April 8, 2013

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, "Developing a Framework to Improve 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), "Developing a Framework to Improve Critical Infrastructure Cybersecurity," noticed on February 26, 2013. We were pleased to learn that NIST had been charged by President Obama in the cybersecurity Executive Order (EO)[1] with the central and important role of partnering with industry to develop the Cybersecurity Framework of standards and best practices to reduce cyber risks to critical infrastructure, given NIST's longstanding commitment to working with the private sector and demonstrated cybersecurity expertise. Intel is also appreciative of the fact that staff from NIST and across the administration view the business community as indispensable partners in addressing our cybersecurity challenges, as demonstrated by your serious and continuing engagement with the business community both during the development of the EO, and since it's issuance.

Intel Corporation, along with our subsidiaries McAfee and Wind River, believe that we cannot delay in collectively addressing the evolving cybersecurity threats facing us all, and indeed our company has been at the forefront of efforts to improve cybersecurity across the compute continuum. Over the last decade alone we have invested billions of dollars to develop software, hardware, services and integrated solutions designed to advance cybersecurity across the global digital infrastructure. This infrastructure predominantly operates via interoperable hardware and software products which do not vary significantly for individual countries and are deployed worldwide. As a leading developer and manufacturer of these foundational information and communications technology (ICT) products, we offer a unique understanding of the gravity of our cybersecurity challenges, and the reality that governments, businesses and consumers are facing a cybersecurity threat landscape that has changed fundamentally. Countering these increasingly sophisticated threats to networks, intellectual property,

---

[1] EO 13636, titled *Improving Critical Infrastructure Cybersecurity*, is available at www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (originally released by the White House February 12, 2013); see February 19 *Federal Register*, pp. 11738–11744.

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

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.

There are several key themes running throughout our responses to the specific RFI questions. Taken together, these themes comprise summary guidance we believe should be helpful to NIST as it builds out the Cybersecurity Framework:

- **Dynamic Cybersecurity risks call for flexible and nimble risk management based solutions**. Cybersecurity risk is dynamic—we face a constantly evolving threat landscape, and we must develop best practices to help mitigate those shifting risks. CI/KR (Critical Infrastructure and Key Resources) Owners and Operators from divergent critical infrastructure (CI) sectors will be more apt to utilize a flexible risk management-based Cybersecurity Framework. This Framework allows companies to prioritize and focus on the most serious threats to the most critical assets, systems, and processes based on their particular industries and businesses—there is no "one size fits all" approach or "check-the-box" model that will work for everyone in all circumstances.
- **The Cybersecurity Framework should be technology neutral and not prescriptive.** Building on the approach outlined above, the Cybersecurity Framework should not mandate the acquisition or deployment of particular technologies, technical solutions or tools, nor should it mandate how such technologies are designed or built, or favor one technology or business model over another. Focusing on normative, business process, and risk management processes rather than prescriptive technology solutions will preserve the flexibility CI owner/operators need to deploy, and update, innovative security measures tailored to the specific and evolving threats they face.
- **There is no need to reinvent the wheel—the Framework should leverage existing global cybersecurity standards and best practices.** The Framework should be built upon existing voluntary and consensus based cybersecurity standards and best practices, as called for by the EO. There is no shortage of such existing standards and best practices—we are aware of hundreds. One of the goals of the Framework should be to spread foundational security standards and best practices out more broadly across the CI/KR community.
- **International alignment and harmonization.** Many CI community members are global companies delivering products and services around the word. The Cybersecurity Framework should align with global standards and best practices, and one of our collective goals should be to develop a Framework that can be used globally, adopted by global commercial providers, as well as in other countries.
- **Cybersecurity is a shared responsibility, but industry should lead.** Private industry is already conducting a significant amount of work around best practices via consortia and other arrangements. The existing partnership model as outlined in the U.S. National Infrastructure Protection Plan (NIPP) can be more effectively utilized to leverage this ongoing work to create a true partnership with the CI community to develop and maintain the Framework.
- **Security is a process, not an end state**. The Framework must support delivery of the business capability of organizational security, allowing businesses to dynamically assess and apply security measures and solutions as appropriate to address risks. Focusing on desired security outcomes affords CI owners/operators the needed flexibility to prioritize to manage risks to achieve a baseline level of security.
- **Continuous improvement of best practices.** The Framework should establish an ongoing process to allow for updating so as to continuously adapt the best practices to keep pace with evolving and accelerating threats.

