December 13, 2013

Via e-mail to csfcomments@nist.gov

Information Technology Laboratory
ATTN: Mr. Adam Sedgewick
National Institute of Standards and Technology
10 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Re: Intel and McAfee comments in response to NIST RFC, "Request for Comments on the Preliminary Cybersecurity Framework"

Dear Mr. Sedgewick,

Intel Corporation and our subsidiary, McAfee, appreciate the opportunity to respond to the National Institute of Standards and Technology (NIST) Request for Comments on the Preliminary Cybersecurity Framework, noticed o October 29, 2013. We would like to commend NIST for continuing its long history of tight coordination and collaboration with the private sector, and in particular for developing the Framework using such an inclusive process. NIST's stewardship in producing what we believe is a highly successful Framework via such an open and transparent process can and should serve as a model for the agencies tasked with implementing other aspects of the EO.

Intel and McAfee share a commonality of interest with governments in the US and globally that we cannot delay in collectively addressing the evolving cybersecurity threats facing us all, and indeed our companies have been at the forefront of efforts to improve cybersecurity across the compute continuum. Over the last decade we have invested billions of dollars to develop software, hardware, services and integrated solutions designed to advance cybersecurity across global digital infrastructure that predominantly operates via interoperable hardware and software products which d not vary significantly for individual countries and are deployed worldwide. Countering the increasingly sophisticated cybersecurity threats to critical infrastructure, networks, intellectual property, and privacy requires the cooperative efforts of government, industry and NGO stakeholders working together to improve cybersecurity in a way that promotes innovation, protects citizens' privacy and civil liberties, and preserves the promise of the Internet as a driver of global economic development and social interaction.

Please see below our narrative comments, concerns and recommendations regarding the Preliminary Cybersecurity Framework, organized by section.

Section 1.0 - Framework Introduction

Better articulating the benefits of the Framework to businesses, its intended usage and scope, and the international standards foundation underlying the Framework could be beneficial to numerous audiences, including both SMEs and the international community. We recommend the following for the Introduction section:

Help companies make the business case for framework adoption.
The Introduction could better articulate the benefits of the Framework, including the business case, to broad cross section of organizations, including large corporations and SMEs alike. While the Introduction understandably touts the important national and economic security benefits of cybersecurity standards and best practices, companies are more likely to be motivated to use the Framework if compelling business case is communicated to them.

Make clear the desired broad applicability of the Framework.
While the EO and the framework are primarily targeted at improving critical infrastructure security, NIST and other Administration representatives have stated the hope that a much more diverse cross section of entities will use the Framework. NIST should make the goal of broader business applicability and uptake of the Framework explicit in the introduction.

Highlight the Framework's usefulness as a tool for internal organization or sector use.
The Framework produced by NIST in collaboration with the private sector is most helpfully viewed as a tool organizations or sectors can use to leverage existing international standards to evaluate their current practices and processes in terms of their security posture, aid them in deciding where they would like to be in the future, and to produce an internal roadmap for getting to where they want to be. By developing both a Current and Target Framework Profile, an organization can evaluate itself against the Framework Core Functions, Categories and Subcategories, thus producing a visual depiction of both the current and target state of its cybersecurity program. Analysis derived from the Framework should not produce metrics for external consumption or comparison across organizations or sectors. Rather, we support use of the Framework as tool for allowing individual organizations to develop, track and plan improvements around internal security practices, processes and procedures.

Make explicit that global standards are a foundational Framework element.
The Framework Introduction points out its reliance on existing standards, guidance, and best practices; however the preference for global standards, and that the Framework align with global standards as called for by the EO, should be made more explicit in the Introduction. Highlighting the practical applicability of global standards will benefit the development of global security marketplace solutions, and will potentially help the Framework gain traction internationally as an alternative to more regulatory cybersecurity approaches.

