Response to Information for:
Developing a Framework to Improve
Critical Infrastructure Cybersecurity
Docket Number 130208119-3119-01

Submitted to:
National Institute of Standards and Technology
U.S. Department of Commerce

Date:
April 8, 2013

Government Markets Group



Level 3 COMMUNICATIONS

Table of Contents

Transmittal Letter

April 8, 2013

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

RE: Request for Information for Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Sir or Madam:

Level 3 Communications is pleased to present this response to your Request for Information in support of Developing a Framework to Improve Critical Infrastructure Cybersecurity.

Our RFI provides information in response the the questions asked by NIST as to our experience in protecting our customers information against cybersecurity threats and our recommendations to enhancing the implementation of future cybersecurity components across national critical infrastructure industries.

We would welcome the opportunity to support NIST as it moves forward with the definition of a new framework to protect the assets of our country and our customers.

Sincerely,

Dale Drew
SVP Chief Security Officer
Level 3 Communications, LLC

1.0 RFI Response

1.1 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?**

Response:
Level 3 is a global telecommunications provider that provides a wide variety of networking and application services, across a wide variety of vendor solutions. This provides us with a unique perspective in operating large, global, complex networks across a wide variety of vendor platforms.

We believe that the greatest challenges to improving cybersecurity practices largely revolve around two major principal issues: 1) advanced cybersecurity research that focus on approaches around cyber threat mitigation, and 2) vendor adoption of industry standard security models.

"Advanced cybersecurity research that focus on approaches around cyber threat mitigation"
Specifically, we believe that more cybersecurity research is needed to develop methodologies and technologies for some critical industry wide challenges, including:

- Zero day prevention and detection
- Security software testing practices
- Distributed Denial of Service Application attack mitigation
- Network based Botnet indicators and algorithms

"Vendor adoption of industry standard security models."
In addition, we also believe that initiatives to motivate vendors to more uniformly adopt vulnerability and log data categorization, reporting and detection automation ecosystems will be a significant step in ensuring security tools can better detect, report and repair security vulnerabilities.

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

Response:
Level 3 believes that the best approach to developing cross-sector standards relies on consistency in security ecosystem approaches.

Adoption of security automation protocols such as CVE and OVAL (and CVSS, XCCDF, etc.) ,other protocols such as CCI or CMSS (for configuration related automation) ,CAPEC and SWSS (for software assurance automation) and CVRF (for reporting related automation) are key to building consistency in vendor solutions that allow a more refined security maturity model that can be normalized across sectors.

Inconsistency in vendor security model approaches, or complete lack of, requires the industry to customize and invent their own implementation solutions, if they have the capacity to even do so.

This causes a breakdown of security in the supply chain for providing and implementing security controls for deployed technology, making "standards" much different in implementation depending upon the maturity of the vendor platform being deployed and adopted.

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?**

Response:
Level 3 utilizes ISO 27001:2005 and NIST 800-53 (MODERATE) as its security policy baseline across its global infrastructure and utilizes NIST 800-30 as its framework methodology for conducting risk assessments within its ecosystem.

Level 3 inventories and audits its infrastructure, systems, and products on a daily basis to identify changes, alterations or modifications to that infrastructure that could cause unforeseen risks, or are in direct violation of established policy that has or can cause a risk or vulnerability.

Risks and vulnerabilities are categorized by severity level relating to the impact that the risk or vulnerability would have to the business if not properly mitigated.

Corrective action is suggested and when not possible, a risk or policy exception is requested. All exceptions are reviewed by the Security Compliance organization to identify mitigating controls and evaluate the impact to security policy.

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

Response:
Level 3 operates a centralized security organization, providing a holistic view of the threat landscape and attack ecosystem. Level 3 is fairly unique in its sector in that it combines its security disciplines vertically to address enterprise security, product security, managed security, production security, and management security; as well as horizontally to address policy, risk assessment, architecture, engineering, operations, compliance and investigations. This security capability addresses both physical and cybersecurity concerns of the company.

