April 8, 2013

VIA EMAIL
cyberframework@nist.gov

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
(Docket No. 130208119-3119-01)

To Whom It May Concern:

Symantec appreciates the opportunity to provide comments to the National Institute of Standards and Technology (NIST) on the development of a Framework to Improve Critical Infrastructure Cybersecurity (Framework). As a global leader in providing security, storage, and systems management solutions, Symantec is committed to assuring the security, availability, and integrity of our customers' information. Today, we protect more people and businesses from more online threats than anyone in the world. We maintain eleven Security Response Centers globally and utilize over 240,000 attack sensors in more than 200 countries to track malicious activity 24 hours a day, 365 days a year. Improving the cybersecurity of our nation's critical infrastructure is essential to securing our national and economic security, and we are pleased to be able to assist NIST in developing the Framework.

The Request for Information (RFI) appropriately recognizes the importance of existing private sector cybersecurity efforts, and builds upon NIST's strong record of building public-private partnerships. Focusing on voluntary consensus-based standards and industry best practices, in particular assuring consistency with voluntary international standards, is the right approach. To be successful, the Framework must use these efforts as a starting point, not duplicate them. Moreover, it must be technology neutral - a framework that mandates any specific product or service, even indirectly, will lack the flexibility needed to be applicable to a broad cross-section of industries and organizations.

But the flexibility must go deeper than that. The reality is that while many security practices will apply to most, if not all, critical infrastructure sectors, every sector will have unique security needs. The Framework must balance the necessity to establish some baselines with the limitations that are inherent in writing such a broadly applicable document, and leave room for those gaps to be filled on a sector-by-sector basis. It is important for those who use the Framework to understand both what it is meant to be (a starting point on the road to good cybersecurity) *and* what it is not (a roadmap that leads directly to a complete security solution). This reality should be made clear throughout the Framework, not just in the preamble or introduction.

While the RFI reflects this, many of those who will look to the Framework for guidance will be experts in designing and supporting information technology (IT) systems, but may not be as well-versed in security. Indeed, it is often the case that organizations install a program for the primary purpose of meeting a

compliance mandate (whether internal or external) and then work backwards from there towards true holistic security. Other organizations do the opposite, starting with security and then determining if that solution meets compliance mandates. In the best case – which the Framework should strive to facilitate – both compliance *and* security are at the forefront of any effort to improve cybersecurity.

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?***

Good security must be proactive, not reactive. This is especially true with cybersecurity, where the threat morphs almost in real time. Implementing – and maintaining – an effective cybersecurity regime requires engagement from the very top levels of an organization. Unfortunately, this is often not the reality today – in some cases senior leadership does not appreciate the threat, in others the focus is on what must be done for regulatory or legal needs and not for the effectiveness of the program as a whole. While a good security program must take into account regulatory or legal requirements, it should not be built solely around them.

Cost too is an issue; security is often seen as a pure cost center, with little tangible value to an organization. Yet more investment does not necessarily lead to better security. So while there is often a need for more investment, the Framework should seek to drive organizations not just to spend more, but rather to make smart investment decisions based on their assessment of the risk. Finally, staffing and education is another challenge; even organizations that are focused on cybersecurity and willing to devote significant resources to it can struggle to hire the technical experts they need. A perfect framework will not succeed if we do not train a sufficient number of cybersecurity experts in the coming years.

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

A broadly applicable framework must balance ease of implementation with broad applicability, while not being so high-level that it provides little value. Achieving such a balance is not easy, particularly with sectors that have competing funding and security priorities. A cross-sector Framework runs the risk of being written for the lowest common denominator; one approach to avoid this would be to include risk-based control sets to allow for applicability from lower security sectors to higher ones.

A Framework meant to be broadly applicable could be incorrectly seen as a single, silver bullet solution, particularly by organizations less focused on security or more interested in regulatory or legal box-checking. The final Framework needs to make clear that it is just that – a Framework, to be applied and implemented differently by organizations depending on their infrastructure, threat profile, and risk tolerance.

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?

At Symantec, policies and procedures governing security risk are managed by the office of the Chief Information Security Officer (CISO) through a Policies, Standards and Guidelines (PSG) program. There is an over-arching Information Security Policy that is then broken down into a wide range of topic areas, from access control to incident management. The PSGs are approved by company leadership and disseminated across the organization.

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

Our Security Governance, Risk & Compliance unit is located within our Global Information Security group, which in turn reports up to our Chief Executive officer (CEO) through the Chief Information Officer (CIO) and the Chief Operating Officer (COO).

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

We examine risk to an asset's confidentiality, availability, and integrity. Data is subject to an information classification scheme to determine its relative value, and risk-based controls are applied progressively (i.e., higher value or riskier data is controlled more stringently). Risk assessment considers classification, probability and impact for data and assets when determining risk factors.

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

Cybersecurity risk is incorporated into our overall enterprise risk management through annual global risk assessments completed under our Corporate Risk Assurance Unit.

