April 5, 2013

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

RE: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt, !

Attached please find the comments of Cisco Systems, Inc. in response to the NIST RFI on Developing a Framework to Improve Critical Infrastructure Cybersecurity. We appreciate that NIST ! has issued this request for information, and are pleased to respond.

If you have any questions, or need further information, please do not hesitate to contact us.

Very Truly Yours, !

Adam Golodner !
Director Global Security and
Tech Policy, !
Cisco Systems, Inc. !

Current Risk Management 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?**

It's an old adage in cybersecurity, but still fundamentally true, when it comes to security practices, one size does not fit all. Each critical infrastructure sector, and each company within that sector, will understand best the challenges it faces improving cybersecurity practices for itself or its sector. Each sector, and many companies within that sector, sits within a different market environment, often a different regulatory environment, different technology environment, and some market participants are global in scope, while others serve specific domestic markets. Further, the threats and risks for each sector, and company within the sector, can differ substantially as well. Nonetheless, it is likely that as sectors or companies respond to this RFI, some common themes in sectors or types of companies will emerge.

For the U.S. IT sector, some characteristics that define the sector are that it is innovation driven, global, built on voluntary international standards (by bodies like the IETF, W3C, and the IEEE) that seek to ensure interoperability and security, and the industry drives innovation and security into the infrastructure through a build-once-sell-globally business model. These characteristics are central to the global success to the U.S. IT industry, and the ongoing competitiveness of the industry. Further, as a global business, IT companies have offices globally, and their internal IT systems are therefore global. Like other sectors, one challenge of enterprise cybersecurity for the IT industry is staying agile, changing with innovation in threats and defense, and seeking to ensure response and recovery.

In addition to challenges, there are significant incentives for IT companies to continually improve security. At a base level, companies want to protect their operations, but also preserve and expand the benefits flowing from the use of IT, benefits that have been a significant driver of global economic growth. IT companies, like other companies, also want to protect their intellectual property, and the availability and quality of the services they provide. And fundamentally, IT companies want an increasingly trusted global Internet and infrastructure, which fuels their future growth globally. These incentives drive the significant innovation and security in IT products and services, draw tens of billions of dollars in IT R&D (which includes R&D related to security) each year, and has spurred global standards like the Common Criteria (ISO 15408 and the related Common Criteria Recognition Arrangement) for product assurance.

With regard to specific issues, the sharing of information is crucial to improving cybersecurity practices, yet the ability and likelihood of sharing often depends on the type of information that might be shared. Some categories of information, like threat analysis, indications of compromise, and tactics, techniques, and procedures, are more easily shared than other types, and can effectively be shared across and within sectors, and have significant value. Security practices tend to be more organization specific and except in general usage (e.g. the categories set out in the Specific Industry Practices section of the RFI) less applicable outside each organization. It is also the case that often detailed security practice information is not shared as it may provide information that could be exploited to breach a system, and in any case often is enterprise specific.

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

The greatest challenges in developing a cross-sector framework will be finding something that works and maintains flexibility, agility, and innovation across different types of infrastructure, architectures, and business models – while at the same time recognizing and respecting the significant differences between and within the different sectors. Further, security threats are certain to evolve over time, and any framework needs to be iterative, and be flexible enough to allow best practices to evolve over time to meet those changing threats. Another challenge is ensuring that the framework doesn't lend itself to becoming check the box compliance, instead of thoughtfully applied security. And finally, as discussed above, information sharing about threats, tactics, techniques, procedures, lends itself to sharing across sectors and within sectors, while specific security practices tend to be organization specific, and a challenge will be how to capture practices like the general categories of Industry Specific Practices listed below in a method that allows organizational specific use.

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?**

With regard to our policies and procedures for governing risk generally, we have an integrated, cross-functional, decision making committee (known as the a risk and resiliency operating committee), that helps drive informed risk and resiliency decisions and risk governance. The committee oversees additional cross-functional working groups that focus on specific issues. The various working groups identify risks, ensure risk owners are assigned, and that risks are mitigated and addressed.

Specifically with regard to cybersecurity, our information security group has adopted a policy management lifecycle around the identification of policy topics, and the creation, approval and review of policies on a regular basis. Policy review and approval is provided by key organizations that include legal, human resources and IT. Through collaboration with our governance risk compliance group, security risks are prioritized and our policies and procedures are adjusted to address these risks. The results of these assessments are communicated to senior management. Further, the Audit Committee of our Board of Directors receives regular updates on information security, and the Audit Committee provides updates to the full Board of Directors.