Section 2.0 - Framework Basics

Tier usage and implementation guidance must be improved.
The discussion of Tiers as currently described in the Framework still seems to be incomplete and may cause confusion because of the lack of discernible linkage to the Framework Core elements, and the lack of clear methodology or implementation guidance to explain how the Tiers should be applied or used. This ambiguity about the intended use of the tiers exacerbates concerns regarding how the Tiers might be misused. For example, some have pointed out that CI/KR owners/operators may try to require vendors to achieve unreasonably high Tier levels through contractual mechanisms, thus skewing the resources and liability

equations for many organizations. A similar concern exists that overzealous sector specific agencies might impose requirements linked to Tiers via regulation. These concerns are valid, and if the tiering is left unexplained and disconnected from the Framework Core it could chill Framework adoption.

We recommend the Framework make it abundantly clear the Tiers are intended for internal use and consumption by companies or sectors. By making it plain the Tiers are intended to be used by organizations to, for instance, conduct self-assessments of their cybersecurity programs and target improvements, the Framework document can help proactively mitigate against misuse of the Tiers externally by third parties.

Section 3.0 - How to Use This Framework

Th Framework should include a more robust "How to Use the Framework" section.
Sections 3.0-3.3 should include more explanation to describe the process, as organizations need clear guidance to understand to how to apply the Framework. For example, informative references should be called out more in *Step 1: Identify*. It would be helpful to understand what each of the subcategories is trying to accomplish through added guidance. Additionally, examples of how companies can extend the Framework to meet operational or enhanced mission needs would also be helpful. More work is also needed to provide implementation guidance in these sections, and NIST should further spearhead an effort in this regard.

Future NIST framework adoption assistance needed.
NIST recently published a proposed definition of "adoption" following the 5th Cybersecurity Workshop in Raleigh, NC. According to NIST, *"An organization adopts the framework when it uses the Cybersecurity Framework as a key part of its systematic process for identifying, assessing, prioritizing, and/or communicating: cybersecurity risks, current approaches and efforts to address those risks, and steps needed to reduce cybersecurity risks as part of its management of the organization's broader risks an priorities"* [emphasis in original].[1]

While we appreciate this effort and understand the importance of providing additional guidance to organizations regarding the concept of voluntary "adoption," we recommend that such adoption guidance remain outside the Framework document itself.

Adoption of the Cybersecurity Framework will require an active and planned outreach program. Once the Framework is officially released, NIST should take an active role in the outreach required to engage those who most need to use the Framework, such as they did with their very successful workshops in the development period. There are many forms of outreach that should be considered, including developing Framework related education materials as well as working with DHS and the SCCs to evangelize the Framework within the sectors, for example. NIST needs to be an active participant in the needed outreach if the Framework is to be successful.

Add a revised methodology to protect privacy and civil liberties for a cybersecurity program to Section 3.0.
While we support the President's direction to NIST in the EO to include a methodology "to protect individual privacy and civil liberties" in the Framework – indeed, in our April 8 comments to the initial RFI we recommended that "the Framework should comprehend global privacy and civil [liberties] practices … based on internationally recognized Fair Information Practice Principles (FIPPS)"[2] - we have concerns regarding the manner in which NIST attempted to execute this privacy and civil liberties objective.

[1] Update on the Development of the Cybersecurity Framework, December 4, 2013, available at http://www.nist.gov/itl/upload/nist_cybersecurity_framework_update_120413.pdf
[2] Se Intel April letter, p. - http://csrc.nist.gov/cyberframework/rfi_comments/040813_intel_part_1_of_3.pdf].

First, the protection of privacy and civil liberties is relegated to separate Appendix B, disconnected from both the cybersecurity risk management processes forming the Functions at the heart of the framework, as well as the cybersecurity activities, mature global standards, and best practices described in the detailed Appendix A Framework Core. Second, Appendix B sets forth broad privacy methodology not circumscribed by organizations' cybersecurity practices, tethered instead to the broad functions and categories generally applicable across an organization's cybersecurity risk management program and activities – despite NIST's acknowledgment that "not all Categories give rise to privacy and civil liberties risks." Further, the broad privacy methodology in Appendix B is mapped to "the few identifiable privacy standards or best practices" that exist, in stark contrast the menu of mature cybersecurity best practices and standards represented by the Informative References in Appendix A.

