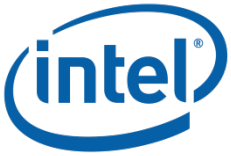

February 18, 2016

Via e-mail to cyberframework@nist.gov

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

Re: Intel comments in response to NIST's Solicitation for Comments on 'Views on the Framework for Improving Critical Infrastructure Cybersecurity'

Intel Corporation appreciates the opportunity to respond to the National Institute of Standards and Technology (NIST) Solicitation for Comments on the Views on the Framework for Improving Critical Infrastructure Cybersecurity noticed on December 11, 2015. Intel has been an active participant along side NIST during the initial development of the Cybersecurity Framework (from here on known as the 'Framework'). We also were one of the 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.* Intel is committed to improving the global security ecosystem and as such has been demonstrating that support by our global outreach in support of the Framework.

We preface our responses to the specific RFI questions with this 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 gauge Framework progress.

- **As an industry, we are at the preliminary stages of Framework understanding.** As more and more organizations implement the Framework, we are learning where the Framework is valuable and where it needs work. Currently the Framework is at version 1.0. Organizations are learning how to integrate the Framework into their existing risk management processes and as such the valuable lessons learned need to be shared. We have also learned where there are pieces missing from the Framework. Today security programs need to understand the threats, both external and internal, to their organization. The Framework needs to incorporate threat lifecycle categories and subcategories into the Framework Core. Additionally, we believe modifications are needed to the Tier definitions in order for an organization to properly evaluate itself. Intel modified the Tier definitions adding Ecosystem, which includes collaboration on cybersecurity issues and participation in information sharing. We believe these are equally essential to a modern corporate security program. Important organizational and

governance issues, not included in the core model, are now included in this new Tier element.

- **NIST's Improvement Roadmap identifies several important focus areas – but not all of them may be appropriate or ripe for inclusion in future versions of the Framework itself.** NIST's Roadmap identifies many important areas of important 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, 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, such as the Technical Privacy Standards, where the prerequisite foundational work to develop standards is in the early stages. 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.
- **Awareness appears significant and broad-based.** Other stakeholders, such as industry associations, are better positioned than Intel to comment on what appears to be significant awareness across the diverse stakeholders in the U.S. However, one aspect of awareness Intel observed first-hand is the growing international interest in the Framework. Accordingly, we 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 it gain traction among international government and industry partners.
- **International participation is needed as Framework 2.0 development occurs.** As is well known, cybersecurity is not simply a U.S. problem. It is a global problem. As such, while the Framework was initially developed in the U.S., it is now very important for the next version of 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. In the initial development of the Framework, NIST had development workshops in different parts of the U.S. to allow local owner / operators the opportunity to actively participate in the efforts. This approach was well-received by all and allowed for a much more robust dialog. The extent of the input would not have happened had the development been limited to the Washington D.C. area. Intel believes NIST should consider having at least one and possibly more development workshops outside the U.S. so as to allow global partners a better chance to participate and add real value to what becomes the Cybersecurity Framework version 2.0.

- **We do not believe there should be a rush to external Framework governance.** As already mentioned, there has been only one release of the Framework to date. Industry and the U.S. government are still working to incorporate the Framework into their existing risk management processes. We are just now learning about what works and what doesn't and where additions and improvements are needed, and therefore we believe this is not the time to consider moving the Framework from NIST's oversight. We need to ensure we can incorporate community input into a subsequent version of the Framework before seriously considering a transition to some external organization. The Framework and its related integration into the U.S. cybersecurity landscape should be mature before non-NIST governance of the Framework is considered.

Please find Intel's responses to the specific questions in the RFI below. Our responses track the manner in which the questions were presented in the RFI: Use of the Framework (Questions 1-9); Possible Framework updates (Questions 10-15); Sharing information on using the Framework (Questions 16-19); and Private Sector Involvement in the Future Governance of the Framework (Questions 20-25). We have attempted to provide a substantive and helpful response to all the questions asked.

Use of the Framework:

1. Describe your organization and its interest in the Framework.

Through computing innovation, Intel pushes the boundaries of smart and connected technology to make amazing experiences possible for every person on Earth. From powering the latest devices and the cloud we all depend on, to driving policy, diversity, sustainability, and education, Intel creates value for our stockholders, customers and society.