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

We do not have a specific "cybersecurity" risk management office. Rather, risks associated with cybersecurity are managed by our global risk management and enterprise risk management teams, in coordination with multiple functions across the company, including the information security team. We find that this is a common approach in the technology sector. Any crisis or incident that could potentially disrupt our business would also be managed by our business resiliency team to address the situation and help to ensure on-going operations of the business.

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

As with other multinational companies, defining and assessing risk is a cross functional job involving multiple functions across the company. Primarily, the global risk management, enterprise risk management, information security, safety and security, legal and human resources teams join forces to identify, assess, and mitigate the risks we face. We also rely on information about current trends and conditions from industry experts in order to understand emerging risks facing companies like ours. From them, we are able to add a broad industry perspective, as well as to learn about specific issues. In addition, we regularly conduct benchmarking exercises with other large, multi-national companies.

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

Cybersecurity is one of the many risks identified and evaluated by our enterprise risk management group. The identification and evaluation of enterprise level risks by the enterprise risk management group is an ongoing process to ensure we address and capture the latest information relevant to assessing the risk appropriately. We have an enterprise risk management risk portfolio where all risks are defined and ownership is assigned to identify who is accountable for managing and mitigating the risk. As discussed in question 3, the Board of Directors receives updates on information security issues, as well as the risks associated with the global economy, execution risk, market transitions, and globalization among other risks.

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

We have developed practices for cyber and network security to address our and our customers' needs. In creating our internal security approach we draw on the leadership and expertise from our in-house InfoSec team, including our Computer Security Incident Response Team (CSIRT), our recognized global thought leadership in the area of security, a robust in-house security awareness and training program, as well as our interactions with outside groups like the IT-ISAC, the global Forum of Incident Responders and Security Teams (FIRST), ISO and NIST practices, and interactions with other information sharing organizations and our customers.

We incorporate elements of a number of different international standards in delivering our risk management framework, but we do not apply them wholesale across our enterprise. A variety of tools and assessment methodologies are used to measure the security posture of the enterprise.

One measure we find useful is how many issues we find ourselves verses how many we learn about from external reports. As we deploy new advanced tools sets, we discover issues we previously were unable to see. This helps us to increase our efficacy in finding issues by using better tools.

It is our continual investment in our practices, combined with mutual exchanges with our customers – both private and public sector - that continually make us more effective in what we do today. Our practices adapt each and every year, and have for twenty-five years. In working with our customers, we are constantly using our discussions and interactions with them as inputs to and exports of our practices.

8. ! What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

In addition to general corporate reporting required of public companies, including disclosure of material risks as part of required SEC filings, we would be subject to state laws on notifications of breaches if they occurred.

9. ! What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

As a large multinational corporation, we, like other companies, use and contract for a variety of services from sectors throughout the economy, including, but not limited to energy, financial services, telecommunications, and transportation. These services are factored into our enterprise risk management practices. As part of our risk management practices, we build-in resiliency and recovery, often by building-in redundancy of service providers, and dispersing geographic dependency.

In addition, we have a robust business resiliency team that is tasked with responding to crises or incidents that could potentially interrupt business. Our business resiliency program includes incident management, business continuity, IT services and data center integrity. The team is designed to respond to all types of incidents that may disrupt business, including cyber incidents.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

We have performance goals for the availability of services and the systems they rely on based on service criticality. Each main service is given a priority rating and based on that rating a service availability goal is determined. For business critical services we seek to provide geographic redundancy and failover.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

See response to question 8.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

The IT industry, and IT networks, are based on the use of industry-led, voluntary international standards developed by bodies like the IETF, W3C, and IEEE, which seek to ensure interoperability and security across global networks. For example, the Internet itself is based largely on these standards and standards bodies. And the Internet is governed by a non-governmental multi-stakeholder governance model, that has fueled the exponential growth of the Internet for a generation. The IT industry builds products based on these interoperable standards and a build-once-sell-globally business model that that drives innovation, security and efficiency into products and networks. The security of IT products is evaluated under the global conformance standard, the Common Criteria (CC), which is both an ISO standard, ISO 15408, and the subject of the Common Criteria Recognition Arrangement (CCRA) among most leading economies of the world. NIST is a partner in the National Information Assurance Partnership (NIAP), the Common Criteria scheme lead for the U.S.