- **The Framework Should Comprehend Global Privacy and Civil Rights Practices**. The framework NIST develops must comprehend privacy and civil rights not from a U.S. standpoint but rather from a global viewpoint, based on internationally recognized Fair Information Practice Principles (FIPPS), that contemplates the multinational operations of many companies.
- **Cross-sector harmonization.** Identifying commonalities in the various risk management frameworks across different sectors will be challenging, but attempting to harmonize these standards and best practices at a baseline level can help produce a security responsive framework to improve cybersecurity across CI.
- **Accessibility of Cybersecurity Framework language to implementing businesses**. Because the Framework will be implemented by private sector businesses, the Framework will be most effective if it is written in a manner and language accessible to business leaders as well as security practitioners. NIST might find that the most efficient and effective way to communicate the Cybersecurity Framework to a wide audience is to adhere to the Federal Plain Language Guidelines.[2]

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: Section I provides responses regarding Current Risk Management Practices; Section II, Use of Frameworks, Standards, Guidelines and Best Practices; Section III, Specific Industry Practices. We have attempted to answer all questions to which we believed Intel could provide a meaningful substantive and helpful response.

[2] *See* Federal Plain Language Guidelines, Revised May 2011, at http://www.plainlanguage.gov/howto/guidelines/FederalPLGuidelines/FederalPLGuidelines.pdf

Section 1: Questions Regarding Cybersecurity Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

There are many challenges to the creation, improvement and adoption of cybersecurity practices across the critical infrastructure community. Among those challenges are identifying and creating flexible and agile cybersecurity practices, efficiently using resources to create and maintain the practices, and improving adoption rates of the cybersecurity practices across the CI community.

Creating Flexible and Agile Practices—Cybersecurity risk is dynamic. We face a constantly evolving threat landscape and we must continuously develop and refine best practices to mitigate these shifting risks. It is important to note that best practices don't change the risk picture – best practices help companies manage risk. Because the threats are not only changing but accelerating, cybersecurity practices must constantly evolve to keep pace. By utilizing flexible and agile risk management frameworks, companies can prioritize and focus on the most serious threats to the most critical assets, systems, and processes based on their particular industries and businesses. Cybersecurity risks may vary by sector and by companies within a sector, so it will be challenging to identify guidelines that balance the specificity to be useful to a particular sector with the flexibility to support a majority of the critical infrastructure / key resource (CI/KR) community. An additional challenge will be to ensure cybersecurity practices keep pace with changing technology and threat landscapes. NIST should engage with technology developers and early adopters to develop best practices that are useful and timely.

Working Smart—Efforts toward improving cybersecurity practices for the CI/KR community should engage a wide range of stakeholders from across the Industry Sectors as well as government partners. Effective management of this large stakeholder community will be challenging, particularly while trying to efficiently leverage existing work and identify new opportunities. NIST should continue utilizing existing Private Sector engagement relationships described in the U.S. National Infrastructure Protection Plan (NIPP) to partner with the CI/KR community in developing and maintaining the framework of best practices. In addition, a great deal of existing cybersecurity work has been done or is in progress within the many industry affinity groups. One example of industry affinity group work is the Common Vulnerability Reporting Framework developed by the International Consortium for Advancement of Security on the Internet (ICASI: www.icasi.org) and other industry collaborators. NIST should invest resources in understanding and leveraging the landscape of cybersecurity practices-related work within existing CI/KR affinity groups such as ICASI. Leveraging this existing work will quickly identify common needs, reduce duplicate efforts, and maximize the opportunity for harmonization of standards and best practices, both within each sector and between them.

