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: McAfee comments in response to NIST RFI, "Developing a Framework to Improve Critical Infrastructure Cybersecurity"

Dear Ms. Honeycutt:

McAfee, Inc. appreciates the opportunity to respond to NIST's Request for Information (RFI), "Developing a Framework to Improve Critical Infrastructure Cybersecurity," noticed on February 26, 2013. We regard the RFI as an important demonstration of a public-private partnership in the critical area of cyber security.

McAfee is committed to working with NIST alongside our private sector and government colleagues to help create a framework that enables industry to create high standards and best practices in cyber security that enable innovation for a safe and creative future.

Thank you again for requesting comments. You will find ours below:

## Section 1: 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?

There are three broad types of challenges we see: attitudinal, technological/ management and policy.

*Attitudinal Challenges*

Many companies still view cyber security as an "IT" issue, or even an afterthought, instead of as a boardroom consideration that affects the entire business, their customers and their shareholders. They focus budget and attention on cyber security only after a damaging event, thus creating a negative perception of the issue instead of viewing it as a business enabler. However, when cyber security is viewed and employed correctly, it can enhance business resilience, customers' experience and confidence, and increase morale of the critical teams responsible for security.

In addition, many organizations hesitate speaking about cyber security because they are concerned about liability or damage to their reputation. Many also fear they will be overly regulated into compliance-based, prescribed security instead of retaining the ability to use their resources creatively to engage in a connected, aware, ecosystem-based approach. Positive incentives established by the government can help to fund the latter approach and alleviate many concerns.

*Technological and Management Challenges*

In addition to attitudinal challenges, there are technological and management challenges as well. Four important security needs of critical infrastructure customers and partners are situational awareness, multi-zone protection, native support for Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) solutions, and continuous compliance. The greatest challenge in deploying an architecture that encompasses all of these countermeasures is the inability to have a consolidated viewpoint by which all of these defense mechanisms can correlate and share data and threat intelligence, thus allowing the administrator to build a more in-depth and robust security infrastructure.

Some of the failings of the current security landscape are caused by the approach vendors of security products themselves have created in that products have been focused on proprietary approaches to solving a specific issue. Often those products are not open from the standpoint of sharing information about the events observed or actions they have to take to provide the protection intended. Having a security infrastructure that cannot communicate critical information—be it events, vulnerabilities or configurations errors—prevents the network administration staff from being able to see the larger picture and blinds them from seeing what is occurring. Today, context is critical to being able to make an informed decision as to what actions to take, but stove-piped security products that do not or cannot communicate that information, provide little towards improving the security posture.

And it is not just security products that are segregated from each other. In many organizations, while security does exist in areas, it is not integrated with operations. Often network security and operations are separated by organizational structures, which can slow down information exchange and response time. Security needs to be integrated at every level of a company's operations.

McAfee fundamentally believes in a connected, adaptable and dynamic security platform to join risk management, operations and internal and external policy to guide automated and human security decisions. With such a platform every network component becomes both a producer and a consumer of intelligence. This intelligence can then be shared within the network and externally (as allowed by policy) to enable an adaptive, learning ecosystem that gets smarter as it protects.

*Policy Challenges*

Some of the greatest challenges to legally and effectively implementing holistic and systemic cyber security measures deal with the complex and often paradoxical relationship security measures have with underlying data assets and the people to whom they relate. For example, the data privacy rights of users and operators of systems are intimately tied to the very protections that would preserve those privacy rights. For example, to authenticate a user, we must collect and retain details that clearly and unambiguously identify that user as the authorized party.

Failure to do so results in poor information assurance, weak predictive measures and faulty forensic or reparative processes. Actively retaining these elements often challenges the legal and user expectation requirements for systems' usage, particularly in a global informational environment.

Data protection requirements must balance the interplay between privacy and security and the various stakeholders that develop, propagate and manage the various requirements and consequences in these linked but not identical fields. Similarly, considerations about liability, public policy, popular perceptions and fears of overly aggressive government oversight all must be addressed and managed for both the public and private sectors.

Finally, most large critical infrastructure organizations or the organizations that support the critical infrastructures either are themselves global entities or heavily depend upon stakeholders and requirements that originate outside of the United States. These global considerations cannot be set aside for the stated purpose of security without impacting the very viability of critical infrastructures and their supporting partners. Privacy is particularly sensitive to these types of risks, as the U.S. is one of very few nations that has not codified a national standard for data protection, thus leaving global entities at the mercy of the exceptions for data processing as regulated internationally.

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

Identifying a common, standardized framework across multi-sectors proves difficult for most organizations, as many are unaware of which sectors they fall into and how these various sectors differentiate from one another from a security perspective.

