System 1, Inc.

April 8, 2013

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

Subject: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt,

System 1, Inc. is pleased to submit our comments to the Request for Information RFI. System 1 is small business specializing in cybersecurity, critical infrastructure, and governance. We have a broad constituency in cybersecurity sand infrastructure protection across the Federal Government supporting approximately 40 organizations, including national laboratories. System 1's experience expands to the state and local level where we have supported the development of multi-state regional infrastructure protection plans. In addition, in the area of cloud architecture we are a certified third party independent assessor (3PAO) under the General Service Administration's FedRAMP program (we teamed with another organization and submitted a joint application). System 1 also supports major telecom providers as well as industry IT suppliers to the Government.

System 1 is responding to the questions posed in the RFI below. We have answered a subset of the questions. Some of our responses provide a broad perspective that we have seen across the Federal Government.

Current Management Practices

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

   Top-level management often perceives cyber security as a compliance exercise and does not perceive real value in its implementation. They see no or little tangible return on their investment and are resistant to reassign resources from accomplishing their business goals to support cybersecurity. Top level management needs to be educated as to the real risks to their enterprise and how they are evolving.

   A second issue is seamlessly incorporating cybersecurity as a cornerstone of good operations. It needs to be integrated into all levels of work. It cannot be "bolted" on as a process. Middle management is largely responsible for taking executive direction and incorporating it into how they achieve their outcome. In many cases because the return cybersecurity investment is not clearly visible, cyber and critical infrastructure are not weighed as a high priority.

A third issue is that as IT is moved into the cloud, security control is delegated to the cloud suppliers. In some cases it lacks transparency and we have "released control" over critical assets to a third party. In addition when clouds are independent and are stacked, for example multiple Software as a Service clouds riding on an Infrastructure as a Service cloud, how is the composite risk defined or determined?

The fourth issue is that cyber and infrastructure protection are not checklist based or strictly compliance based processes. The challenges from a cyber perspective rapidly evolve over time and we deal with issues like advanced persistent threat for which there is no simple mitigation. Cybersecurity requires a body of "thinking" personnel because the technology, vulnerabilities and threats change rapidly. Cyber hygiene, the implementation of approaches to mitigate common or uni-dimensional threats, significantly reduces the risk, but the threats to high value targets are difficult to defend against.

A fifth issue is that when cyber security is risk based it is no longer one size fits all but is tailored to a sector's context (for example, mission, environment, threat, and vulnerabilities). Determining the organizational risk tolerance is key to implementing a risk based approach. Risk tolerance needs to be characterized and communicated by sector leadership and then cascaded down to the organizations within that sector.

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

If the organizations use a set of standards to protect across an industry, for example FISMA/NIST for the Federal Government or NRC/NERC for nuclear power plants, then each of the sectors should be on a level playing field. Adopting different frameworks across different sectors may be acceptable if the controls are tailored to that sector or industry.

The most effective way to implement cybersecurity standards is to pick one for the entre sector and then all participants use the same standard. This will lead to some degree of tailoring, making the implementation and the assessment processes more uniform and cost effective.

An implementation challenge is that once a standard is agreed upon it is used to measure performance with the expectation that everyone will be rise to a satisfactory level – however by definition very few organization will be compliant with a new standard. Where organizations are not compliant with the standard, there are often efforts to reinterpret the standard to "water it down".

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?

Often senior management does not know how to approach cyber risk. The NIST 800 series are commonly used across the Federal Government to provide a risk based framework and approach. Implementation at the organization level is based on NIST. Governance is tailored to risk framework at the organizational, mission, and system level and used to determine risk tolerance. Risk tolerance is often difficult to define where

intellectual property or privacy is at play. Often risk can be easier to be defined at the programmatic, operational or business unit level since it is easier to define how risk affects their enterprise.

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

The risk framework and risk tolerance on an organization basis is usually determined at an executive level, typically at the Undersecretary level within the Federal government. Implementation typically is delegated to the Chief Information Officer's organization. In some private sector organizations, cybersecurity risk has been promoted to the Board of Directors level, but mitigating a response is usually at the level of the Senior Risk Manager or Chief Information Officer.

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

This has always been a thorny issue. There has been a great deal of subjectiveness or "cyber theater" associated with characterizing cyber risk. Some organizations that we have worked with have developed systematic metrics and approaches for defining and assessing cyber risk by evaluating threat actors and other factors.

At a technical level, risk is tied to their perception of mission impact should the system fail or be unavailable. However this assessment is done at the mission essential function level which has a more narrow focus of functions that are considered critical than the lower level operational staff (who think their systems are always mission essential).

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

Rarely is cybersecurity risk fully incorporated into an organizations risk management strategy. Much of that depends on corporate culture and whether cyber is viewed as a technology issue or a boarder issue relating to the intrinsic value of the information that the organization produces. It varies based on leadership, internal and external requirements, mission, environment, and recognized threats.