Security has long been an Intel priority. Security, along with power-efficient performance and connectivity comprise the three computing pillars around which Intel concentrates its innovation efforts. In early 2014, Intel formed the Intel Security Group, a new business unit to further the security pillar. This business unit combined our subsidiary McAfee with all other security resources within Intel, forming 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 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. We also work collaboratively with government, industry, and non-governmental organization 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.

2. **Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.**

   Intel was one of the very early adopters of the Framework. We are responding from a position of piloting and our use of the Framework. Initially, McAfee and Intel responded to and participated in the Framework development as two separate organizations. Since then, McAfee has been fully integrated into Intel Corporation as the Intel Security Group. We are responding today as one organization that both have used the Framework and produces security related products to assist in implementing the Framework.

3. **If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).**

   Intel has used the Framework at a macro and micro level for risk management. At the macro level, Intel has utilized the Framework to examine risk for our office and enterprise compute environments. At a micro level Intel has utilized the Framework to manage risk for specific IT services, capabilities and infrastructure. Intel has also encouraged its suppliers to align with the Framework.

4. **What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?**

   Intel has had a positive experience with the flexible nature of the Framework. Intel's use of custom tier definitions which aligned with our internal risk management language and business processes helped with ease of use. We have found the Core Functions and Categories align well with our current risk management practices.

5. **What portions of the Framework are most useful?**

   Intel has found the Core Functions and Categories align closely with our existing risk management practices easing the alignment of language and implementation in our use cases. In addition, for the standard office compute environment, we found the existing Sub-Categories to be somewhat useful. By taking a flexible approach to the Framework, Intel was able to reduce the overhead needed to align to our existing practices and processes.

6. **What portions of the Framework are least useful?**

   At a macro-level for facilitating the risk tolerance discussion, we found the Subcategories to

be least useful. We found the Subcategories easier to use if we structured them as we internally managed the capability. The alignment with our internal processes allowed for SMEs and risk management personnel to more easily self score current state and discuss target or "to be" future states.

We also believe there should be a more robust consideration of the threat component of the risk defined in the Framework. There is opportunity at a minimum, at the category level to address threat intelligence and threat management. Also, the accompanying documentation should explain more robustly how to address the threat landscape when using the Framework.

The Tiers construct itself is useful as a way to both encourage discussion about what level the organization should operate for each assessed item, and to compare that to its actual status. However, the Tiers assessment model currently provided is essentially a maturity model. While maturity models are very useful for assessing a capability at a macro level, they have much less applicability at the lower, more atomic levels of the Framework because of the differences in the way the individual components are implemented along with their interdependence. Consequently, much interpretation and variability results from trying to apply the current Tiers model, limiting the clarity of the resulting risk landscape. We outline some ideas for alternate Tiers models in the "Possible Framework Updates" section.

7. **Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?**

Our initial pilot of the Framework examined risk for our office and enterprise environments. In addition, we have tested the Framework against specific services and components of our infrastructure to perform more micro-level assessments and have found utility there for the Framework. We expect a heavier lift when expanding the Framework to examine risks in our design and manufacturing compute environments due to the complexities and uniqueness of that infrastructure. As community pathfinding efforts expand to those types, we hope to leverage those experiences.

8. **To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.**

It is much too early to be able to cite metrics and we believe it is not yet possible to report on the right things. The Framework is targeted as a tool for improving the visibility, communication and overall posture of an organization's security program. In our case the initial implementation of the Framework has given us perceived positive results. The Framework has helped us identify both strengths and opportunities to improve; sparked in-depth and better-informed risk tolerance discussions; harmonized risk management language across the enterprise; provided improved visibility into Intel's risk landscape, and allowed us to better set security priorities, develop capital and operational expenditure budgets.

Improving a large organization's overall security program does not happen overnight but the Framework has facilitated our path-to-improvement. A single year or two worth of data is not enough to accurately report reductions in risk.

