October 10, 2014

Via e-mail to cyberframework@nist.gov

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

**Re: Intel comments in response to NIST RFI, "Experiences with the Framework for Improving Critical Infrastructure Cybersecurity"**

Dear Ms. Honeycutt:

Intel Corporation appreciates the opportunity to respond to the National Institute of Standards and Technology (NIST) Request for Information (RFI), "Experiences with the Framework for Improving Critical Infrastructure Cybersecurity," noticed on August 26, 2014. We would like to commend NIST for continuing the inclusive coordination and collaboration with the private sector that marked the development of the Framework during the first eight months since the Framework 1.0 release. NIST's continued stewardship and close partnership in first producing and now working with private and public sector organizations to foster Framework awareness, understanding and development has been an essential element of the Framework's early success.

Security has long been an Intel priority. Indeed, security, along with power-efficient performance and connectivity, comprise the three computing pillars around which Intel concentrates our innovation efforts. Less than one year ago, Intel formed a new business unit to further the security pillar – the Intel Security Group – combining our subsidiary McAfee with all other security resources from across Intel to form a single organization focused on accelerating ubiquitous protection against security risks for people, businesses, and governments worldwide. Intel has long shared the sentiment with the U.S. and global governments that we cannot delay in collectively addressing the evolving cybersecurity threats facing us all, and Intel and Intel Security will continue to lead efforts to improve cybersecurity across the compute continuum. One way we have demonstrated such leadership is by investing billions of dollars over the last decade to develop software, hardware, services and integrated solutions to advance cybersecurity across the global digital infrastructure. Another is by working collaboratively with government, industry, and non-governmental organization (NGO) stakeholders 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.

**Intel Corporation**
Government Affairs Office
1155 F Street N.W.
Suite 1025
Washington, D.C. 20004

We preface our responses to the specific RFI questions with the below summary feedback regarding the major areas of inquiry presented in the RFI, as well as our sense of the timing of this and other efforts to understand Framework progress.

- **Reminder: We are at the preliminary stages of Framework understanding.** As the development of the Framework was nearing its completion, former NIST Director Pat Gallagher said we were "at the end of the beginning." We know NIST fully understands Dr. Gallagher's words hold true today, just eight months since Framework 1.0 was released. We also understand why NIST and other government stakeholders are anxious to gain a better understanding of whether the Framework is "working," and that some of those stakeholders will perhaps be less patient than others as we collectively seek to make sense of the early Framework feedback generated by this RFI. Nonetheless, as an organization currently using the Framework, we believe the fact that we are at such an early stage must be reiterated, and we urge NIST and other stakeholders to view the RFI responses through this lens – because it is early, we should expect wide disparities in both awareness and experiences, particularly amongst and between organizations of different sizes and risk-management maturity levels. In other words, while we hope the responses NIST receives provide beneficial learnings, we do not believe this preliminary feedback should be considered definitive.

- **Awareness appears significant and broad-based.** Other stakeholders, such as industry associations, are better positioned than Intel to comment on the degree of awareness among government and industry stakeholders in the U.S. However, one aspect of awareness Intel observed first-hand is the growing international interest in the Framework. Accordingly, our responses below focus on Intel's participation in international outreach efforts, and urge NIST and other stakeholders to redouble their broad outreach efforts to include international partners. Continued education efforts to promote the voluntary, flexible, risk management approach and the international standards underpinning the Framework may help the Framework approach gain traction among international government and industry partners.

- **Intel's early experience with the Framework has proved valuable**. Intel is using the Framework across our enterprise, as further detailed below. With the caveat that we are still in the early days, some of the early benefits we have realized through our initial use of the Framework include: (1) improved harmonization of risk management methodologies and a common language across internal stakeholder communities; (2) low implementation cost, as the Framework is aligned well with Intel's existing risk management processes and was easy to learn because it was based on existing industry best practices; (3) improved visibility into our risk landscape, enabled by mapping risk assessments of Framework Core items across our enterprise to create a single risk "heat map" to better visualize certain organizational trends and groupings; and (4) enablement of better-informed risk tolerance discussions among decision makers regarding our enterprise risk goals and strategies.