The net result is that Appendix B as it appears in the Preliminary Framework is likely unintentionally confusing, as many organizations seeking to use the Framework might interpret it as calling for the creation of a parallel privacy and civil liberties protection program in addition to and beyond the scope of the cybersecurity risk management program contemplated by the Framework proper. Additionally, because Appendix B as written includes broad and open-ended standards and best practices listed as Informative References which don't have clear nexus to cybersecurity– and thus may be interpreted as applying broadly to an organization's commercial operations– we are concerned that the current approach may chill adoption of the Framework. Finally, the Appendix Framework Core already appropriately includes measures and controls designed to protect privacy and civil liberties, including the protection of PII – fact which adds another layer of confusion and complexity for those organizations seeking to apply the Methodology.

We recommend NIST take a simpler and more streamlined approach to incorporating a privacy and civil liberties methodology in the Final Cybersecurity Framework 1.0 that it publishes in February, 2014. In our view, the clearest way to communicate to organizations that they should both consider the impacts of their cybersecurity activities on, and take steps to protect, individual privacy and civil liberties, is to include simple implementation guidance along these lines as a separate subsection following, or as part of, Section 3.0, "How to Use this Framework." Including the privacy methodology here, as opposed to in an Appendix, should make it much clearer to organizations contemplating how to use the Framework that they should be considering the potential impacts of their cybersecurity activities on individual privacy and civil liberties, as opposed to trying to broadly protect privacy beyond the cybersecurity context. Additionally, the Methodology should:

- Scrap the Informative References included in the current Appendix B given NIST's acknowledgement that "few identifiable privacy standards or best practices" currently exist, and the identification of privacy standards development as a key "area for improvement in Appendix C.
- Identify only those potential privacy and civil liberties considerations related to cybersecurity activities, and articulate corresponding measures and controls to ensure consideration of "proportionality" between security and privacy considerations by organizations using the Framework (as opposed to attempting to map privacy and civil liberties considerations to all functions and categories articulated in the Framework Core).
- Make clearer that the Methodology called should leverage organizations' existing privacy programs and processes, and be complementary to its cybersecurity and business operations, as opposed to calling for the creation of a new or separate privacy protection program. One way this could be accomplished is by amending Line 391 to read, "The Framework is designed to complement existing business, cybersecurity, and privacy operations."

Appendix A: Framework Core

Ongoing Compendium maintenance is needed.
The third footnote in the document states, "*NIST developed a compendium of informative references gathered from the RFI input, Cybersecurity Framework workshops, and stakeholder engagement during the Framework development process includes standards, guidelines, and practices to assist with implementation. The Compendium is not intended to be a exhaustive list, but rather starting point based o stakeholder input.*"

It is important to actively maintain the Compendium in conjunction with the Cybersecurity Framework. Since the Framework is primarily targeted at critical infrastructure, it would be appropriate to establish a location where CI/KR organizations could go for additional references that pertain to their sector. Because of the dependency relationships the CI/KR landscape fosters, maintaining these types of references in any place other than NIST means some may have trouble finding what they need and make correlating dependency information harder. We recommend NIST evolve the Compendium into document that targets the expansion of the Cybersecurity Framework Informative References to include sector specific references as provided by the CI/KR owner/operators and others.

Appendix C: Areas for Improvement for the Cybersecurity Framework.

Automated indicator sharing should be prioritized.
Today there are many forms of information sharing, as noted in the Framework. It is important NIST assist in developing trusted means for automated information sharing to include threat indicators and indicators of compromise. To accomplish this in an automated fashion takes trusted implementations based on solid standards. NIST should be a catalyst in putting those types of standards in place.