9. **What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?**

One of the benefits of a structure such as laid out in the Cybersecurity Framework is the ability to map specific items to the Core subcategories. Each of the Subcategories have Informative References which provide a means for potentially linking specific regulatory items to aspects of the Framework. If each regulatory agency was to initiate a project to map their regulations to the Framework, they would be able to see which are duplicative, unique or do not map at all. While some regulations or their implementation items may not map directly, there will be many that will. Those that do will allow agencies to be able to compare their results and provide a potential means for identifying duplication. At that point the specific actions taken will have to be pursuant to the Cybersecurity Enhancement Act of 2014.

Possible Framework updates:

10. **Should the Framework be updated? Why or why not?**

We believe the Framework should be updated. In our uses of it we found various areas that need to be added / updated. First there should be more 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.

The Framework Implementation Tiers needs to be examined to assure the definitions used to describe the Tiers are complete for evaluating an organization's degree of sophistication as it relates to their security organization. At Intel we augmented the definitions of the Tiers with a new element, Ecosystem. We believe this is an essential gauge for more accurately determining the level of rigor for an organization. Understanding an organization's role in the larger ecosystem, including the level of cooperation and information sharing, is critical in a modern corporate security program and as such should be evaluated against as well.

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 threats they face each day if they are going to be able to properly protect themselves and their assets. As the Framework is a risk-based framework, it is critical it include threat aspects integrated into the Core so the organization can properly evaluate themselves.

Additionally, we need to review and develop a means to enhance the Framework, assuring we can extend it in the future so publically approved extensions, such as industry focused or missing pieces can be incorporated without negatively impacting the existing version of the Framework.

11. What portions of the Framework (if any) should be changed or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.

As stated above, the Tiers construct is helpful to Framework users, but the current model does not facilitate fully accurate risk assessments. Additionally, it has become apparent that different organizations and even industries may need to consider alternate risk assessment models. We propose here several different approaches industry and NIST may consider for development and inclusion as additions to the current Tiers model.

- Explicit declaration of risk tolerance. The current model asks the assessor to judge the level of preparedness needed to meet the organizations goals. However, hidden in that assessment is an essential understanding of the organization's tolerance of risk for that item. To set the preparedness level, an assessor must first understand—or more likely guess at—that tolerance. That hides the core aspect of the assessment and introduces other interpretations that may obscure the real issues. An alternate model would address that core consideration directly by stating the grading scale in terms of risk tolerance. That scale would range from "Highly tolerant of risk" (1) to "Very little risk tolerance" (4). The guidance would reverse the current interpretation, by recommending grading the actual status of risk tolerance as evidenced by the level of resources and capability for that item.
- Attacker capability model. A model several industry Framework participants are already using describes Tier levels in terms of an *attacker's* capability, and the level to which the organization needs to protect itself for each item. For example, the grading scale could range from "novice" (1) to "highly advanced threat" (4). Guidance describes details about the hypothetical attacker's capability at each level, and what is needed to protect against them. This approach also directly addresses the organization's concerns about risk in and impact to each item as described in the preceding example.
- Limit Tiers to the Framework Category level. Current Framework guidance implies the Tiers construct can be, or even should be, applied at the Subcategory level. However, as discussed previously, this could introduce a significant margin of error. Instead, the Framework guidance could explicitly recommend assessment only at the Category level, but also leveraging the Subcategories as both a means to understand the scope of each Category and to assess it comprehensively. This approach strikes a balance between the utility of a maturity model at the top level vs. the granularity needed for a comprehensive risk picture. This approach was used successfully by Intel in our initial

pilot of the Framework.

12. **Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?**

Maybe it is not so much specific recommendations to be made here by industry as it is describing the potential means for 'official' mappings to be done. Today the Framework Core, which includes the mapped informative references, are one document; one integrated whole. If the Framework Core was separated into its own versioned document then categories, subcategories and informative references could be added without changing the Framework process document. This would allow NIST to make additive, incremental improvements allowing organizations to benefit and not be impacted. There will always be additional updates needed. Just supplying a list of standards, guidelines and practices will require we sync the changes with new / future releases of the Framework. This will cause many to wait much longer than necessary. By developing a means for updating the Core, then changes can be made to the Framework Core without negatively affecting how people use the Framework process.

13. **Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?**

During Intel's pilot use of the Framework we intentionally separated those individuals that participated in the Corporate Target Profile creation from the actual Assessment team. We did this so we did not bias the SMEs in what we were expecting to achieve. The Assessment team was not aware of the target profile until the results were compiled. We believe this approach was essential to the integrity of the processes. We feel this approach needs to be documented in the Framework process itself.

