From: **Landfield, Kent**
Date: Mon, Apr 10, 2017 at 4:05 PM
Subject: Intel and McAfee Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Mr. Games,

We appreciate the opportunity to be able to respond with our Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity. Included are the joint comments from Intel Corporation and McAfee LLC.

We look forward to continuing the dialog on improving the Cybersecurity Framework and to attending the Framework development workshop in May.

Thank you.

Kent Landfield
McAfee, LLC.

[Attachment Copied Below]

April 10, 2017

Via e-mail to cyberframework@nist.gov

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

Re: Intel and McAfee's comments in response to NIST's Solicitation for Comments on 'Cybersecurity Framework Draft Version 1.1'

Intel Corporation and McAfee LLC appreciate 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*, noticed on January 25, 2017. Both Intel and McAfee have been active participants alongside NIST during the initial development of the Cybersecurity Framework.

During the initial development of the Framework, McAfee and Intel responded to and participated in the Framework development workshops as two separate organizations. Since then, McAfee was fully integrated into Intel Corporation as the Intel Security Group. This business unit combined Intel's subsidiary McAfee with other security resources within Intel, forming a single organization. Recently Intel Security has been spun out as McAfee, an independent cybersecurity company which, as a standalone business, is focused on accelerating ubiquitous protection against security risks for people, businesses, and governments worldwide. We are responding today in unison as two organizations that both have the same perspective on the proposed changes to the Framework.

Intel was one of the very early adopters of the Framework and was also one of the first companies to come out in public support of the Framework, as we did by publishing of our whitepaper, *The Cybersecurity Framework in Action: An Intel Use Case*, as well as giving multiple presentations and engagements at the Framework workshops, 2015 RSA Conference, and other venues. Intel and McAfee are committed to improving the global security ecosystem and as such have been demonstrating that support by our global outreach in support of the Framework. Intel and McAfee have long shared the sentiment with governments worldwide that we cannot delay in collectively addressing the evolving cybersecurity threats facing us all, and Intel and McAfee continue 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. We preface our responses with this summary regarding the major areas of change represented in the draft 1.1 version of the Framework.

1. **The Framework needs to continue to be as widely applicable as possible.**

   Items specific to the U.S. Government seem to have been added, which have little place in a document with such wide global applicability.

2. **The Framework needs a known process for updating it incrementally.**

   There needs to be a known and well-documented process established where components of the Framework can be updated, such as the informative references in the Framework Core, without having to completely reissue the entire Framework.

3. **We do not believe the Measuring and Demonstrating Cybersecurity is ready to be included.**

   This section is confusing as to what it is trying to do. It seems to be trying to establish a language for use but does not do so in a manner that adds benefit and improves the Framework. This needs much more discussion and rework to be a useful component of the Framework. This is one area that would be better addressed outside the Framework in an ancillary document targeting measurement.

4. **Supply Chain Risk Management (SCRM) is overly impactful as currently defined.**

   As was the case with earlier efforts around incorporating technical privacy standards, we believe the current incorporation of cyber supply chain risk management in this draft is immature and overly impactful for most organizations, and needs considerable rework.

5. **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, i.e. the definition is self-referencing. There needs to be a clearer explanation of the Tiers and their value to the overall evaluation process.

6. **Rework language that makes it seem the Framework is only for Critical Infrastructure organizations.**

   The Framework has broad applicability and as such, should not dissuade others from utilizing it.

7. **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 educational, requirements, and strategy approaches.

8. **The Framework is missing various items critical to any organizational cyber risk management program improvement process.**

   Some areas of this document need expansion and further explanation, for example, External Participation is not just about "information sharing." There are also additional processes organizations need to incorporate as they implement and improve their cybersecurity risk management program.

Notes to Reviewers

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

- ***Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?***

  Yes. We believe there are two crucial and fundamental areas missing from the Framework: threat intelligence and vulnerability disclosure.

  Today, security programs must have a detailed understanding of the threats, both external and internal, technical and human, to their organization. The Framework needs to incorporate the threat intelligence lifecycle into categories and subcategories of the Framework Core. This may also include adding additional categories or subcategories as appropriate.

  Vulnerabilities found in an organization's products or infrastructure can have a critical impact on an organization's security posture. Often those weaknesses are discovered by entities outside the organization. There is a common misconception that vulnerability disclosure processes are only for product vendors. Vulnerabilities exist not just in products but potentially in an organization's deployed infrastructure as well. It is important to provide a known channel for entities outside the organization to report issues in a private and structured way, describing what they have encountered and provide a means to communicate with them while the issue is being corrected.

  Additionally, we believe modifications are needed to the Tier definitions for an organization to properly evaluate itself. We believe the Tier definitions for External Participation needs to be expanded beyond just simple information sharing to include more focus on other areas of coordination with external parties such as a vulnerability disclosure process.