Interdependencies should be included.
"Interdependencies among and between sectors" was topic addressed in the RFI and draft Preliminary Framework that was not included in the current Framework. The topic should be included in the Areas for Improvement since, for example, threat or mitigation in one sector could have adverse repercussions in another sector. Further, we recommend that NIST document use case and implementation guide that demonstrates how the Framework can help address interdependencies. While this is a challenging topic, it is a worthwhile area for future improvement.

Appendix D: Framework Development Methodology

While this information is useful in a draft, this appendix and the information provided is not necessary to the final version 1.0 of the Cybersecurity Framework. The development effort would make useful case study but as critical part of the Framework itself, there seems to be little value to include it other than for historical reference.

Additional materials are neede to support the CSF

We believe supporting collateral documentation should be created and made widely available to assist organizations considering whether to use the Framework, and to help spur Framework use:

- Customer consumed means to assist with Current and Target profile generation
- Measurement / assessment – internal Tier calculations
- Economics of CSF with success stories
- Making the business case
- Integration of cyber physical systems
- Collection of sector specific supporting materials

We also recommend the development of a centralized location for documents such as the compendium to create a knowledge base of how-to documents where sector related supporting materials can be housed. Whether this compendium is maintained by NIST or another entity, it is important to have central location where people are directed to that can be easily found. The availability of such a central reference repository would help greatly in assisting with adoption. The types of supporting materials should include materials to assist education and corporate process integration. We recommend NIST list reference to such a location in the Cybersecurity Framework itself, so those using the Framework have a starting point to gather additional information related to their mission, services, and sector.

NIST can provide incentives support

While DHS is the lead federal agency responsible for incentives and the voluntary program, NIST can and should play a key role here that will help foster adoption of the Framework. While some incentives under consideration will require budgetary and legislative actions, NIST can assist in communicating the benefits of Framework to Federal Agencies, to incentivize them to begin to use the Framework as baseline for cybersecurity policy development, and to streamline regulations. As Agencies review their current cybersecurity regulatory requirements pursuant to Sec. 10 of the EO, NIST can play an important role in assisting Departments and Agencies to map existing regulations to the Framework. Such mapping exercises will provide real value to regulated private sector entities by identifying the common set of regulatory requirements regulated industries already have to deal with today, eliminating overlaps among existing laws and regulations, and enabling equivalent Framework adoption in cost-effective manner.

Governance and Future Directions

We recommend the creation of a cross-sector industry advisory panel, tasked with developing and implementing a governance plan. To ensure the long-term success of the Framework, we believe an ongoing, formal strategic dialogue between NIST and the various industry sectors is necessary to help future versions of the Framework evolve in a way that is beneficial.

NIST has already stated they would rather not be responsible for the Cybersecurity Framework development process long term. One model the panel described above should consider, and that we are supportive of, is an industry-driven non-profit organization taking over the long-term governance of the Framework. There is precedent for this; a similar model already exists for the Smart Grid and NSTIC IDESG efforts. This model has the advantage of having an independent, non-governmental body steering the process and the private sector taking the lead on this critical topic.

Summary

Thank you again for the opportunity to provide comments on the Preliminary Cybersecurity Framework. The Framework commendably represents an effort to solve the complex problem of better protecting our critical infrastructure and other entities from cybersecurity threats, in a way that harnesses private sector innovation and market forces while addressing the cybersecurity needs of governments, businesses and citizens. The transparent and collaborative process NIST has led, in partnership with the private sector, in developing the Framework thus far can serve as model not only for other USG agencies as they implement other aspects of the EO, but for other governments worldwide seeking to address cybersecurity challenges. We look forward to continuing to partner with NIST as it develops Cybersecurity Framework 1.0, and to participating in the creation of future versions, as well as the ongoing governance of the Framework.