The Common Criteria allows for evaluations by non-governmental independent labs, and mutual recognition by CCRA countries, allowing the IT industry to certify once and sell globally, avoiding any disparate and conflicting country-specific requirements that would undermine interoperability and security of the network. Further, the use of independent labs (accredited by the CCRA schemes) helps ensure the protection of the core intellectual property and innovation of IT companies. The CC is forward looking, and can evaluate for new issues, such as supply chain (where a pilot has been authorized), and new generation mobile devices. Importantly, the benefits of the Common Criteria evaluation and certification process inures to the benefit of all IT users, as the same product that achieved CC certification for national security systems under the build-once-sell-globally business model, is the same product that is sold into, and used by, private industry globally. Having and adhering to this global standard is of paramount importance to security, the interoperability of the network, and the IT industry.

As a general matter with regard to cybersecurity standards, global standards are critical not only for interoperability and developing global markets, but for improving cybersecurity posture. Poorly designed or implemented, or conflicting, national standards in the area of cybersecurity can create unnecessary risks that extend beyond the borders of a nation. Therefore, modern global standards tend to exhibit principles such as being voluntary, transparent, and expert-driven, and provide for interoperability, scalability, stability and resilience. These kinds of standards have a positive role to play in cybersecurity.

Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. **What additional approaches already exist?**

Many sectors have sector specific best practices and standards. Each of these sectors will understand best the challenges of and priorities for securing their enterprise, and providing service. In industries, enterprises or networks that are global, the use of global standards are particularly important. Many mature enterprises do not use any particular standard wholesale, but use and incorporate elements of many different standards or best practices to undertake enterprise cyber risk management. Some approaches that have gained mindshare include the NIST 800-series on risk management; risk assessment, and security controls guidance the ISO-IEC 2700x series on information security management system and information security management; and the Information Systems Audit and Control Association Risk Management Framework COBIT 5. Having said this, many sectors have industry specific approaches that enterprises and operators draw upon. For the IT sector and IT product security, the international Common Criteria is the global standard for product integrity evaluation and certification. Given the build-once-and-sold globally business model of the IT sector, the benefits of the Common Criteria obtained to sell to national security systems (with in the U.S. the Committee on National Security Systems deciding which information assurance or information assurance enabled products require certification) flow to all private sector users of the product.

2. **Which of these approaches apply across sectors?**

Different types and information and approaches apply across sectors in different ways. Information sharing about threats, tactics, techniques, procedures, lends itself to sharing across sectors and within sectors, while specific security practices tend to be more organization specific, with mature organizations (those having an installed base of systems) drawing on elements from some of the practices mentioned in response to question 1 above, as well as the thoughtful use of many of the Industry Specific Practices defined in the RFI below. Defining which elements can be applied as effective cross sector approaches, along with a healthy respect for the sector or enterprise specific practices, will be part of the work in creating the framework.

3. Which organizations use these approaches?

Many federal, state, and local governments, research institutions, and some colleges and universities use many elements of the NIST guidelines. M any global organizations draw from elements of the ISO or ISACA approaches, as well as they have the benefit of recognition around the world.

4. What, if any, are the limitations of using such approaches?

As discussed in response to questions 1 and 7 of the Current Risk Management Practices section, in mature organizations security practices tend to be more organization specific, with organizations drawing from elements of the practices mentioned in the response to question 1 above, as well as the thoughtful use of many of the practices set out in the Specific Industry Practices section below. Organizations should be prepared to modify, and add pertinent detail to whatever approach, or combination thereof, is implemented. Organizations may also have to tailor the approach to their environment and add detailed controls or processes where these may be beneficial. These issues are particularly important in new operating models, like cloud computing where a la carte services are moved in and out of the enterprise to gain efficiency and in many instances security.

5. What, if any, modifications could make these approaches more useful?

It may be possible to enable a modular approach, where enterprises use elements of existing relevant best practices that fit their enterprises, architecture, installed base of systems, future services, and business processes. The modular approach could also integrate in elements of the changing landscape (e.g., cloud computing, BYOD, etc.) that are needed to ensure that these approaches continue to be relevant to the risk factors encountered by organizations. The increase in the rate of change of the IT environment necessitates frequent review and update of the elements applied to the risk management of an enterprise.