NIST is taking the first steps by gathering the information needed to understand what is common across the critical infrastructure sectors. There will undoubtedly be differences, such as in a classic network environment where staff can update systems by patching vulnerabilities quickly versus those environments where changes cannot be made as easily due to the age of the equipment or the mission it is supporting. In certain sectors it may be hard to put additional software on the running systems. Testing required to assure any change is not adversely affecting the operational aspects of the devices can be complicated by the primary purpose / mission as well as uptime requirements of the devices.

While the intent is to create a reasonable and consistent standards-based security framework, we may encounter situations where needed pieces of that framework do not exist but are critical to the success of the framework. For example, a well-defined scoring mechanism that can be consistently applied across the framework to demonstrate an organization's current measurable security posture does not really exist. We have many that would be needed as input to an organizational scoring model, but today there is not a standard way understood by industry participants that can be directly applied to a cross-sector security framework. Developing it and assuring it is recognized as a valid approach will take efforts by many.

In addition, if a "standard" is the goal, then it must be vetted by the proper standards organization, be it a national standards body or an International standards body. Specifications, while core building blocks for creating standards, are not really standards. Using the word "standards" has an official connotation. Official standards bodies create "standards"; all other

organizations create specifications. Granted, a specification can be developed by a coalition of the willing and adopted as a convention by all participating, but if a literal standards-based framework is the objective, then it should be understood that 1) there may be missing standards that will need to be developed, and 2) that process will take time.

Furthermore, developing a standards-based cybersecurity framework is one thing; deploying it and making that framework useable in all sectors is another. NIST should be open to the potential for a multi-level framework wherein certain sectors may only be able to run a lowest common denominator framework due to their deployed operational restrictions. Other sectors may not have such restrictions and could layer on top of that basic framework those capabilities that a more advanced or mature security framework may include. This approach provides NIST the ability to create a layered framework model that is not limited by the restrictions of any specific sector and that enables a highly advanced framework. This model also could be used to provide sectors the ability to mature their cybersecurity deployments over time, providing the capability of adopting another more advanced component (or layer) of the overall framework.

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?

We maintain a Governance, Risk and Compliance Committee to review risk and approve policy. This committee is made up of key executive management with Board of Director level oversight.

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

In the vast majority of companies the CISO reports to the CIO. This structure works as long as the CISO has the independence to deliver technology with agility as controls are needed to ensure the confidentially and integrity of data. If, however, through size and complexity that independence is compromised or hindered, the CISO should have a peer relationship with the CIO.

In addition, in some organizations, the computer security staff resides in a different operational organization than the network operations staff. This can cause problems when time is of the essence. Having to traverse an organizational structure to get approval for effecting a network change needed to address a security concern can delay the effectiveness of the change. The attackers are working at wire speed, and in most organizations, responders are working at human speeds, and in some cases the humans are working at organizational speed.

Of even greater concern, however, is the fact that if cyber security risk management is confined to the IT department, it never receives the appropriate level of attention. Security needs to be considered an issue of risk—from the boardroom. Only then can we base cyber security investment on a holistic prioritization of corporate assets and create a connected ecosystem with high return on investment. When left as only an IT decision, cyber security is often underfunded, not prioritized within executive decisions and done based on point gaps rather than designed to create long-term resiliency. Transitioning cyber security to a boardroom concern and investing in resilience is one of the most effective steps toward safer networks focused on connected, asset-based ecosystems.

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

The maturity of security controls and security architecture directly influences risk assessment process. A mature cyber security program reduces risk levels to brand reputation, legal and operational continuity by limiting the institution's vulnerability to intrusion attempts and the changing threat landscape.

Assessing risk is the process of identifying and understanding threats to confidentiality, integrity, and availability of information and Intellectual Property. A risk assessment consists of the identification and valuation of assets, compared and analyzed against the potential threats and vulnerabilities. The resulting information is used to develop strategies to mitigate those risks and produce work efforts. Once security requirements have been identified, controls should be selected and implemented to ensure risks are reduced to an acceptable level.

From a legal perspective, risk is parsed out among the following:

- Customer and employee data legal compliance to existing laws and regulations
- International Data Transfer risks and compliance, such as the Safe Harbor schema between the European Union and the US Commerce department and US Federal Trade Commission
- Operational and organizational risks relating to training, awareness, preparedness and measurement
- Economic risk in terms of the ability to transact and do business given our own data practices and the requirements as negotiated and required by our customers regarding our management of their data
- Reputational risk where we stand to lose our relevance as a leader in the data protection space if we are perceived as being less than transparent or weak in our ability to provide excellence in both security and privacy.

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

Based on what we see among our customers, many large organizations, such as the major banks, have a well-integrated risk and cybersecurity risk management program. The greater concern lies with small businesses, which comprise 99% of the business fabric of the U.S. Smaller companies do not usually have the resources for large teams or expensive solutions, yet they have intellectual property, personally identifiable information, and brand reputation to lose – just as any large company. For small business, as for any size business, cybersecurity should be an issue of risk at the board level – even in the smallest of companies. Additionally, we need an approach that enables small companies to implement a connected, holistic approach that considers their networks an ecosystem of traditional, mobile and cloud devices and services.