Improving Adoption Rates—Cybersecurity practices are only effective if they are adopted and implemented by the CI/KR community. Awareness of the threat landscape is vital to driving adoption of best practices. Improving Public Private Partnership information sharing mechanisms to provide the CI/KR community with timely and actionable threat intelligence will enable the

community to accurately prioritize adoption and implementation of cybersecurity practices. An informed community will drive improved adoption rates of current best practices as well as generate demand for improved or new best practices. Many CI/KR companies operate within the highly interconnected global digital infrastructure and marketplace. To improve ease of adoption and implementation, cybersecurity standards and best practices should align with international standards and best practices to the extent practical. As previously noted, the technology and cyber threat landscape is constantly evolving and therefore cybersecurity best practices should have a robust continuous improvement loop. This allows practitioners to continually update existing practices and develop new practices based on new or emerging risks. Maintaining an up-to-date and relevant suite of best practices useful to a wide range of the CI/KR community will be vital to improving adoption rates of these practices.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

The cybersecurity risk and threat landscape is constantly evolving, and best practices must keep pace to mitigate these shifting risks. A flexible and nimble risk management framework enables CI/KR companies to prioritize and focus on the most serious risks affecting the most critical assets, systems, and processes based on their particular industries and businesses. Identification of common risks and technology solutions is a cornerstone in the development of a flexible risk management framework useful to CI/KR companies across many sectors.

However, developing cross-sector standards may be challenging due to the complexity in identifying cross-sector commonalities in technology or implementation of technology. For example, implementation of a SCADA solution may vary by technology vendor and by usage, e.g. natural gas facility versus water treatment plant. Striking a balance between sector or industry specificity and usefulness will be essential to its wide adoption by the cross-sector CI/KR community. CI/KR owners and operators may vary by a variety of factors such as size, technological maturity, degree of automation, degree of centralization or decentralization, and amount of technical resources. All of these factors will influence the adoption or implementation of specific standards.

In addition, many in the CI/KR community are global companies and deliver products and services around the world and so must comply with sometimes conflicting international standards. Aligning the U.S. framework with international standards and best practices will be an important challenge.

3. Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

Intel has a robust set of Corporate Information Security and Privacy policies and procedures to govern and manage cybersecurity risk across our enterprise. Intel's information security programs are based on a risk management philosophy, and key security decisions are risk-driven. In general, Intel's cybersecurity needs fall into two categories: (1) protecting our own systems and networks, and (2) developing processes for enhancing the security features of our products and services.

Risks related to our systems and networks are handled by both a centralized set of corporate information security policies and procedures which are managed by Intel's IT security department and by a decentralized process by which each Intel business unit can also maintain specific information security policies and procedures unique to their products and services. Intel business unit policies and procedures may be more restrictive than the set of corporate information security policies and procedures. Exceptions to policy are managed through an approval and tracking process

with a set of risk-based criteria for management approval. In addition, for certain functional areas, such as Intel's external facing web services or outsource vendor services, Intel has defined corporate risk reviews and governance structures put in place to oversee the business process. For example, prior to outsourcing a business process or data management activity to an external vendor, a security risk review examining factors such as location and type of data being outsourced may be performed.

Information security policy is communicated via annual training for employees, updates to employee communications websites, and supplemental training activities. Specific job roles such as a system administrator may require additional information security training based on that role's risk profile. IT security regularly benchmarks various internal programs such as Training and Awareness against external companies to assess effectiveness and best practices.

The IT security department may also perform targeted risk assessments based on emerging technology or identified threats. For example, the implementation of a mobile device to access the Intel network may undergo a risk review ranging from a technical risk assessment to a policy enforcement risk assessment. Intel's IT Security Operations Group employs a rapid risk assessment process to examine malware and vulnerability risk and to inform our patch pipeline process.

Risk assessment activity is also a component of our Design for Security engineering lifecycle. This process is implemented within our business units, which are chartered to manage product security assurance. Key decision points within the product development process may require security risk reviews. Our factory security programs are based on risk evaluations focused on the unique needs of our manufacturing environment.