6. How do these approaches take into account sector-specific needs?

Any approach has to take into account sector-specific needs, as well as the particular circumstances of the enterprise. A modular approach may be able to accommodate company, and sector, specific needs and avoid conflicts, while still maintaining the benefits of overall useful practices. It is important to prevent conflicting recommendations that may occur when attempting to manage sector specific guidance across industries and global boundaries.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

As a general matter, there should not be a conflicting, or divergent, set of best practices or standards.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

The DHS sector coordinating councils (SCC) have a great role to play in sharing and promoting the use of the voluntary framework. The SCC are the heart of the public-private partnership, and making them as effective as possible is key to the voluntary use and dissemination of the framework and other best practices. The success of the SCCs and the voluntary public-private partnership in the U.S. is also important as an example for the path forward for other countries dealing with the cyber issue now and into the future. Having successful voluntary SCCs and the use of the framework will set the right precedent globally. With regard to sector specific agencies, the members of each sector will have the best sense of the proper role of the sector specific agencies.

9. What other outreach efforts would be helpful?

In addition to the sector coordinating councils, outreach to small businesses and educational institutions is important. Small businesses need to understand what measures they can take to protect themselves and their customers, and educational institutions (both K-12 and higher education) can inculcate good cyber practices to young people so that it becomes second nature, and not a novel concept.

As a general matter, continued emphasis on cyber awareness and education across the economy continues to be critical. Understanding cyber risks and security practices need to become second nature, and integrated into the way we work and interact with each other.

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- Separation of business from operational systems;
- Use of encryption and key management;
- Identification and authorization of users accessing systems;
- Asset identification and management;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;
- Security engineering practices;
- Privacy and civil liberties protection.

1. ! Are these practices widely used throughout critical infrastructure and industry?

Most of the practices are used at some level of maturity in larger organizations, but use will likely vary across and within sectors. Also, most organizations have a mix of an installed base of systems, recent systems, and adoption of leading edge technologies, business practices, and business models. Those organizations having the greatest amount of divergent systems, those planning to or utilizing cloud computing or similar model, and those integrating personally owned devices into their IT systems have to work hard to implement these practices consistently across their organizational boundaries.

We find that the knowledge and experience in applying these practices is often concentrated in the IT organization. We also find that these practices are often most effective where the operational users of the IT in any particular business function have an understanding of the importance of security, and there is good dialogue between the user group and the IT department about the benefits these practices bring. Even within the enterprise, awareness and education is important.

2. ! How do these practices relate to existing international standards and practices?

Many best practice guides and standards address these practices. The complex challenge is negotiating some of the competing technical, cultural, business, and security considerations. Further, even if the category is utilized, if not performed with skill and diligence, organizations may not realize the limitations of their implementation of the practice.

3. ! Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

The majority of these practices are considered by entities as they plan for their cybersecurity operations. The relative importance of these practices would be dependent on the business practice at issue, and the risks, vulnerabilities, and threats to that process. There likely is substantial variance across organizations in the ability to undertake the detection and handling of the most sophisticated intrusions. It is important to have a base understanding of an organization's infrastructure and operations – systems and users on the network, location and access control to data, and where the borders of a network really are. Getting to this base understanding, and thoughtfully applying and integrating the right practices across both the existing installed base and forward leaning systems and operations, is of a high priority. It is also important to undertake network security architectural work up front, as architecture security engineering practices are valuable for creating resilient architectures and corresponding technology deployment plans.

4. ! Are some of these practices not applicable for business or mission needs within ! particular sectors?

All of these practices, or similar, are presented to greater or lesser degrees in existing guidance.

While organizations may place greater emphasis on some aspects due to particular risk factors, none of these practices would typically be considered out of scope.

5. ! Which of these practices pose the most significant implementation challenge?

Sectors, and enterprises within sectors, vary substantially, and some of the practices are of a higher priority, and relate to more or less critical business functions, depending on the particular enterprise or organization. This is why priority setting is so important. Also, the mix of installed base, newer and newest technologies and business operations to be performed also informs which practices impose significant implementation challenges.

One practice that is of significant importance, and often an implementation challenge, is the consistent, operational, discipline to apply and measure the use of these practices, and adapt, over time. A related challenge is the resiliency of important processes, which allows for services to continue under stress. Resiliency requires an intimate understanding of not only individual important processes, but also their dependency upon and relationship to each other. Consistent implementation of resiliency processes requires consistent awareness and discipline, which can prove difficult in highly distributed or fast moving environments.