This ecosystem concept is well described in the white paper from the National Protection and Programs Directorate within the Department of Homeland Security: (http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf). Done correctly, networks can detect behaviors over time and begin to recognize, almost biologically, threats before those threats can overtake network functionality. Maturity models have shown

that for any size organization, a wise design up-front leads to increasing security and decreasing cost over time. A connected, behavior-based approach enables network components such as phones, laptops and servers to communicate observed behavior amongst each other. Security can thus be managed in real-time based on policy that adapts to current threats and provides resilience: the ability to run while under attack.

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 will respond both as an organization that must manage its own risk, and as a supplier of security related tools that our customers use to protect their networks.

*Securing Our Organization*

At the highest levels in McAfee there are polices that provide official directives to employees who must make present and future decisions. We consider policies to be business rules and distinguish them from standards and guidelines. Standards consist of specific mandatory security controls and explain how policy statements are to be satisfied. Guidelines consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place. Finally, we have procedures, or step-by-step instructions, to assist employees in implementing the various policies and standards.

Operationally, we use an Intellectual Property Controls Framework as an architectural guideline for securing systems. It's a defense in depth approach that combines technical and non-technical controls. The outermost layer includes the aforementioned policy framework and a robust Security Awareness and Training program. Audit and remediation is the next layer that identifies vulnerabilities and validates compliance against security policy. Next we employ physical security of the assets with access controls systems and identity management of users and devices.

Internal layers consist of our network security activities representing firewall, intrusion prevention system, penetration testing, scanner deployments and enterprise security network architecture. The application security layer starts with standard and secure operating system builds, deployment of data loss prevention and process control within the application. The innermost layer of ring zero is the centralization and federated control of the data element that is being protected.

*Supplying Leading Security Products*

As a supplier of security products, we believe in an open architecture for the integration of security products. This is very important from both an operations and information perspective. Over the last 10 years security automation efforts have been laying the groundwork for transforming how networks are managed. The Security Content Automation Protocol (SCAP) was developed in conjunction with security vendors, various US government agencies and the MITRE Corporation. This effort has begun to lay the plumbing needed to break down the proprietary approaches security vendors have used in the past for evaluating and measuring the state of networked devices such as servers, desktops, routers and other devices. Operations that

used to require staff to touch each endpoint and take a massive number of staff hours to complete can be completed and managed from a central point in the network in very little time. The SCAP component standards consist of:

- Means to identify software vulnerabilities and configuration errors
  - Common Vulnerabilities and Exposures (CVE) - Standard identifier and dictionary of security related software flaws
  - Common Configuration Enumeration (CCE) - Standard nomenclature and dictionary of software misconfigurations
- Means to name and identify systems
  - Common Platform Enumeration (CPE) - Standard nomenclature and dictionary for product naming
  - Asset Identification
- A means to encapsulate policy evaluation guidance
  - eXtensible Checklist Configuration Description Format (XCCDF) - Standard XML for specifying checklists and for reporting results of checklist evaluation
- A means to check state of a device
  - Open Vulnerability and Assessment Language (OVAL) - Standard XML for test procedures
- A means to automate asking administrative questions
  - Open Checklist Interactive Language (OCIL) - Standard XML for human interaction
- Scoring mechanisms for measuring the impacts
  - Common Vulnerability Scoring System (CVSS) - specification for measuring the impact of vulnerabilities
  - Common Configuration Scoring System (CCSS) – specification for measuring the impact of configuration issues
- A mechanism for aggregating and reporting results of the evaluations
  - Asset Reporting Format (ARF)
- And the Trust Model for Security Automation Data (TMSAD)

These component specifications provide a standardized means for specifying how evaluations are performed. SCAP validated products produce the same results when given the same SCAP content to drive the evaluation. Additionally, the results generated are in a standardized format, allowing the results from one SCAP security product to be the input to another security product. This has proven very successful in the field in enabling network staff to do much more in less time. We believe SCAP and its component specifications are the building blocks for the security framework that NIST is working to develop under the Executive Order.

Additionally, there is an effort initiated by SANS titled, "***SANS Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines***," which states: "The strength of the Critical Controls is that they reflect the combined knowledge of actual attacks and effective defenses of experts in the many organizations that have exclusive and deep knowledge about current threats." The success of the guidance specified in the Top 20 Critical Security Controls has been demonstrated over the past few years. It also should be noted that this is a living document that is continually refreshed to assure the guidance provided continues to be useful.