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

Symantec looks to a number of government and industry frameworks, including but not limited to ISO/IEC 27001, NIST Special Publication 800-53, and the Payment Card Industry Data Security Standards (PCI DSS). *See also answer to Question 1 in Section 2.*

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?

Regulatory requirements vary by sector. In addition, there are private security frameworks, such as the PCI DSS. We comply with relevant Securities and Exchange Commission reporting requirements and risk guidance, and if necessary, the myriad data breach and data security requirements adopted by the different States.

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

Our operations are dependent on the full panoply of critical infrastructure.

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

Symantec employs Inter-company Service Level Agreements between enterprise security and other business areas within the company, as well as operational availability target agreements with our Information Technology department, to ensure system availability.

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?

Symantec complies with PCI reporting requirements, which includes quarterly scan results and status, as well as an annual report on compliance. We also comply with reporting requirements under federal securities laws. Finally, when necessary, we comply with the myriad data breach and data security requirements adopted by the different States.

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

Trusted conformity assessments are important to the success of any framework. If a conformity assessment for the NIST Framework was set up so that it could satisfy multiple standards, it would be more readily accepted and implemented because of the reduced cost and burden of demonstrating compliance with a variety of standards. As such, NIST should look closely at existing and developing standards and frameworks, and develop similar assessments to the maximum extent practicable. Reliance on and reference to international efforts will also help blunt the inevitable charge that the U.S. is developing its own specific security standards.

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?

There are numerous existing standards, guidelines, and best practices that directly or indirectly address cybersecurity. Examples include:

- NIST Special Publication 800-53;
- Federal Information Processing Standard (FIPS) Publication 140-2;
- NIST's Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP);
- NIST Interagency Report (NISTIR) 7628 Guidelines for Smart Grid Cyber Security;

- Numerous publications from the Software Assurance Forum for Excellence in Code (SAFECode);
- Tools and projects through the Open Web Application Security Project (OWASP);
- International Common Criteria Schema;
- International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) Standards 27001 & 27002 (ISO/IEC 27001 and 27002);
- ISA (International Society for Automation)/IEC-62443 Standards
- Health Information Trust Alliance (HITRUST) Common Security Framework;
- IEC 80001 Application of Risk Management for IT Networks Incorporating Medical Devices:
- COBIT Business Framework for the Governance and Management of Enterprise IT;
- Vocabulary for Event Recording and Incident Sharing (VERIS); and
- The SANS Institute 20 Critical Security Controls.

Note that this is not an exclusive list, and these are provided only as exemplars; inclusion of a standard on this list should not be seen as endorsement by Symantec, or vice versa.

2. Which of these approaches apply across sectors?

The examples above define current methodologies for network environments, product development and general IT security guidance. Each of the above referenced provides key elements to be considered within any framework or security policy.

3. Which organizations use these approaches?

Many organizations, including Symantec, utilize various components from each approach. Which elements and how they are utilized is driven more by the organization and its needs than it is by the approach itself. How and when a particular approach may be used is also driven by the evolving threat environment – what is right for today may not address the needs of tomorrow.

Security product development organizations may not include elements of each approach into the products they deliver; however the developmental process must be monitored by specific approaches. Though originally defined for government agencies, standards such as FIPS 140-2 have proven to be highly relevant for commercial uses, including in the financial, healthcare and payment card industries. Of course, encryption for any personally identifiable information (PII), intellectual property (IP), source code, trade secret or critical infrastructure-related information is critical.

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

The main limitation is that these approaches – and the disparate application of the approaches across various organizations and sectors – often lead to gaps within a comprehensive IT security framework. In addition, many approaches do not provide a clear path to maturity. There is no one-size-fits-all solution, and often gaps between inter-locked approaches/organizations can create confusion and areas of vulnerability. Finally, many current approaches are device-centric, not information-centric. Good cybersecurity requires a defense in depth, one that protects data in transit and at rest, and that is tailored both to an organization's infrastructure and to the threats it faces. As such, any framework or standard must be viewed through that lens and adapted to the unique circumstances in which it will be applied.

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

A complete Framework will consider the end-to-end path for information flow and ensure that there is no "weak link" in the chain. Typically, this means utilizing a defense in depth approach, whereby

appropriate security is applied depending on the link of the chain being protected, whether data centers, networks, industrial control system devices, or commercial off the shelf (COTS) IT systems.

Creating a tiered approach is often useful – create an initial target set of controls and then an organization can iteratively expand to an increased set of controls according to its needs. To the extent possible, a good approach will include some details on how to meet the requirements set forth, rather than just describing a desired end state. However, details of the "how" should not be so restrictive as to limit the inherent flexibility of an approach.

Indeed, the best approaches recognize the need for flexibility both operationally and in implementation, and build that in from the outset. Collaboration and partnership with industry is also essential, for two reasons: first, the ideal solution is developed with the full breadth of industry expertise; and second, organizations will be more willing to implement a solution that they assisted in developing.

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

The answer varies with the approach. Some existing standards have attempted to reach sector-specific needs, while others are more general in design. However, as with higher level approaches, sector-specific approaches must be flexible because even within a specific sector, the application of a security approach will vary greatly from company to company.