This unique structure gives Level 3 full visibility into the ecosystem of an attack, allows for consistent methodology in protecting its critical assets, and allows for real time monitoring of all aspects of the ecosystem.

Level 3 places its global security organization under the Global Technology Office, which has oversight for all of its technology decisions and directions. As a technology company, it is critical that security have first line of sight of security risks relating to technology and business decisions.

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

Response:
We define risk by anything that impacts the integrity and availability of the services we provide to our customers.

Level 3 maintains a compliance organization that is responsible for providing a holistic view of both physical and cybersecurity risk calculations that effect the operation of the company.
Level 3 utilizes NIST 800-30 as a general guideline in reviewing risks. This risk methodology encompasses the following areas:

- The Level 3 security architecture
- Level 3 products and services
- Level 3 applications and data flows within its products and services
- The Level 3 back-office environment
- Specific projects and requests within the above categories not within current policy or practice

This approach allows us to maintain a view of the entire landscape, while at the same time testing the effectiveness of our control framework through individual and specific projects and initiatives.
To ensure effectiveness of its Security program and validity of its risk assessment process, Level 3 takes the following steps:

- Conducts an audit of all employee and production systems every 24 hours to validate systems against security policy,

- Conducts self-assessments monthly through a RED TEAM approach that tests the effectiveness of specific controls and processes.
- Measures our security controls through 60 detailed metrics which are reviewed monthly
- Conducts quarterly internal audits via the compliance team to test specific areas of control,
- Conducts bi-annual audits through an independent, but internal, Internal Audit organization,
- Conducts annual audits by third parties to test against PCI-DSS, SASE16, FISMA Moderate, FISMA Low, NISPOM, PSN CAS(T), and external pen testing.

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

Response:
Level 3 offers global telecommunication services to some of the world largest production environments and enterprise networks. Our security model must be incorporated into everything we do from a cultural and network/product design perspective, to ensure the most reliable and secure environment to our customers.

Level 3 maintains an Enterprise Risk Council comprised of several critical internal functions at the individual contributor and executive level that focus on company-wide risks by reviewing roadmap initiatives, major projects, and new risks and threats to ensure we have continuous capability to identify threats to the Level 3 asset portfolio.

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

Response:
Level 3's security policy architecture is based on ISO27001:2005 with additional controls from NIST-800 53A (Moderate). In addition, Level 3 is certified for PCI-DSS, PSN CAS(T), NISPOM, and SSAE16 and incorporates many of those policy requirements into its corporate security model.
In addition, Level 3 utilizes DoD STIGs for its configuration baselines.

Level 3 utilizes a wide variety of commercial and open source tools to protect its infrastructure. Level 3 operates a highly diverse vendor environment with a very complex global presence and as such, many of the security tool needs we have are not commercially available. As such, Level 3 also develops a number of the tools and infrastructure it needs to protect its network and maintains a dedicated engineering organization.

Many of the commercial and open source security tools that companies like Level 3 rely on for security capability do not uniformly conform to standard security models; such as CVSS and CVE or OVAL. As such, Level 3 must, develop, implement and maintain much of this capability itself, which is a significant distraction from its threat management objective. A consistent standards based security ecosystem model absolutely needs to be developed to solve for this issue.

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?**

Response:
Level 3 participates in several compulsory regulatory reporting requirements; each with their unique cybersecurity standards, reporting formats, reporting frequency and auditing demands. A significant amount of time and effort is spent on these efforts, which could be spent protecting the network via a single, holistic security framework model with a consistent vulnerability and incident management approach.

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

Response:

Level 3 is a Global Telecommunications provider that has a high reliance on the energy and transportation Sectors to be successful.

With over a million square feet of datacenter space, Level 3 consumes large amounts of high capacity energy in providing those services to customers. In addition, Level 3 relies on a highly consistent, very reliable transportation sector to ensure its network assets are delivered to key, critical constraint locations as quickly as possible to deliver services to customers.