We are also subject to Federal Trade Commission (FTC) regulation based on our products, services and public statements regarding our privacy and security competencies. In addition, we are a Safe Harbor certified company and thus must follow the Fair Information Principles as embodied by that agreement as well as submit ourselves to jurisdictions across the EU and Switzerland. Internally, we look to other standards such as the Generally Accepted Privacy Principles standard as promoted by the American Institute of Certified Public Accountants and the Federal Sentencing Guidelines as generally applied to compliance efforts regarding responsibilities and programmatic approaches to compliance within the organization.

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?

A partial list of these reporting requirements includes the following:

- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards (CIPs) – though not regulation per se
- Breach notification laws in 48 states and associated cyber security "reasonable security" requirements in companion State and local level
- NIST 800-53
- NIST 800-137
- USGCB
- FISMA
- SANS
- The Sarbanes-Oxley legislation

We are also subject to all sectorial federal and state laws relating to data protection either directly or as a vendor to our customers. Additionally, we do business in nearly 80 countries, and most of these countries have detailed and specific data protection laws and requirements and often both data protection and privacy laws and regulations, as well as specific cyber security rules and regulations.

The mobile, ISP and payment industries have additional industry-specific regulations that may not be codified as law external to those industries, but which comprise concrete requirements for our business.

The regulatory landscape is broad, wide and as local as to townships and taxing authority data and global as APEC and other multi economy requirements and standards.

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

All business assets have interdependencies upon critical infrastructure. A good example is electric power, which enables all communications, IT systems, financial systems and other critical needs. Power can be backed up with a diesel generator, usually for a maximum of three days, depending on a delivery of diesel, which calls upon another cascading set of dependencies from oil/gas to transportation. Information is nearly always at the heart of the ability to seamlessly weave together and deliver such needs. Thus there is a need to protect the

confidentiality, integrity and availability of the information that drives the provision of such critical infrastructures.

Today, cyber is the nexus of critical infrastructure. Blocking a cyber attack is a great first step, but existing approaches tend to stop there. The most important steps, however, are answering questions such as, "What have you learned from blocking that event? Why did you block it? And what can you now share with the rest of the network in real time?" Someday, perhaps we can even share this information with other networks, companies, ecosystems or countries.

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

Cyber security metrics are one component that helps facilitate decision-making, manage budgets, create awareness and improve performance. Organizations can use metrics as a benchmark to apply corrective actions, deploy counter measures and improve overall performance of IT systems. Security metrics can cover a broad range of measurable features depending on the scope and authority of the INFOSEC departments. Effective security metrics should be used to identify system vulnerabilities, better determine where to utilize security resources and help determine work efforts of implemented security solutions.

Metrics on areas such as the following could be useful:

- Security Cost
- Information Security
- Business Conduct
- Security Audits
- Background Checks
- Business Continuity Disaster recovery
- Security Costs as a percentage of total company revenue
- Audit implications
- Security operations
- Physical Security and Premises protection
- Policy Check
- Procedure Check

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?

We are required to comply with federal and international regulations as well as industry standards. This process is typically handled through activities such as an external audit or assessment. A consultative process with the governing body is used to assess the cyber security related risks to the organizational missions and business functions. The output is a menu of management, operational and technical security controls, including policies, processes and procedures are routinely reported.

When building the framework, it is important to avoid imposing a disproportionate financial and administrative burden or imposing requirements that are not proportionate to the risk presented by the network or information systems.

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

Cyber security is a global economic, business and safety issue, transcending international, corporate and competitive boundaries. Global standards are key to ensuring that risk can be managed and security be provided that is product and country-agnostic, enabling voluntary worldwide communication and participation in connected systems.

Even where entities may not agree on specific products or guidelines, global standards of communications and expression of risk will allow the global ecosystem to be safer and more aware of areas that are not as safe, providing more choice and awareness to users – corporate, government and consumer.

Standards provide a foundation upon which the security industry can build. As previously mentioned, security products need to be able to connect to and share information they gather with other parts of the security infrastructure. Standards enable that type of communication to occur and to allow for much more advanced tools to be built and fielded. For example, the Internet Engineering Task Force (IETF) is an international standards body that provides a venue for advancing the interoperability needed. It is a place where consensus can be achieved in an open and transparent way. Organizations such as IETF allow for participation from all who wish to contribute, working towards true global standards that can be fielded regardless of geography.

National standards bodies also play a critical role. In the case of SCAP, much of the work was developed in conjunction with NIST, a US national standards body. National standards bodies can be a great place to incubate an effort that is later taken to an international forum.

That said, not all standards bodies have the same goals or intentions. It should be noted that technical development is needed. That can be accomplished in a reasonably timely fashion only in a technical, not political standards body.

Today, however, there is no dedicated security related standards body – a fact that can be seen as an impediment to developing security standards. On the other hand, we can say that security should not be something separate; instead, it should be an integral part of all network and computing operations and standards.