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

In an ideal world, sector-specific standards development is the best approach. However, even such an "ideal" sector-specific approach must take into account not just IT concerns, but also cross-sector considerations.

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

Sector-Specific Agencies and Sector Coordinating Councils (SCCs) have unique perspectives on their particular sector and the regulatory and standards framework that exist across it. As such, they should be involved in the Framework effort from its beginning. In particular, the SCCs are able to offer a sector-wide perspective on different approaches and methodologies that is vital to the process. NIST would be well-served by engaging with SCCs and to use them as a resource throughout the process. In addition, the Government Coordinating Councils (GCC), not solely the SSAs, should be engaged for their cross-government perspectives and relationships and roles with critical infrastructure entities.

9. What other outreach efforts would be helpful?

See answer to Question 8 in this Section. NIST has a long and productive history of working collaboratively with industry and others, and should continue that practice with the Framework by seeking input from across the public and private sector, as well as from academia.

Specific Industry Practices

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?

Specific practices vary among sectors, and within sectors they differ from company to company. As a general matter, those organizations that do have effective security programs use all of the identified practices, adapted to meet their specific needs and risk tolerance.

Unfortunately security is still often secondary to the strict requirements for reliability, uptime and performance. It is frequently viewed more as insurance against attacks that may or may not occur rather than as an enabler for core business functions. This mindset is beginning to change, however, and the Framework can be a part of accelerating that important shift in attitudes.

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

In general, many security practices are implemented consistent with the relevant portions of one or more frameworks or standards, most of which have international application either by design or in practice. NIST standards in particular are widely viewed as useful reference points internationally. In addition, work by the German Federal Office for Information Security Agency is generally compatible with US and other international efforts, and often offers good security guidance.

Of course, as noted above, no single standard or practice should, or even can, be applied as written to provide effective security to an organization. Instead, standards and practices must be constantly adapted to protect against the anticipated threats and to secure a particular system or systems.

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

While individual security needs are specific to each application, identification and authorization of users and monitoring capabilities are a threshold security need for almost any organization. Similarly, encryption and key management is essential, whether an organization is storing PII, IP, manufacturing processes, or other trade secrets. Other practices may vary in importance depending on the critical infrastructure at issue; for instance, in a sector that relies on supervisory control and data acquisition (SCADA) and/or industrial control systems, separation of business and operational systems is more relevant than in some other sectors. The level of mission and system resiliency needed will vary from operation to operation, and can depend on an organization's risk threshold.

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

See answer to Question 3 in this section.

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

The ease with which a particular practice can be implemented is driven by too many variables to answer broadly – it will vary by sector, organization, system, and application. *See also answer to Question 3 in this section.*

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

See answer to Question 3 in this Section, Question 7 in Section 1, and Questions 3-5 in Section 2.

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

Symantec has a methodology in place to assess our risk and allocate resources, and to do so on an ongoing basis. Most organizations that operate or own critical infrastructure do as well, but the sophistication of the analysis and the extent to which it drives investment will vary from one to another.

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

Symantec has a process in place to recognize, respond to, and mitigate cybersecurity risks. Many organizations have similar processes in place, but they vary in sophistication from one to another.

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

For a discussion of the importance of privacy and security, see answer to Question 11 below.

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

As a global company, we conduct business around the world. As more countries consider adopting security policies or frameworks, the U.S. must lead the way in demonstrating that good security practices and standards are not bound by borders. As such, it is essential that the NIST Framework reflect international norms and standards, and that it cannot in any way be portrayed as a US-centric or US-specific security standard. Anything else could provide a rationale for other nations to adopt inflexible, indigenous "security" standards that are incompatible with international norms and that are often covert efforts to limit the access of U.S. IT vendors into their markets.

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

This question seems to presuppose that a strong cybersecurity program would necessarily infringe on privacy. This could not be further from the truth - implementing a strong cybersecurity program is an essential first step toward *protecting* privacy and civil liberties. Privacy and security are not in conflict; if someone's data is not secure, then neither is his or her privacy. Any data that a company holds – whether PII or trade secrets – must be protected by a layered defense, including but not limited to access controls, monitoring, and data encryption. If the NIST Framework leads to more secure systems and data, it will by its very nature improve privacy and protect civil liberties, because it will limit breaches, intrusions, and loss of data.

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

As NIST recognizes, the Framework should start with voluntary consensus standards and industry best practices, not duplicate them. Moreover, it must be technology neutral; a framework that mandates any specific product or service will lack the flexibility needed to be applicable to a broad cross-section of industries and organizations. Finally, the Framework should balance the necessity to establish some baselines with the limitations that are inherent in writing such a broadly applicable document, and leave room for those gaps to be filled on a sector-by-sector basis. The organizations that use the Framework need to see it as a starting point, not a complete solution.

* * *

Symantec thanks you for the opportunity to provide this input, and to assist in the development of the Framework. We look forward to working with you throughout this process. Please do not hesitate to contact us if you need additional information or if we can be of further assistance.

Sincerely,

Cheri F. McGuire
Vice President
Global Government Affairs & Cybersecurity Policy