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

Response:
Level 3 utilizes security governance metrics to measure the effectiveness of its security program while ensuring we remain highly adaptable and flexible as a business.

Our objective is to ensure we deliver service within specific service intervals that incorporate resiliency, reliability, security, and product performance characteristics.

This service delivery metric is measured to ensure all of the critical aspects of product delivery are properly working and in tune with delivering business needs quickly.

When there is an impact to our service delivery metric, which is attributed to a security issue, a root cause analysis is performed to ensure we understand what element drove the delay; always with a focus on ensuring the security organization is tightly integrated into the key, critical pieces of the business to be able to perform its risk assessment quickly and develop and implement the necessary controls as part of that service delivery.

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?**

Response:
Level 3 maintains reporting relationships with several state and federal regulatory bodies in reporting security related issues. Generally, Level 3 is required to provide a copy of its security architecture approach, answers to specific security control questions, and in some cases, submit to a third party audit with the audit results being provided.

Each regulatory body has different reporting requirements, frequency intervals, levels of detail required and different security standards to abide by. In practice, far more resources are put into Program Managing these reporting relationships, than we spend in protecting the actual infrastructure; taking valuable capability away from the ability to better protect infrastructure.

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

Response:
Level 3 believes that significant benefit could be achieved if more focus was spent on hardware and software vendor standards and certifications. This would help ensure the introduction of more secure products and product capabilities as well as more standardized vulnerability and incident reporting capabilities.

We also believe there is tremendous value in a voluntary compliance and reporting program that allows companies and vendors to be assessed to specific standards and be able to have an industry reporting site that reflects; participation in those recommended standards and their current certification level or pass/fail status. This will help push adoption of the standards within the industry and within cross-sector supply chains.

1.2 Use of Frameworks, Standards, Guidelines, and Best Practices

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

Response:
Level 3 believes there is no shortage of frameworks and standards for the industry; we believe there is tremendous value in collapsing these standards and frameworks to reduce the certification impact on companies while still maintaining high levels of security controls.

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

Response:
Level 3 utilizes FISMA and ISO27001 as its standards framework and requires its vendors to follow many of these requirements when delivering solutions or capabilities.

However, today there are no standards that easily track through the supply chain to validate the capability of a solution being utilized in the industry.

3. **Which organizations use these approaches?**

Response:
Level 3 can only speak to its use of and experiences with approaches. We do ask our supply chain vendors to adhere to a number of security practices that tend to be a blend of many of the approaches, to find the right balance between identifying vendors with mature security frameworks, but whom are adaptable to threats.

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

Response:
Excessive documentation, reporting, reporting formats tend to be big limitations regarding the execution of security framework models. However, the single largest limitation is that the approaches tend to not focus on the suppliers of technology and capability, but rather the ones whom have built services on such technology.

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

Response:
We believe that standards frameworks should be more ecosystem focused, i.e. identifying standards, processes, guidelines and best practices for each step in the ecosystem and supply chain.

Specifically, we believe that standards need more focus in the following areas;

- Suppliers of technology
- Reporting of compliance
- Ecosystem approach
- Standardization of vulnerability data and logging infrastructure
- Research arms into new detection and mitigation techniques
- Reporting and information sharing on new attacks, risks, etc.

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

Response:
By focusing on the supply chain and the ecosystem as a whole, sectors will have better capability to introduce new capability into their portfolio with a level of assurance from a security perspective.

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

Response:
If an existing framework is utilized as the sector-specific cyber security framework or baseline, it can be

expected that a 'one size fits all' objective will not be feasible. Additional sector-specific components would need to be developed and adopted. The various sector-specific ISAC groups should provide the in-sector feedback loop for any sector-specific security components. ISAC groups should also be the cross-sector information conduit between sectors

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

Response:
We believe that the creation, communication, adoption and requirement of an ecosystem based standards process that cuts across the entire supply chain of technology will be a significant step forward in standards adoption that naturally encourages development of sector and technology specific requirements and allows security related vendors to focus on core technology solutions.