## Section 2: 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?

The security landscape is continually improving and maturing. We see where we can go using the security automation and other related existing security standards. The problem is that we are just now getting to the point where those building blocks can be reasonably assembled into real operational security frameworks. The federal government has been leading the way in the use of consistent security frameworks. The emergence of CAESARS and CAESARS / FE provide an excellent example of a framework that would provide better manageability and usability to those responsible for securing critical organizational networks.

There are examples of other efforts as well. Today NERC CIPS are considered a best practice in the energy sector. The security industry has been collaborating to establish best practices to help provide guidance on various aspects of cybersecurity as seen by the SANS 20 Critical Security Controls.

Other governments are addressing the same types of issues, as illustrated by the DSD Australian Defence Signals Directorate (DSD) efforts. DSD is Australia's authority for information security, providing the government with:

- Advice and assistance to federal and state authorities on matters relating to the security and integrity of information
- Greater understanding of sophisticated cyber threats
- Coordination of and assistance with operational responses to cyber incidents of national importance across government and systems of national importance.

Today many organizations seem more focused on following industry best practices in their currently deployed security technologies – for example, how to properly configure DNS, protect against malware and scan for vulnerabilities – rather than standardizing on a security framework. Many organizations have staff that are overworked and are not able to step back and totally reevaluate their approach to networked security – even if that is what is really needed. Providing a standard framework for integrated network security operations is a positive step in assisting these types of organizations. The security framework in itself can become an industry best practice.

2. Which of these approaches apply across sectors?

Anytime you can instill industry best practices, such as the system hardening guides produced by organizations such as Center for Internet Security (CIS) or operational best practices such as the SANS Top 20 Critical Controls, the sites that use them will improve their security posture. The problem is better visibility is required into what is occurring on organizational networks. That

requires standard content formats, standard results formats / feeds and the ability to measure improvement on the network.

In the US Federal world the CAESARS effort is a part of the "Continuous Monitoring" efforts. In the commercial world today that same approach is call "Situational Awareness". The intent of both is to put in place a security framework that provides the organization with timely visibility into their networked infrastructure to assure they know what is occurring and can act appropriately.

Standard metrics and approaches to demonstrating improvement are required if we are to expect any real positive results from this effort. The ability to aggregate security component related measurement information into a standardized means for evaluation allows for the transparency needed to gauge where staff need to focus their efforts. In all sectors, security effectiveness needs to be measured and then managed based on those measurements. Security improvements will not happen overnight, but as incremental security improvements become a core part of an organization's operations, they will add up quickly and the site's security posture will become demonstrably better.

3. Which organizations use these approaches?

Today it is the more mature sectors that are attempting or have attempted to develop and implement security frameworks. For example, the energy sector, financial services organizations, as well as larger organizations such as the Fortune 100 companies have dedicated cyber security staff and/or resources to methodically step back and view how security frameworks can make their efforts to secure their networks more consistent and their results more positive.

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

All of these approaches guard against the threat we already know. The problem lies in the threats we have not yet seen. To manage those we need to equal or surpass the innovation and agility of our adversaries with innovative approaches.

Also, in many of these and other existing approaches, compliance becomes confused with security, as can happen with CIPS. Meeting these recommended standards does not ensure cyber security or resilience. Rather, it ensures a minimal coverage of what is known, vice an innovative behavioral approach that can enable a company to more quickly detect new attacks and bounce back more quickly when the adversary does get in – and they will get in.

As with any type of truly novel innovation, solutions to the growing issue of cyber protection must be balanced and tested against current and proposed data security and privacy concerns and legal structures.

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

All of these approaches would be more beneficial if focused on the type of security discussed above: a connected approach to detection, measurement, monitoring and response that leads to an ever-strengthening system based on behavior and intelligence. That currently is the best

known way to build resilience against an attack designed to thwart everything for which we are prepared.

Continuous Monitoring of systems is an excellent microcosm of what is needed. On the broader macro level, systems, and groups of systems, need to learn from what they are watching and inform other parts of the system as well as – in the future – other systems as well, as permitted by evolving global privacy policy.

Sectors can monitor their events and compare them to those in other sectors and geographies. As previously stated, blocking an attack is a great first step, but existing approaches tend to stop there, when the most important steps are what have you learned from blocking that event, why did you block it, and what can you now share with the rest of the network in real time?

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

Most sectors' cybersecurity needs will be very similar. ICS and SCADA are also similar across the sectors they enable. The connected and aware approaches that we advocate in this response can apply to all sectors, as logs will reflect cyber events and can be shared – as global policy will allow – across sectors, companies and countries.