14. **Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?**

The nine areas specified in the Roadmap are of differing focuses. Certain areas have direct applicability to improving the Framework itself while others are more focused on using the Framework to align Federal or International uses or improve other NIST initiatives. The use of the Roadmap, at the time it was published, seemed more of a tool for NIST's use as they moved forward with version 1.0. There are areas that seem to directly apply such as Authentication and Automated Indicator Sharing. The Roadmap does identify areas needing to be addressed. Items directly affecting the improvement of an organization's security program should be included. In all areas there may be informative references that could be included in the Framework. Roadmap efforts such as Supply Chain Risk Management, Data Analytics and Technical Privacy Standards are going to be ongoing efforts that require

development outside of the Framework itself. If in the future, there are aspects that intersect with the Framework then those aspects should be included.

15. **What is the best way to update the Framework while minimizing disruption for those currently using the Framework?**

Today the Core is a part of the actual versioned document. If the Core was published as a separate but required document, then both the Framework Core could be extended with new Informative Reference and Categories without changing the process document. The two could be improved and versioned independently if desired.

However, updating the Framework should not disrupt those currently using it since most of what we are considering doing to improve the Framework would be additive to the existing structure. Organizations will incorporate newer changes as needed by integrating them with their existing risk management processes.

If there were going to be radical changes to the Framework's process and structure, then all will be affected.

Sharing information on using the Framework:

16. **Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?**

Our work to-date has been original work. We used the Framework as a framework and modified it as appropriate to more easily integrate it into our existing risk management processes. We have contributed to the resources NIST has made available in the form of our Use Case whitepaper. Intel was one of the first organizations to really come out in support of the Framework as a result of our piloting it. We accomplished our pilot while working with NIST staff to assure we were making the Intel modifications in accordance with the spirit of the Framework. The time NIST spent answering our questions and listening to our concerns was highly useful and greatly appreciated.

17. **What, if anything, is inhibiting the sharing of best practices?**

Best practices may be the wrong term. As we are developing implementation processes, tools and guidance, it really is about lessons learned. We have learned a reasonable amount about the Framework and how to apply it. It is those stumbling blocks, missing pieces, things that worked well and things that didn't, tools that were needed and looking at how to integrate the Framework's process into the organization's existing risk management processes that need to be shared. We tried to do just that by publishing our whitepaper, ***The Cybersecurity Framework in Action: An Intel Use Case***. We felt we could contribute to others better understanding of the Framework by documenting our piloting of it.

There needs to be a means for organizations to easily share their experiences. The NIST Industry Resources page linked off the NIST Cybersecurity Framework Home page is a great start in that it is a single page where those interested in learning can go to get more information. More emphasis on producing use cases and lessons learned documents should be made clear as the Framework moves forward.

In addition, there are opportunities to promote or accelerate alignment to the Framework. One such opportunity could be in driving the development of foundational tools such as contract language guidance for alignment to the Framework. Another opportunity would be to foster alignment by GRC Vendors in offering Framework-related capabilities. Areas such as SCADA and ICS system security could also benefit from pathfinding efforts to utilize the Framework to manage risk.

18. **What steps could the U.S. government take to increase sharing of best practices?**

While the question may be targeted towards what the U.S. government can do to help industry in sharing best practices, there is a different area where the U.S. government could be very beneficial in helping the global spread of the Framework.

During Intel's global travels and corporate outreach on behalf of the Framework, we have seen a great deal of interest in the Framework from other governments. These governments have done their research and indicated they feel the Framework is something they should encourage their industries to align with.

The U.S. government is actively using the Framework. The U.S. government's efforts to incorporate the Framework into the government's mission and activities should be documented and published. If the U.S. government was to document uses of the Framework within U.S. government agencies and departments, it could be an extremely useful both for reporting to the U.S. legislative branch while providing an informative document for other governments to be able to consider how it could be applied inside their government. The focus would be simple, how and where is the Cybersecurity Framework being used inside the U.S. government, what are some of the lessons learned and pitfalls to avoid. This could help foster more rapid adoption of the Framework within other governments across the globe.