- **NIST's Roadmap identifies several important focus areas – but not all of them may be appropriate or ripe for inclusion in future versions of the Framework.** NIST's Roadmap identifies many important areas of future focus necessary to improve cybersecurity, whether by NIST or other stakeholders. While all of the Roadmap areas are no doubt important, some may

not be suitable for incorporation into the Framework, such as Cybersecurity Workforce. Other Roadmap areas may potentially mesh with the existing Framework structure and content, but are not yet ripe for inclusion in the Framework proper – for instance, areas such as Technical Privacy Standards, where the prerequisite foundational work to develop standards is just beginning. This is not to say that all of the Framework areas aren't worthy of NIST's attention, but rather that, NIST and other stakeholders should be both patient and selective as we collectively tackle these cybersecurity challenges and evaluate which Roadmap focus areas warrant inclusion in future versions of the Framework.

Please find Intel's responses to the majority of the specific questions in the RFI below. Our responses track the manner in which the questions were presented in the RFI: Section I provides responses regarding Current Awareness of the Cybersecurity Framework; Section II, Experiences with the Cybersecurity Framework; Section III, Roadmap for the Future of the Cybersecurity Framework. We have attempted to answer all questions to which we believed Intel could provide a substantive and helpful response. As a result, please note we have not answered certain questions that are more appropriately answered by industry associations or organizations in regulated industries.

## Section 1: Current Awareness of the Cybersecurity Framework

*Recognizing the critical importance of widespread voluntary usage of the Framework in order to achieve the goals of the Executive Order, and that usage initially depends upon awareness, NIST solicits information about awareness of the Framework and its intended uses among organizations.*

6. ***Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?***

This summer Intel Security staff traveled to countries on multiple continents for meetings with high-level government officials and to hold public sector summits, all to promote the Framework approach in those countries. Everyone our staff talked to viewed the Framework as a positive step, and expressed interest in understanding how they might be able to use it locally. For example, in a meeting in one country, we were handed a set of security recommendations an agency planned to publish as guidance for that country's critical infrastructure (CI) community. The agency representatives pointed out they had read and comprehended the Framework, and incorporated concepts from the Framework into their own guidelines. In high-level government meetings in a second country, we discovered while few officials had yet to read the Framework text, they were aware of it and had a great deal of interest in learning more about the Framework. After in-depth discussions regarding the Framework, each of the officials expressed interest in how the Framework was developed, plans for future efforts to improve it, the proposed usage of the Framework, and how representatives from their country might become involved in future Framework development efforts.

***8. Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?***

Intel and Intel Security have conducted extensive outreach regarding the Framework via numerous bilateral and association meetings with governmental officials, through the media, and at public conferences and seminars, both in the U.S. and abroad. We have participated in webinars and held public sector summits on the Framework and its policy implications. Raising awareness and encouraging best practices, including discussions of the Framework, is an integral and ongoing part of Intel's efforts to foster improvements in global cyber risk management.

***9. What more can and should be done to raise awareness?***

NIST continues to do an excellent job in raising awareness of the Framework by holding developmental workshops, such as the upcoming event in Tampa, and the external outreach that NIST representatives have conducted. However, there appears to be a lack of coordination between the outreach efforts of NIST and the Department of Homeland Security (DHS). We believe the overall Framework outreach effort would benefit from tighter alignment between the two organizations and synchronization of their efforts.

Additionally, NIST should reach out globally to other governments and offer to assist them in understanding the Framework and its approach, while encouraging them to participate in the future Framework development. It may be beneficial to find a country willing to host a Cybersecurity Framework development workshop, focused on education and international alignment with the Framework, as was done during the initial geographically-distributed Framework development here in the U.S.

## Section 2: Experiences with the Cybersecurity Framework

*NIST is seeking information on the experiences with, including but not limited to early implementation and usage of, the Framework throughout the Nation's critical infrastructure. NIST seeks information from and about organizations that have had direct experience with the Framework. Please provide information related to the following:*

***1. Has the Framework helped organizations understand the importance of managing cyber risk?***

Intel has long recognized the importance of managing cybersecurity risk and supports many efforts worldwide to improve the security of the Internet. We welcome the positive impact the Framework will have on underscoring and supporting improved cybersecurity throughout the global ecosystem.

***2. Which sectors and organizations are actively planning to, or already are, using the Framework, and how?***

Intel has been an active supporter of the Framework since first proposed, and we began a pilot project to utilize it internally shortly after Framework 1.0 was published earlier this year. Industry associations and other stakeholders are better positioned to answer the question of which sectors and organizations are using the Framework.