Sector specific agencies and related coordinating councils can assist by promoting the adoption of this Ecosystem framework as part of their purchasing requirements.

9. **What other outreach efforts would be helpful?**

Response:
We believe that agencies can push technology innovation by fostering and sponsoring technology challenge RFIs within the industry to identify cutting edge solutions and capabilities and determining how those solutions can evolve into an Ecosystem Framework.

1.3 Specific Industry Practices

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

Response:
Yes. For the telecommunications industry, many of these approaches are in place today.

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

Response:
Level 3 utilizes FISMA and ISO, but much effort is focused on "mitigating" capability when specific solutions, capability or technology is unable to meet the standard. This creates inconsistency in application from company to company and sector to sector.

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

Response:
Level 3 believes that several standards and technology solutions exist today that provide the most critical elements to uniform and holistic cybersecurity;

- The development and use of a vulnerability inventory standard; CVE, CPE
- The development and use of a vulnerability rating system; CVSS / Oval / XCCDF
- The development and use of an incident/logging reporting system; SCAP

We also believe much more work needs to be done in the incident logging reporting standards to institutionalize the way in which network, system, application and data log files are represented, analyzed and reported for security exposures.

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

Response:
Often times, customers of technology solutions require sector adaptation of standards where they may not be best suited; which ultimately requires those providers to "stack" multiple compliance requirements that "bog" down the security control framework. For example, the financial sector requires SSAE16 and/or PCIDSS requirements, which are completely separate standard frameworks.

Level 3 believes that an ecosystem approach would allow for a single "core" security control framework, with sector specific requirements (spurs) that would minimize the burden of having to maintain several dozen, competing standards requirements.

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

Response:
The lack of an ecosystem standard means that there are varying degrees of automation capability in assessing risk, performing assessments of vulnerabilities and monitoring for exposures as part of a mature continuous monitoring program. In fact, the most significant failing of the standards process is the lack of automation and vendor consistency which requires significant amounts of manual effort and intervention, to several dozen different standards bodies, all whom require different reporting formats and mitigation requirements.

This manual process ultimately erodes the value that the standard was meant to serve; it causes a lack of adaptability to new threats, uniform adoption of counters to those threats, and consistent applicability of the standard. Implementers end up limiting their focus on serving the Program Management elements of the standard, rather than addressing the true risk mitigation the standard was intended to provide.

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

Response:
Level 3 utilizes a combination of NIST 800-53 and ISO 27001:2005 with a dedicated engineering team to attempt to provide a degree of risk, vulnerability inventory and detection, and effectiveness measurement consistency.

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

Response:
As a global telecommunications provider to several critical infrastructure components, Level 3 takes security very seriously. Security is part of the culture of its business and the company has worked hard to implement consistent security practices from the ground to the cloud across its entire service portfolio.

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

Response:
Level 3 maintains several global security operations centers that monitor the security of Level 3's infrastructure on a continuous, real time basis. In addition, we audit our entire production infrastructure every 24 hours to identify new threats and exposures. Level 3 has a formal process for identifying new exposures and escalating their corrective actions as appropriate, via the implementation of the Level 3 Computer Emergency Response Team (CERT).

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

Response:
Level 3 operates a shared technology platform. Providing exposure information to customers, regulators, and sector agencies tends to put that information more at risk from disclosure and abuse.

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

Response:
Level 3 operates a global security organization and we work to implement security practices and standards globally.

Data and PII security concerns continue to be a significant challenge as they differ from country to country and often region to region or state to state; requiring different personnel, reporting and

governance controls over data and PII security.

We often have to regionalize data, which requires additional personnel, support, infrastructure and costs that ultimately increase the cost of doing business.

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

Response:
Standards need to globalized across the entire ecosystem to ensure there is consistency in application and approach.

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

Response:
Level 3 believes that a global ecosystem framework that focuses on the supply chain of technology solutions is a key, critical element to maturing our standards framework that will bring the consistency across sectors necessary for us to be adaptable, flexible in the reporting, inventory, categorization and mitigation of risks.