Sector-specific needs can be measured with the help of the Sector-specific Risk Assessments that have been conducted across CIKR as part of the NIPP framework. Per the Executive Order and corresponding Presidential Directive 21, when the NIPP framework is reviewed, the risk assessments may be a key part of the NIST framework in determining standards that apply to each sector and across multiple CIKR sectors.

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

Sector representation will help to ensure that any sector-specific or nuanced areas are covered in a cross-sector framework, but it is not clear that every sector needs its own cyber standards. Simplicity may be the best tool to engage the strongest participation for the most effective framework.

As previously stated, the cyber issues across sectors will often be very similar, However, this question cannot truly be answered until the real work of gathering the requirements from across the different CI sectors has been done.

Existing frameworks that have been mentioned here have been developed via a "coalition of the willing." They have been companies and individuals that saw the need for a framework or commonly agreed to specification and have come together to do the work. They have been focused around sectors or efforts in the past, not because it was predetermined that was the right approach, but because that was the forum the work was initiated in. Since the effort behind this RFI is to develop a cybersecurity framework that is cross-sector, it seems that going forward a sector-specific effort should only be considered if there are sector specific additions or enhancements needed to the NIST developed framework.

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

Together, the sector-specific agencies and sector coordinating councils can help to create an incentives-based framework and perhaps some of the actual incentives.

9. What other outreach efforts would be helpful?

Outreach is critical for the developed framework to be successful. There are those that work closely with the federal government and will of course know of this effort and will follow and participate. There are many, many more that will not even know about this effort until near the end of the EO timelines.

In the security automation space outreach was critical. The word about the valuable and needed work had to get out. The security automation success was as much about the technical aspects of the solutions as it was about the evangelizing done by community that built it.

As this effort proceeds, it is important that outreach to CI sector specific organizations occurs. Each of the CI sectors has its own consortia, Information Sharing and Analysis Center (ISAC), press, analysts and industry trade associations that are specific to the 18 critical infrastructure sectors.

When building a global training class, it is impossible to have a single person do all training. What they can do, however, is to conduct "train the trainer" classes. This multiplies the capabilities and allows the training to be achieved quickly in many different areas of the globe simultaneously. That model is what is needed here. NIST needs to locate those CI sector specific industry trade associations, consortia and ISACs and educate them as to what it is the effort is trying to achieve. In this fashion, NIST would be training those that will then take that knowledge and share it with their specific sector customer organizations.

We also believe the small business community would benefit from not only outreach but also sharing of threat information as occurs in the best ISACs.

Outreach is critical to adoption. Without getting organizations to adopt the newly developed cybersecurity framework and associated best practices, the intent of the effort cannot succeed.

## Section 3: 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?

Large companies regularly use these practices. Smaller companies often lack the resources to be as thorough, and get caught in the trap of purchasing "point" solutions for say one area (e.g. intrusion detection) but do not think holistically about their entire ecosystem where access control, IDS and even privacy issues must connect together when considering events in both real-time and human-time analysis.

This is where regulation would make CIKR less secure by focusing on specific areas and not taking a holistic, ecosystem approach. Adversaries would know how to attack, given it would be the areas that are not regulated. Innovation would no longer be well funded or rewarded, as funding would go toward the regulation-prescribed areas.

The list above is currently very valid. New technologies and new attack vectors will rapidly outpace the timeliness of this list, and the list itself and policy around it needs to rapidly adapt, which regulation cannot.

We are asked if these practices are used widely. For the most part, the answer is yes. However, that can and should change with time as new technologies become available. We see the benefit of the voluntary standards-based framework being the flexibility to adapt to changes in our systems and overall ecosystem – as per the NPPD ecosystem paper mentioned previously.

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

In these areas, the US takes a leading approach. The EU, Australia and Singapore are putting some similar practices in place, with opportunities to collaborate. Australia's Information Security Manual (ISM) is a great international practice to follow and emulate for this purpose. We should note that EU privacy policies will be key to any international cyber threat intelligence collaboration.

In the last couple of years, we are seeing standards adoption becoming more evident around security related compliance. Some countries have software vendors that are developing and selling SCAP enabled products. SCAP security automation products are being actively developed in the US, Brazil, Germany, and India. We are also seeing countries are adopting SCAP related security automation specifications and enumerations. The Common Vulnerability and Exposures enumeration is currently in use in China, Taiwan, Israel, US, Finland, Malaysia, Switzerland, Hong Kong, Korea, France, Germany, Japan, Australia, and others. The success the US has had with security automation efforts has not gone unnoticed globally.

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

While all of these practices listed are important, there are a few that stand out. We see mission/system resiliency as critical. To achieve this, a good cyber security investment up front leads to decreasing costs and increasing resiliency (based largely on the other items on the list) over time.

Encryption and key management are vital to protecting critical information from prying eyes. Having a network where all the assets are identified and rogue devices are immediately identified means the organization has a better foundation in which to monitor activity and compliance. Additionally, having all users identifiable to the environment allows for separation of roles and informational need to know capabilities.