***3. What benefits have been realized by early experiences with the Framework?***

Even in our initial experiences with the Framework we have recognized a number of benefits to utilizing the Framework, including some that were unexpected pleasant surprises. These benefits include:

- Improved harmonization of risk methodology and language – The Framework has been effective in enabling a common risk management methodology and language across internal stakeholder communities.
- Low Cost to Implement – The Framework aligned well with Intel's existing risk management process. Because the Framework is based on existing industry practices, the Tiers, Core elements, and common vocabulary were easy for stakeholders across the enterprise to learn and use and facilitated uniform, accurate and rapid assessments across disparate domains of risk. To date, the development of tools, training of stakeholders, and utilization of the Framework has been accomplished at a relatively low cost. In addition, to reduce overhead, our approach has been to embed the Framework over time into existing governance and prioritization processes.
- Improved Visibility into Risk Landscape – We have also realized benefits we had not anticipated. For example, mapping assessments of common Core items by various subject matter experts (SME's) in a single risk "heat map" enabled quick identification of outliers, significant variances, and visibility issues. Highlighting these issues led to additional discussion and assessment, allowing us to further improve visibility into our risk landscape. By similarly mapping results from various business units we anticipate being able to visualize certain organizational trends and groupings regarding our risk landscape. Gaining the benefit of these new insights would not have come nearly as easily without a unifying mechanism like the Framework.
- Enabled Risk Tolerance Discussions among Decision Makers - One of the most important and valuable benefits of the Framework was spurred by the internal discussions it helped foster. The Target versus Actual discussions were especially helpful, as they encouraged participants to discuss and compare strategies across domains as they relate to our enterprise risk goals. They also helped facilitate agreement between stakeholders and leadership on risk appetite and other strategic issues, understandings which in turn can guide the organization in security project prioritization and funding. The Target versus Actual discussions yielded one of the most valuable benefits we realized as a result of our use of the Framework - the resulting alignment across the organization on risks and priorities. For this reason, we strongly advise against an organization using Tier Targets established by outside agencies or third parties, as pre-fabricated targets would likely pre-empt the relevant and necessary internal organizational dialogue regarding risk and prioritization that we found so valuable.

***4. What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?***

We have detailed the most helpful aspects in our answer to Question 3 above, especially the benefits realized as a result of internal discussions fostered by working with the Framework. To date, we have not found any aspects included in the current Framework *un*helpful.

A few issues surfaced we believe should be addressed in supporting materials or the next revision of the Framework itself.

- Sub-Categories – In an agile approach to initial utilization, our pilot assessment and target-setting primarily focused on use of the Categories. The Subcategories were referred to only occasionally to clarify the exact scope of the parent Category, and to provide detail on particular subcategories that may have impacted scoring. However, most of the supporting materials and guidance for the Framework are aimed at using the Subcategories, with the parent Categories used only as the reference. In our view, supporting materials and guidance for both Category and Sub-Category-focused approaches should be developed. In addition, it would be helpful to provide examples of how to balance the need to identify risk at the granularity of the sub-category with a light weight "heat map" approach. Our pilot approach examines Target and Actual scoring at the category level while using the sub-category detail to isolate areas of over-and-under investment. We suggest NIST provide additional use cases that demonstrate the various ways an organization can apply the framework.
- Threat Assessment – Additional guidance on the role and use of threat assessments during the setting of Tier Targets is needed. The topic of threats and threat assessments came up many times during discussions with stakeholders, and we believe developing clearer and more thorough guidance on this topic as well as possible use case examples would be helpful.
- Use Cases – Additional use cases, examples and case studies are needed throughout the Framework, including variations for organizations of various sizes and security resource levels.

***5. Do organizations in some sectors require some type of sector specific guidance prior to use?***

The Framework is appropriately organization-focused, and thus able to account for disparities amongst organizations' size, resources, and risk-profiles. While organizations within a given sector may share common characteristics, in our view there will likely always be disparities between how different organizations, even those in the same sector, may choose to utilize the Framework. Accordingly, while voluntary sector-specific guidance may prove useful for some—particularly those organizations first learning to use the Framework—we advise against requiring such guidance. As we have stated in previous Framework submissions, we do not endorse neither prescriptive nor one-size-fits-all solutions for improving cybersecurity.

***6. Have organizations that are using the Framework integrated it with their broader enterprise risk management program?***

For Intel, the answer is yes. We are currently piloting a program to align our enterprise cybersecurity management to the Framework. Additionally, as various internal risk management and governance processes start or reach appropriate milestones, we are introducing Framework concepts and integrating applicable portions into these processes. We have made these alignments without negative impacts to existing project planning or roadmaps. We expect that over time the balance of our security programs and projects will have substantially aligned their risk management processes to the Framework.