  We believe these are equally essential to any modern corporate security program.

- ***How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?***

We believe the Cyber Supply Chain Risk Management (SCRM) changes proposed for version 1.1 are too large and complex an effort for most organizations to actively support and should not be included in their current form. While the Framework was initially targeted at Critical Infrastructure organizations, it has become readily apparent the Framework is useful to a wide range of organizations from the smallest to the largest. Not all users of the Framework are large corporations capable of mobilizing large resources to address security issues. In many cases, essential services are supplied by SMBs who have disproportionally few resources available. The SCRM changes, while well intended, could put a burden on organizations of all sizes. In essence, to implement the SCRM requirements in the recent modifications, organizations may have to stand up a new internal governance office to monitor and manage what is requested in the draft. That potentially adds significant and unnecessary cost and complexity to utilizing the Framework.

Additionally, we believe SCRM should not be included in the Tiers at all since it is already covered by other areas specified in the Tiers. Supply Chain Risk Management is a component of an organization's Risk Management Process. There is no need to call out individual components in the Tiers.

The SCRM section, as written will have a real impact on adoption. While we agree, there is a need for SCRM to be called out in the Framework, there is still work needed to integrate it correctly to assure it is a positive and not a costly addition to the Framework.

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

  As described above, the SCRM aspects will impact all organizations and we will be one of them. One of the positive aspects of the initial version of the Framework is that it was lightweight and fit well into our existing risk management processes. Modifications such as SCRM, as documented in the draft, start to deviate from that initial, successful goal.

- ***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 are not able to address this question directly but we ask you keep in mind the Framework needs to be flexible enough to address organizations of all sizes and missions. It should continue to be a useful tool focused on assisting organizations in improving their overall cyber risk management program. If the Framework becomes too onerous to implement, it will have a negative impact on the overall ecosystem with unintended consequences.

- ***Does this proposed update adequately reflect advances made in the Roadmap areas?***

  NIST's Improvement Roadmap identifies several important focus areas – but not all of them may be appropriate or ripe for inclusion in the Framework itself. NIST's

Roadmap identifies many important areas of future focus necessary to improve cybersecurity, whether by NIST or others. Some areas in the Roadmap are not suitable for direct incorporation into the Framework, for instance, the Cybersecurity Workforce. Other Roadmap areas may potentially mesh eventually with the existing Framework structure and content, but are not yet ready for inclusion in the Framework proper. Areas such as the Technical Privacy Standards, where the prerequisite foundational work to develop standards are still a work-in-progress, are premature to include.

- ***Is there a better label than "version 1.1" for this update?***

  Yes. Once approved and published, the "current version of the Framework" would be an accurate way to describe it. The intent of the question seems to indicate NIST is looking for a different name for this specific version. That would not be helpful as we have worked hard as a community to brand the Cybersecurity Framework globally.

- ***Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?***

  We believe it is time to review and update the Framework Roadmap using the same successful collaboration process used initially to develop the Framework. It is time to refocus the Roadmap on the requirements and goals of the Framework itself and not on the programs supporting it. If nothing else, the Roadmap should be reorganized to indicate what are programs and what are items being worked for inclusion in the Framework itself. NIST and other stakeholders should be both patient and selective as we collectively evaluate Roadmap focus areas to build out future versions of the Framework.

Our Comments

Measuring and Demonstrating Cybersecurity

While we believe the ability to measure and track changes/trends in an organization's program for improving their cybersecurity risk posture is an extremely important aspect of any risk management process, it is important the language describing the process is crisp, precise and adds value to the overall evaluation.

Statements such as "*In combination with Informative References, the Framework can be used as the basis for comprehensive measurement*", when combined with others such as, "*Therefore, the measurement system should be designed with business requirements and operating expense in mind. The expense of a measurement system may increase as the accuracy of measurement increases*" do not seem particularly helpful in achieving the initial statement. A large benefit of the Framework is that it can be applied quickly and with minimal overhead. The above requires all organizations using the measurement aspects of the Framework to design their own measurement system. This is a very difficult task even for mature cybersecurity programs, and

the challenges of meeting this requirement could easily dissuade organizations from utilizing the Framework altogether.

It would have been more useful if this section had not focused on language but instead focused on a process for rolling up Subcategory scores to arrive at an overall Category score. Organizations would benefit by using that information in creating roll-up result documents for shareholder use, for example, heat maps or integration with corporate governance and operational dashboards.

The entire section is confusing as to what it is trying to accomplish. It seems to be trying to establish a language for use but does not do so in a manner that adds benefit or improves the Framework. This is one area that requires a good deal more explanation to be effective and valuable. We believe this topic would be better addressed outside the Framework in an ancillary, Framework-related document specifically targeting measurement and we recommend NIST take that path.