All Corporate Security functions report into a central Information Security Program Office (ISPO) managed by our Corporate Security Officer (CSO). The ISPO ensures a centralized escalation path for risk-based decisions and allows for a clear communication path to senior management on cybersecurity related risks. The ISPO creates regular cyber threat-related analysis and routinely briefs various levels of Intel management and key stakeholders on new and emerging threats. Periodically, Intel's executive leadership will utilize one of the many available employee communication channels, such as employee web, e-mail, business unit meeting, etc., to give a "tone from the top" security message to reinforce Intel's commitment to information security practices.

4. Where do organizations locate their cybersecurity risk management program/office?

Intel has a centralized Information Security Program Office (ISPO) that coordinates cybersecurity risk management initiatives across Intel. ISPO is a corporate function reporting into senior management at Intel. Within key business units, there are cybersecurity risk management programs which dual report into their business unit and into the CSO. For example, the IT Group has a large cybersecurity risk management group supporting the Intel enterprise network. The head of the IT Security Group reports into both the CIO and the CSO. This centralized program office is intended to coordinate and align cybersecurity efforts across Intel as well as provide some common services such as cyber threat analytics. In addition to cybersecurity, the CSO also is responsible for aligning and coordinating Intel's privacy-related programs.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

Intel relies primarily on internally-conducted risk assessments to determine cybersecurity risks. Since there are many facets to cybersecurity, we use a wide range of assessment methods. This allows assessors to select a method that best fits the type, scale and scope of the issue for an effective and efficient assessment. These methods include audits, traditional factors-based

assessments, program assessments, threat tree analysis, tabletop exercises, wargames, and others. Many aspects of the environment are assessed as well, not just networking components. Many areas such as technologies, processes, outsource vendors, office areas, manufacturing equipment, data flows, and personal devices may also be included in the cybersecurity risk assessment.

These assessment methods are generally based on industry best practices and are well developed and integrated at Intel. As part of an effort to further mature the effectiveness, Intel has incorporated some specific techniques and guidelines into all our methods. For example: since calculating the probabilities of cyberattack is notoriously difficult, Intel uses a threat-vulnerability-consequence (TVC) approach to measure risk, instead of the impact-probability approach typically used in insurance and other industries. Intel also incorporates standards or industry best practices, when available, to measure each of the TVC factors. In cases where such measurement techniques are not available or suitable, we develop our own techniques, tailored to the business and technical needs of the assessment methodology. Quantitative measurements are used when available, but qualitative measurements are the norm. Qualitative scales are typically limited to a low number of divisions, with well-defined and vetted evaluation criteria for each division. Regardless of assessment methods utilized, final risk results are usually mapped to a color-coded risk matrix familiar to most staff at Intel, so that communication of cybersecurity risk is uniform across business units and domains.

Participants in assessments are trained in the methodology basics, and assessment leaders receive additional training. Additionally, an important part of the training covers how to properly scope an assessment to meet both the technical and business needs of the customer.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

Cybersecurity risk is a fundamental component of Intel's overarching risk management. Intel recognizes that cybersecurity is embedded in most functions and aspects of the company, so it must be an important consideration in our various risk decisions.

For the most part various risk domains are managed independently by the Intel business unit responsible for that domain, e.g. the Finance unit manages financial risks, Information Technology (IT) handles enterprise network and systems risks, etc. Additionally, each of those business units is represented in various response teams and risk management functions that deal with cybersecurity. The Corporate Information Security and Privacy Office (CISPO) provides coordination and alignment on cybersecurity risks across the enterprise.

For example, assessing the risk to Intel's industrial control equipment requires a strong partnership between the IT security group and our factory automation teams. A joint working group examines the risks and reports their results to senior management, including the CSO, CIO, and factory leadership. In this way, we can easily update our overall risk picture, and effectively coordinate the required controls.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

Protecting Intel's systems and networks against a shifting and sophisticated array of threats requires a framework of information security risk management-based internal controls. While there are many helpful examples of existing frameworks which have informed the development of our Security Plans and Controls Framework, one particularly apt example of an accepted internal controls framework that we follow is the COSO Framework. Although developed as