We have found adopting the Framework approach in areas with strong cyber risk management practices and cultures incurs very low program management overhead. In those cases, utilization was light-weight organizationally, as it leveraged existing processes and organizational structures. We have

invested less than 150 total work-hours (in a multinational company with 100K+ employees) at about the halfway point of our enterprise-wide pilot. Along the way, we have developed a small set of tools, light-weight processes, and training aids for better process repeatability, so future efforts may require even less overhead.

***7. Is the Framework's approach of major components—Core, Profile, and Implementation Tiers—reasonable and helpful?***

From our perspective, yes. As we have detailed in other sections, we have applied the Framework components successfully in various business units and at several scales, adjusting it easily as needed for unique requirements. Our experience demonstrates the Framework components are comprehensive, flexible and extensible.

***8. Section 3.0 of the Framework ("How to Use the Framework") presents a variety of ways in which organizations can use the Framework.***

***a. Of these recommended practices, how are organizations initially using the Framework?***

Before studying Section 3.0, we created our own process based on our experience with risk management, as we wanted to ensure our process comprehended our specific environment. Later, in comparing our process to Section 3.0, we found our process was quite similar with a few minor variations, for example, instances where a few steps were combined or executed in a slightly different order.

***b. Are organizations using the Framework in other ways that should be highlighted in supporting material or in future versions of the Framework?***

Based on our initial experiences with the Framework, we recommend NIST add these items to the supporting materials:

- Considerations for tailoring the steps in Section 3 to organizational capabilities.
- Considerations for tailoring the Categories and Subcategories to the organizational environment.
- Expanding the definitions of the Tiers, with additional detail and usage notes.

***c. Are organizations leveraging Section 3.5 of the Framework ("Methodology to Protect Privacy and Civil Liberties") and, if so, what are their initial experiences? If organizations are not leveraging this methodology, why not?***

NIST incorporated the privacy methodology in Section 3.5 as part of the Framework Core (rather than in an Appendix) to make it clear that organizations using the Framework should consider the potential impacts of their cybersecurity activities on individual privacy and civil liberties throughout their cybersecurity risk management practices. Intel has long integrated our security and privacy risk-management functions, and accordingly we did not need to leverage the Section 3.5 approach because it was already consistent with our existing security and privacy risk management practices.

***d. Are organizations changing their cybersecurity governance as a result of the Framework?***

Intel's relatively mature risk management practices predate the Framework. Indeed, the Framework incorporates the risk management approach and many of the consensus industry standards, best

practices, and guidance identified by Intel and other stakeholders during the Framework development process. Therefore, it should not come as a surprise we are not dramatically changing our practices as a result of using the Framework. However, as noted previously, the structure and common vocabulary established by the Framework have been very useful in aligning practices used by various business units and technology domains across our enterprise. Additionally, we are simultaneously engaging our governance, risk management and compliance (GRC) program to further our efforts to align with the Framework.

***e. Are organizations using the Framework to communicate information about their cybersecurity risk management programs—including the effectiveness of those programs—to stakeholders, including boards, investors, auditors, and insurers?***

We are currently using the Framework to communicate risk information to immediate stakeholders such as practitioners and managers. Eventually, we anticipate using the Framework to communicate to all relevant stakeholders eventually. However, the methods and characterizations needed to do that – for example, a straightforward means by which to digest and visualize often complex results for varied stakeholder groups - have yet to be determined and will require further detailed study.

***f. Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties?***

We are not using the Framework in this way at this time but we are exploring how to do so in the future. We believe the ability to express cybersecurity requirements in alignment with a common language and structure to a variety of third parties is an important benefit of the Framework, one that can potentially prove valuable across our ecosystem.

***9. Which activities by NIST, the Department of Commerce overall (including the Patent and Trademark Office (PTO); National Telecommunications and Information Administration (NTIA); and the Internet Policy Taskforce (IPTF)) or other departments and agencies could be expanded or initiated to promote implementation of the Framework?***

We recommend NIST initiate and support communities of interest (CoIs) in which best practices, discoveries, tools and resources are shared among participants. We also recommend NIST organize CoIs around levels of expertise as well as technology. Additionally, in areas where administrative or agency interfaces with industry already exist, NIST should leverage those existing structures and programs wherever possible, rather than creating new ones. For example, many small and medium sized businesses already have established relationships with the Small Business Administration (SBA), and are familiar with the services SBA provides and how to access them.