Implementation Tiers

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 normally not a good way to convey information effectively. We would like to see more clarifying information up front and not 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 would constitute the differences from one Tier to another. Additional descriptions of each Tier could go a long way in clarifying the latter.

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

Supply Chain Risk Management

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 SCRM changes proposed for version 1.1 are an extremely heavy lift for most organizations to actively support and should not be included in its current form. The SCRM changes, while

well intended, could put an extreme burden on organizations of all sizes. In essence, to implement the SCRM requirements in the current 1.1 draft, organizations may have to stand up a new internal governance office to monitor and manage what is requested. That adds real cost and complexity that is not necessary.

We believe SCRM should not be included in the Tiers at all. Supply Chain Risk Management is a component of an organization's *Risk Management Process* and *Integrated Risk Management Program*, both of which are components of all current Tier definitions. There is no need to call out individual components in the Tiers. If done in this manner, the Tier definitions could become bloated and complex, neither of which is a desirable outcome.

In draft version 1.1 there is an entirely new Category (ID.SC) added under the Identify Function. This seems extremely limiting. Not all cyber SCRM activities will or should reside in just one function. We believe SCRM-related concepts and activities should be incorporated across the Functions, into existing Categories, creating new subcategories where relevant and appropriate. As with items such as cyber threat, information sharing, vulnerability disclosure, and other areas, SCRM references, such as SP 800-161 and SP 800-53, should be added to the appropriate and relevant subcategory Informative References.

International Outreach

There is growing international interest in the Framework. Accordingly, we urge NIST and other stakeholders to redouble their 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 it gain traction among international government and industry partners and help align the cybersecurity governance and regulatory actions taken by other countries. The Cybersecurity Framework development collaboration has been working to bring consistency to voluntary approaches towards cyber risk management in the US. International understanding of it and participation in its development is needed. As such, while the Framework was initially developed in the U.S., it is now very important for the Framework to have active participation from our partners across the globe if it is to be applicable and gain acceptance in other parts of the world.

Federal Alignment

The proposed section on Federal Alignment should not be included in the Framework document. We do not see any value in including specific U.S. Federal government guidance and directions in a document that has global applicability. This seems completely out of place and adds no value to the Framework itself. It has the potential to negatively affect the international perception of the Framework and hinder global adoption and use. Instead, such guidance should be in a separate document targeted directly at the U.S. Government that can be modified as needed for USG purposes without adversely affecting the Framework.

Updating the Framework

Today the Framework is comprised of two distinct pieces, the process documentation and the Core specification. The Core includes mapped informative references. As initially developed, both are one document; one integrated whole. We have seen over the past few years the need for other informative references to be included. There will always be additional updates needed. Today, simply supplying an updated list of standards, guidelines and practices require we sync the changes with new / future releases of the Framework. This causes many to wait much longer than necessary. By developing a means for updating both the Process documentation and the Core, changes can then be made to either part of the Framework without negatively affecting how people use it. This topic should be discussed at future Framework development workshops.

Additional Considerations

Lessons Learned: 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 including those.

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 the hurdles we have had to overcome. This would go a long way to providing valuable input on improving the Cybersecurity Framework. These sessions could also provide valuable input for creating a secondary deliverable documenting an improved process leveraging the lessons learned, pitfalls avoided and some emerging best practices in integrating the Framework into an organizational security program.

Missing Threat focus: One area missing in the first version of the Framework are people, processes and technology related to Threat. While the Framework's Roadmap included Automated Indicator Sharing, we believe it goes well beyond that. We believe Cyber Threats, Insider Threats as well as Physical Threats to the corporation and their mission is sorely needed to round out the Framework. Today's corporate security organizations all need or have a Threat Management component to them. It is vital for organizations to understand the evolving threats they face each day if they are going to be able to properly protect themselves and their assets. As the Framework is risk-based, it is critical it include risk-related threat aspects in the Core so an organization can properly evaluate themselves.

Integrity of the assessment process: When performing our evaluations, we intentionally separate those individuals that created the Target Profile from the actual Assessment team. We do this so as not 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.

Include reference to the new Information Sharing and Analysis Organization (ISAO) construct: The Framework's reference to ISACs in section 2.2 should instead reference ISAOs as the foundational information sharing construct. ISACs are a form of an ISAO.

Summary

Thank you again for allowing us the opportunity to provide our comments on the Cybersecurity Framework version 1.1 draft. Over the last few years the Framework has successfully helped to change the 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 cyber security 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. Both Intel and McAfee look forward to continuing to partner with NIST as it develops future versions of the Cybersecurity Framework.