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

All of these practices apply to all and across all sectors.

Additionally, they may not individually seek out critical infrastructure as a reference, but the intentions and foundations of these security practices are the very building blocks that will help NIST and other agencies build this framework.

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

This may depend on the criticality of the sector's mission. Some sectors may have a more tightened or intricate, specific framework, which may require a bit more effort in the initial implementation. Areas involved with SCADA and secure grid are good examples of potentially more challenging implementations/deployments.

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

ISO standards are often referenced. Encryption standards are used to show a responsible level, and the SANS controls or NERC CIPs may be employed to demonstrate a level of best practice in some areas. Largely, implementations are not based currently on a single framework or standards.

In all these areas if there are products that support standards then they are often used. Reality is, as much as we would like to think there are widely deployed standards for all the practices listed, there are not. In many cases even best practices are weak or not widely understood. We would hope that organizations would leverage standards if they exist but standards have not been as important to organizations as was solving the problem they are trying to address. This is a matter of maturity when it comes to understanding security. The security industry is just now getting to the point where most all understand security standards are critical to moving forward but that does not mean the ones in place today address all the needs of the practices listed. In many areas, security related standards are just now emerging.

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

Large organizations have a broader perspective as previously stated to view cyber security as a business and boardroom-level issue vice an IT subset. Standard methodologies for resource allocation are more common.

Information Technology operates a formal portfolio guiding investment decisions. The IT Portfolio process balances risk and complexity with cost and resource capacity. Portfolio investments are evaluated monthly and portfolio decisions are made quarterly by a committee of IT leadership. The company maintains a Portfolio Manager to assess details and make recommendations to this committee.

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

Increasingly, given breach notification laws in some states and responsibility to protect PII, more companies are putting processes in place. For example, a formal escalation process is defined and documented in the event of data breach. Companies should maintain a listing of entities to contact based on federal guidelines, industry best practice, and contracts with customers. It is impossible to plan for every possible event or contingency, but one must have a framework that is flexible but consistent. Having a plan in advance is crucial to the success and evaluation of risk to an organization.

Continuous Monitoring of the network and asset management gives actionable data to assess the severity of risk to assets. Key elements of a formal escalation plan include:

- Preparation
- Containment
- Recovery
- Identification
- After Action
- Eradication

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

As previously discussed, data protection requirements must balance the interplay between privacy and security in addition to the numerous stakeholders who develop, propagate and manage the various requirements and consequences in these linked but not identical fields. Innovative solutions that allow for system and process improvements will be necessary as we increasingly engage in an interconnected information ecosphere that is truly global in nature. Similarly, considerations about liability, public policy, popular perceptions and fears of overly aggressive government oversight or intrusion upon data privacy protections all must be addressed for both the public and private sectors.

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

The global information and communications technology (ICT) industry is fast moving and depends on rapid innovation to meet customer requirements. Governments should further the adoption of global security standards to address security assurance concerns and to better secure the critical infrastructure, as opposed to taking a geographically siloed or local jurisdiction focused approach to security regulations. Focusing on the development of country-specific regulations – especially those that disadvantage products developed in other countries – will impede the continued development of security products intended to be sold and operated globally.

Regulations tend to force budget allocation to compliance, a shorter-term goal often leading to protecting against a subset of known vulnerabilities while leaving others wide open until regulations catch up. Further, regulation discourages investment in new technologies for better security, which leaves little funding or incentive for true scientific innovation worldwide. Governments seeking to establish security assurance standards and other security standards should view the ICT industry as an indispensable partner in such efforts and should leverage private sector expertise. Governments should evaluate previously developed international standards, such as Common Criteria, and modify these standards as required rather than create new country-specific standards. If new standards are determined to be necessary, these should be developed, approved and adopted via international standards organizations.

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

One of the most critical factors in crafting a successful solution that respects and protects the privacy and civil liberties of relevant participants in that system is to allow for some flexibility and innovation in the technical, procedural and knowledge based solutions going forward. Current law and best practices can be difficult to navigate for both public and private sector organizations, and there is no indication that successful navigation will be any simpler in the future in our highly connected, increasingly globalized communities. Accordingly, the nature of the risk to critical infrastructure is global. Thus, any system designed to protect information and infrastructures must similarly be implemented with global objectives and protections in mind and allow for modification and correction where needed to continue to demonstrate the highest levels of respect for personal and intellectual property data.