***10. Have organizations developed practices to assist in use of the Framework?***

Based on our experiences with our pilot program, we developed a small set of tools, light-weight processes, and training material to aid our internal efforts to utilize the Framework. These tools include a risk scoring worksheet and "heat map," customized Tier descriptions describing maturity as dimensions of people, process, technology and ecosystem engagement, and training material for assessors and facilitators.

## Section 3: Roadmap for the Future of the Cybersecurity Framework

*NIST published a Roadmap in February 2014 detailing some issues and challenges that should be addressed in order to improve future versions of the Framework. Information is sought to answer the following questions:*

1. ***Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?***

The Framework Roadmap identifies many important cybersecurity issues. However, not all of these issues and challenges should be directly addressed in the Cybersecurity Framework itself. Areas such as Authentication and developing the informative references required for International Alignment may potentially be addressed in future versions of the Framework. Automated Indicator Sharing may also emerge as a valuable component for Framework inclusion in the future, but a great deal of work needs to be done outside of the Framework process before this area is sufficiently mature to incorporate elements into the Framework.

In our opinion, other areas identified in the Roadmap are more appropriately addressed outside of the Framework. For example, Federal Agency Cybersecurity Alignment is an important area where we need to make progress but should not be incorporated into the Framework itself. Conformity Assessment and Cybersecurity Workforce are two other areas where work is certainly needed, but more appropriately undertaken outside of the Framework improvement efforts.

Elements of other identified Roadmap areas may eventually be ripe for inclusion in future versions of the Framework, but are sufficiently complex and underdeveloped that NIST and other stakeholders would be better served by driving the foundational work needed to address these challenges outside of the Framework context. Supply Chain Risk Management (SCRM), for instance, presents a broad cybersecurity challenge worthy of our collective attention – but SCRM is a complex global policy challenge around which there is currently little consensus regarding approach, best practices or standards development. Technical Privacy Standards is another area where the prerequisite foundational work to develop standards is just beginning – this work should be allowed to develop outside the Framework, with NIST and other stakeholders working with international standards bodies to increase the likelihood of international adoption.

Finally, Data Analytics as described in the Roadmap is too broadly defined, and tackling this challenge will require a long-term research effort. We recommend, for example, that work be undertaken to evaluate how to utilize big data as an integrated part of an overall situational awareness program while accommodating privacy interests, but caution against prescriptive solutions of any sort. We recommend future versions of the Roadmap provide a clearer distinction between Framework development areas and cybersecurity process/program areas.

2. ***Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?***

Yes. An additional priority area the Framework should comprehend is the cyber threat intelligence lifecycle. While automated indicator sharing is listed, that is just the mechanism by which intelligence can be shared. Cyber threat intelligence is a much broader discipline, essential to a robust cybersecurity risk management program, and needs attention in the Framework. For example, it is

critical we have a robust understanding of relevant threat agents/actors, their tactics, techniques and procedures, incidents, campaigns, and other threat aspects to best prepare for and respond to cybersecurity attacks. Incident handling and vulnerability management are also essential pieces of cybersecurity risk management and warrant consideration for inclusion in future versions of the Framework.

3. ***Have there been significant developments—in the United States or elsewhere—in any of these areas since the Roadmap was published that NIST should be aware of and take into account as it works to advance the usefulness of the Framework?***

We are unaware of any significant developments since the Roadmap was published.

Thank you again for the opportunity to share some of our outreach efforts regarding and initial experiences with the Cybersecurity Framework, as well as our thoughts on how to address the Roadmap issues. While we believe the responses NIST receives to this RFI will likely demonstrate broad Framework awareness and a diversity of experiences regarding organizations' initial experiences in using the Framework, we again urge NIST and other stakeholders to view the responses from a perspective that acknowledges the Framework's unquestionable youth. We also encourage continued Framework outreach by NIST and other stakeholders, particularly internationally, where we have observed a strong and growing interest by the governments in multiple countries. We look forward to continuing to partner with NIST to help Cybersecurity Framework 1.0 gain traction in the U.S. and internationally, and to participating in the creation of future versions, as well as the ongoing governance of the Framework.

Best Regards,

Peter M. Cleveland
Vice President, Legal and Corporate Affairs
Director, Global Public Policy