the "Framework for Improving Critical Infrastructure Cybersecurity." The "Framework" is used throughout the document as the main reference. Besides the page headers, the term "Cybersecurity Framework" is used twice in the document -- in the heading of section 1.2 and in actual text in section 4.0. The industry has named it the Cybersecurity Framework. We recommend introducing the term "Cybersecurity Framework" earlier in the introduction with a statement referring to its subsequent use as the "Framework." Then the dual use make sense.

Secure Software Development

Many corporate network security and infrastructure staff develop specific applications, middleware or integration components for specific corporate needs. Many of these development efforts are "quick and dirty" development efforts meant to solve a specific integration or short term "gap" need. Often, the software created is meant for short-term use but ends up in production environments, making the organization's infrastructure much more vulnerable to attack. It is important for organizations to consider security while internal tools are being developed. We believe there needs to be some mention in the Core of the importance of "security and privacy by design" principles. Often these types of tools are not appropriately identified and understood and are overlooked. While these types of capabilities and internally developed tools are needed to assure business objectives are met, often only a single developer knows about their existence and the level of security considerations that went into their development. Internally developed tools need to have just as much security review and focus as vendor developed tools -- and in many cases, more.

We expected this type of risk was already covered in the existing informative references for asset inventory, software integrity or code scanning language. We have, however, been unable to find

it. As this is more common approach to integration issues, we believe it needs to be identified and addressed.

Roadmap issues

Confidence Mechanisms

One of the problems industry had with v1.1 Draft 1 was the apparent direction change on the use of the Framework from the standpoint of organizational improvements vs. external audits and conformance assessments. The latter leads to increased expenses for organizations that are not focused on improving a security program and more focused on proving something to outsiders and regulators. The section on Confidence Mechanisms uses examples of organizations developing third-party review processes and certification capabilities. These examples are not needed to prove the point NIST is trying to make. Calling out these type of efforts as examples seems to indicate that NIST is encouraging movement away from voluntary self-assessment that has been a major reason for the success of the Framework.

Informative Reference Mappings

Today the Informative References are a limited, static set of standards -- CIS CSC, COBIT 5, ISA 62443-2-1:2009, ISA 62443-3-3:2013, ISO/IEC 27001:2013 and NIST SP 800-53Rev. 4 -- from five different organizations. From the beginning, a process needed to be established where the informative references in the Framework Core could be updated without having to completely reissue the entire Framework document. We have seen over the past few years the real need for other informative references to be included and/or mapped to the Framework.

McAfee welcomes the discussion in the Roadmap on Referencing Techniques. Additionally, we wholeheartedly encourage the rapid development of the online searchable format NIST is pursuing. A capability such as this provides for the addition of a much more robust set of mapped standards to be used as informative references.

International outreach is critical for aligning and improving global cybersecurity.

Cybersecurity is not a single nation's problem. It is a global problem. The Framework would benefit from much more international participation during its continuing development. At the same time, the Framework is an important tool for helping to harmonize cybersecurity initiatives and legislation throughout the global community. The Framework has the potential to be extremely beneficial in this regard by providing common requirements as well as educational and strategic approaches. We applaud NIST for the work it has done in this area and urge NIST and other stakeholders to redouble its outreach efforts to include international partners. Continued educational efforts to promote the voluntary, flexible cyber risk management approach and the international standards underpinning the Framework will help align the cybersecurity governance and regulatory actions taken by other countries.

Summary

Thank you again for allowing us the opportunity to provide comments on the Cybersecurity Framework version 1.1 Draft 2. We are pleased that NIST has been mindful of the recommendations from industry and has reflected them in Draft 2.

Over the last few years the Framework has successfully helped change the security landscape dialog from “compliance” to “risk management” within a large portion of U.S. organizations. This is an extremely positive trend. It is important the Framework continue to pursue this path. The Framework commendably represents an effort to solve the complex problem of protecting ourselves from cybersecurity threats in a way that harnesses private sector innovation while addressing the cybersecurity needs of governments, businesses and citizens. The focus on reviewing, understanding and improving organizational cybersecurity protection programs is a positive change from where organizational focus has been in the past. The transparent and collaborative process NIST led in developing the Framework has served as a model not only for other U.S. government agencies, but for governments worldwide seeking to address cybersecurity-related issues. McAfee looks forward to continuing to partner with NIST as it develops future versions of the Cybersecurity Framework.