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

Truly effective cyber security helps to provide resiliency across critical infrastructure sectors, economic stability, and the reduction of the profit model currently appreciated by the criminal community. We must look at cyber security as foundational technology, as well as an economic issue of risk mitigation and investment. True resilience will require co-design of intelligent action with the hardware components that execute electronic instructions. Every network is an ecosystem that is part of the greater global ecosystem. Every component of one ecosystem should be connected to and able to communicate with others to learn and inform, just as

organisms in nature adapt to changing threats and surroundings. Network resilience is also dependent upon a global policy initiative to enable data privacy as well as combine and correlate situational awareness in real time to help drive the innovation and protect the freedoms that define our way of life.

Small- and medium-sized businesses also must be key stakeholders in and contributors to the framework. Small business comprises 99% of the business fabric in the US. These companies do not have the resources for a dedicated security staff or expensive solutions, yet have as much PII and IP to protect as their larger counterparts. A solid framework and government role needs to incentivize and enable small business to make sound cyber security investments with high ROI.

Our framework must embody the technology, policy, and market incentives to foster innovation and agility. That will improve cyber resilience across CIKR.

Additionally, the demand for security experts is greater than the supply. There is a shortage of talented computer security experts, making it difficult to protect networks and intellectual property. Cyber-ops curriculum is needed broadly across the universities to establish a security foundation. Many firms cannot afford to attract and retain cyber talent to adequately defend the company.

## Summary

While we applaud the Administration and NIST for addressing the need for a foundational cybersecurity framework for the identified Critical Infrastructure sectors, the approach is lacking in two areas critical to the connected security of the United States. Those two areas are small businesses and home users.

Small businesses often lack the resources and experience to be able to properly field and manage a secure computing infrastructure. To gauge the significance of the problem we have to consider how important small businesses are to the U.S. economy.

In total, small firms:

- Represent 99.7 percent of all employer firms
- Employ half of all private sector employees
- Pay 44 percent of total U.S. private payroll
- Generated 65 percent of net new jobs over the past 17 years
- Create more than half of the nonfarm private GDP
- Hire 43 percent of high tech workers (scientists, engineers, computer programmers, and others)
- Are 52 percent home-based and 2 percent franchises
- Made up 97.5 percent of all identified exporters and produced 31 percent of export value in FY 2008
- Produce 13 times more patents per employee than large patenting firms[1]

[1]

Furthermore, small businesses employ about half of U.S. workers. Of 120.6 million nonfarm private sector workers in 2007, small firms employed 59.9 million and large firms employed 60.7 million.[2]

For the purpose of this effort, small business should be considered a critical infrastructure component for the health of the US economy.

Additionally, the home user has been widely understood to be the soft underbelly / weakest link in Internet security in the United States. Consumers are at a worse disadvantage than even small businesses. Most consumers know little of proper computer security. They go to a big box store, buy a computer, printer, laptop and a wireless router, go home and set it up. They follow the minimal instructions, get it communicating with their service provider's broadband or DSL router and celebrate when they are able to get a web page to print. Most home users feel at that point they have done all they need to do. Default set-ups, configurations and passwords stay that way. Certain vendors help with recommending setting up the firewall and automated patch installation. Beyond that, their systems are at the mercy of those that prey on those types of environments.

Adversaries use these systems as a part of a compromised set of systems used to target advanced attacks against corporate, financial and governmental institutions in the US. Meanwhile, the end user / home owner is oblivious to the rootkits and key-loggers installed on their systems and that their personal information and bank accounts are only an attacker's focus away. This is a problem becoming more apparent and critical as we further integrate high speed broadband across the US.

The following was taken from a Department of Commerce website describing Computer and Internet Use at Home.

- As of October 2010, more than 68 percent of households used broadband Internet access service, up from 64 percent one year earlier. Approximately 80 percent of households had at least one Internet user, either at home or elsewhere.
- Cable modem (32 percent) and DSL (23 percent) ranked as the most commonly used broadband technologies. Other technologies, including mobile broadband, fiber optics, and satellite services, accounted for a small, but growing, segment of households with broadband Internet access service.
- Over three-fourths (77 percent) of households had a computer – the principal means by which households access the Internet – compared with 62 percent in 2003.[3]

As previously mentioned, we applaud the Administration's efforts to create a consistent cybersecurity framework to be used within the critical infrastructure sectors of the United States, but feel we need to go a step or two farther.

---

[2] U.S.Dept. of Commerce, Census Bureau: Statistics of U.S. Businesses, Current Population Survey and Business Dynamics Statistics; and the Edward Lowe Foundation (http://youreconomy.org).

[3] U.S. Dept of Commerce, "Exploring the Digital Nation - Computer and Internet Use at Home", November 8, 2011, http://www.esa.doc.gov/Reports/exploring-digital-nation-computer-and-internet-use-home

We need to assure that the framework created works for small businesses, as well as larger organizations and companies. We also need to create a separate standard framework and trusted best practices education resource for home users. By doing this, we will be helping to deal with the entirety of the problem, and not simply disposing of the problem to a more vulnerable landscape.