Also as discussed in response to question 1, implementation of good security practices benefits from robust communication inside the enterprise - between the IT department and the users of the IT in operational units, so that everyone understands the security issue, the usefulness of the practices, and how security practices can be implemented while still achieving, supporting, and enabling the underlying business goals enabled by the use of IT.

Finally, there is often some tension between the implementation of one practice and the goals of another practice. Resolving this tension often involves making informed choices. Having a process to understand and negotiate these tensions is critically important.

6. ! How are standards or guidelines utilized by organizations in the implementation of these practices?

Many mature enterprises do not use any particular standard or guideline wholesale, but use and incorporate elements of many different standards or best practices to undertake enterprise cyber risk management. Many mature organizations also take a proactive approach and typically implement elements of standards and guidelines as part of a security and risk management framework that draws upon applicable consortium and/or industry best practices, and pertinent manufacturers and service providers recommendations. When applying some of these practices, often there are overlapping and sometimes conflicting recommendations that must be reconciled to suit the organizational risk posture. Organizations that have not spent significant time working through best practices are often faced with guidance lists that are accumulative, and would result in significant duplication of effort, and need to identify and harmonize conflicting recommendations.

7. ! **Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?**

Mature organizations would have such a methodology in place, likely aligned with risks as identified in their risk management program. This methodology itself would be subject to a "plan, do, check, act," or similar feedback mechanism, to ensure its ongoing relevancy and adequacy toward addressing risks in a holistic risk management program. Less mature organizations may still have a methodology, or some portion of it, in place, but frequently the full feedback mechanism is not operational and thus the effectiveness of the methodology may vary over time and eventually become largely incidental to addressing risk.

8. ! **Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?**

Many organizations have an incident response plan that will categorize incidents by impact or severity. If an incident changes in severity the escalation process will be implemented and the necessary resources applied to address the risk. There can be multiple escalation processes depending on the type of incident that occurs. One practice related to escalation is the timely recognition of the incident and the corresponding need in many environments to maintain important functions in a degraded or under-stress mode.

9. ! **What risks to privacy and civil liberties do commenters perceive in the application of these practices?**

The impact on privacy and civil liberties have to be part of every implementation of a cyber strategy. Security and privacy are not mutually exclusive, and can co-exist. Many of the components listed in the question implicate both privacy and security, and these implications should be understood and thought through as each of these components are incorporated into a security plan.

10. **What are the international implications of this framework on your global business or in policymaking in other countries?**

The IT industry is a global industry, both as to the products it sells, and to the location of its own enterprise infrastructure. This is why international standards are so important. The industry is based on international standards that seek to ensure the interoperability and security of networks and products. What the NIST does here sets a precedent globally. The international implications and effects are core to the continued success of the U.S. IT industry as a leading innovation industry into the future. This is why international standards, like the Common Criteria, and the ability to innovate and drive security and interoperability into networks and products is so key. One screen to apply to the framework is whether something proposed works internationally, and whether the U.S. would be happy if another country suggested the same thing, or something of the same kind, but of an exaggerated scale. NIST is setting the global path forward, and like most of NIST's work, adhering to base principles of global networks, innovation, interoperability, and standards are good principles to apply here.

Recognizing that the IT industry is global, standards-based, interoperable, and that security needs to driven by innovation, and the build-once-sell-globally innovation and business model, the Executive Order seeks to ensure that the framework provides guidance that is 'technology neutral,' that is that it doesn't get the government into the design, development, or manufacture of commercial IT products, and doesn't pick winners and losers. This same sentiment is expressed in the leading drafts of U.S. legislation. To do otherwise would undermine the very innovation and security we need to promote security, and give other governments license to interfere with the core innovation engine of the IT sector, impose country specific requirements, and pull apart the very innovation, interoperability, and global standards that are needed to drive security and innovation into the global network. Any country specific requirement would also undermine the Common Criteria, the global product evaluation methodology that undergirds security and innovation globally.

11. How should any risks to privacy and civil liberties be managed?

See response to question 9.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?

It would be useful to examine the applicability of existing best practices or standards for information sharing about threats, tactics, and techniques and which practices are most useful for sharing and making actionable these types of information.