19. **What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?**

NIST was very effective getting industry to meet and discuss openly during the Framework development workshops. It would be beneficial if NIST held a similar set of workshops in differing parts of the country where the focus of the workshops was to have organizations

actively participate in discussions on how they are using the Framework, what their lessons learned during the process. These workshops would provide 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.

There should also be an outreach to trade associations, and other industry consortia to encourage their membership to publish their experiences with the Framework describing how they are using it.

Private Sector Involvement in the Future Governance of the Framework:

20. What should be the private sector's involvement in the future governance of the Framework?

As has occurred in the past, the private sector needs to be intimately involved with the development of the Framework and have an active role in its future. Up until this point, NIST's oversight and has been extremely collaborative with the public sector. So much so that other Federal groups are trying to replicate the developmental model for their projects.

There are some that feel future Framework advancements needs to be done outside of NIST in a private sector organization. We believe it is really too early to decide this. NIST has been very successful in weaving related efforts it has into the Framework. In fact, the Framework, while developed in extremely close coordination with the private sector, is globally referred to as the NIST Cybersecurity Framework. NIST has a positive reputation that proceeds the development of the Framework. It has successfully used that to garner participation during development and usage of the outcome. As a nation, we are just now starting to see real positive response and usage of the Framework. Moving governance to a private sector non-profit would diminish its recognition and stifle its adoption. NIST is recognized globally for the good work it has done in many areas. This is one of them. We need to see more acceptance and adoption globally and within the U.S. business community before we actively consider moving ownership and governance to and outside organization. We believe the Framework should stay under NIST's leadership through at least the next version. NIST's outreach to other governments is vital to global acceptance and adoption and an outside organization would not have that influence or access.

21. Should NIST consider transitioning some or even all of the Framework's coordination to another organization?

At this point we do not believe this would be valuable for the long term success of the effort. It is too early in the development and adoption to consider transitioning coordination to any other organization. A great deal of discussions will need to occur before serious consideration of any specific organization is undertaken.

22. If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers,

Informative References, methodologies)?

The Framework is useful because it is a relatively simple process for an organization to implement. Taking it and parting it out would destroy its value. If transitioning must occur, all of it must be transitioned at the same time.

23. If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?

Can an organization be identified that has the respect, brand and financial where-with-all to continue to support the Framework development, it's adoption efforts and global outreach? Today the Framework is respected because of the process of development, the overseeing organization (NIST) and the outreach efforts that have occurred on its behalf. If the Framework was to be transitioned, it would need to be to a not-for-profit so it was not seen as a hook for corporate revenue. We do not believe at this time, however, the Framework would thrive and grow outside of NIST.

24. How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?

While much of this is conjecture, organizations currently using the Framework would probably continue to. The question really is how would future adoption and improvements to the Framework be seen by those currently using it and those considering its use. If there was a transition (and we hope that is not the case at this time), NIST would need to be seen as a complete partner to the organization the Framework was being transitioned to. A direct handover without NIST's involvement would be disastrous to the future of the Framework. NIST would need to continue outreach efforts on behalf of the new organization and work with the leadership of the new governing body to assure proper global contacts are made so as to continue the progress towards global adoption we have seen occurring under NIST's leadership.

25. What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?

There are many factors that need to be examined and questions that need to be answered. Below are but a few.

- Has the organization any **true** experience with successful, highly collaborative efforts?

- Is the target organization a non-profit where conflicts of interest are not possible or perceived to be possible? Does it have some direct linkage to a for-profit company? If so, is there any conflict of interest here?
- Does the organization currently have the respect and 'brand' that would encourage active participation of the private sector going forward?
- Is the organization currently recognized globally?
- Does the organization have the funding and continuing revenue stream to be successful long term?
- Will the organization be able to do national and global outreach to continue to attract use and participation in improving the Framework?
- Does the organization have experience in cybersecurity and risk management related areas?
- Is the organization a recent startup focused on governance of the Framework?
- Does the organization have existing ties to international standards bodies to assure the alignment with other efforts?

Summary

Thank you again for allowing us the opportunity to provide our comments on the Cybersecurity Framework. Over the last two 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. 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 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 other governments worldwide seeking to address cybersecurity related issues in their countries. Intel looks forward to continuing to partner with NIST as it develops Cybersecurity Framework 2.0.