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

There are a number of workable risk management frameworks use for cybersecurity. Frameworks range from NIST, ISO, COBIT, to industry specific sets of criteria such as DOE's risk roadmap, NRC's guides or NERC requirements for nuclear plants. There are a wide variety standards or frameworks that can be adapted or tailored but identifying and communicating risk tolerance within a specific sector is key. Insider threat has been shown to be a significant risk by some estimates as much as 50% of the cyber risk. Many of these standards do not adequately address insider threat.

There are a number of dashboards like NIST's PRISMA tool to commercial dashboards from private sector companies including Telos and IBM (Q1 Labs).

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?

Most of the current reporting requirements in the Federal Government revolve around DHS's Cyberscope and incident management through USCERT. These are driven by various laws such as FISMA and state privacy breech laws, regulatory guidance such as OMB memorandum, bulletins, and circulars, NRC regulatory guides, and organizations standards.

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

There are some interdependencies that are readily apparent for example, aviation, healthcare and finance are heavily dependent on the communications infrastructure. Agriculture is dependent on the water supply system and transportation systems. Most critical assets are dependent on the electrical and communications grid.

There has been a methodology incorporating interdependency analysis developed and implemented for the identification or critical physical and cyber assets. The resulting list of critical infrastructure and key resources created are protected at an enhanced level due to their sensitivity.

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

In almost every major strategic plan risk management is a major tenet. There are risk-based frameworks, Continuity of Operations and Continuity of Government requirements and plans from a PDD, HSPD, and NIST perceptive plus annual testing. These requirements and frameworks drive organizational behavior in response to managing cybersecurity risk. The organizational definition of risk tolerance has been loosely defined along with prioritization of risk reduction activities. This means there may be a wide variation in the way that cyber assets are protected across a single enterprise.

In the Federal Government, the focused requirements from HSPD-7, which superseded the requirements in PDD-63, are enforced through OMB, but enforcement and monitoring has decreased.

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

It is necessary for a sector to use a uniform set of cybersecurity standards within a mission area. There are parallel sets of standards previously identified and mentioned in our response. Some of the organizations developing these standards may play a role in assessing performance. They could also act as accreditation bodies to ensure assessors meet certain minimum qualifications.

Use of Frameworks, Standards, Guidelines, and Best Practices

This area addresses a number of questions like; what additional approaches already exist or which organizations use these approaches? Instead of responding directly to these questions since we have confidentiality agreements and non-disclosure with our clients however we suggest the process below:

Our emphasis is on the NIST standards and guidance. These could be used but when assembled due the complexity, their large number, and size, if an organization does not have detailed knowledge of how they work and can be implemented, the effort can appear daunting.

We suggest that NIST work with government and industry to identify good practices and then identify some implementation patterns that can be communicated across the sector and potentially other sectors. Training should be structured around good practices, templates and examples. It should be set up so that the implementing organization can have access to this information. We also suggested that teams be established to help facilitate uniform implementation across the Government. Whenever possible, leverage sector specific good practices that already exist within organizations.

Specific Industry Practices

System 1 will be able to provide more detail in these areas as the working group's effort is initiated. One current example that we have been working on is a multi-year cybersecurity transformation effort. This is being developed into a NISTIR, a Government-wide good practice. Ultimately implementation of this model will lead to cultural change and the incorporation of security through all aspects of the mission and throughout all life cycle stages. The flexibility of this approach incorporates elements that can be used in the cloud, mobile devices, and supports the notion of "secure access to information, anywhere, at anytime".

Agency management approved the approach to build and implement an agile cybersecurity program. This will eliminate thousands of pages of unnecessary documentation, create a move from "security shelf ware" to dynamic risk evaluation and authorization, and ultimately result in lower costs. Some of these approaches include:

- Risk based governance – A new security policy/plan was developed with a new Governance document (incorporating elements of NIST SP 800-39). These documents realign roles and responsibilities to make decisions more agile and risk based. The approach encourages the mission owners to assess and acknowledge risk in their normal course of business. The new governance process increases the ability to make risk based decisions.

- Streamlined processes – The approach has resulted in a number of streamlined processes and approaches. The current process of authorizing systems every three years will be replaced by authorizing systems once and continuously monitoring. This results in the documentation only being updated as needed, saving time and money (NIST SP 800-37). Also, an information repository with security information will be created to support transparency and open government.

- Consolidated and simplified cyber architectures – There were over 100 systems. The new cyber architecture leverages concepts in NIST to allow the construction of "system of systems" or enclaves in agency lingo. This has reduced the number of enclaves to about 15 and in turn reduces the administrative burden. This reduces complexity and cost since new systems or tools may be "dropped" into enclaves with predefined sets of controls. It is then up to the system and enclave owner to make sure that all the necessary controls are enveloped, controls for the enclave are modified, or new controls are deployed.

- Continuous Monitoring – The key to maintaining enclave and system authorization is continuous monitoring. Many agencies are in the process of implementing the elements of a program stemming from NIST (NIST SP 800-137). The agency is implementing a dynamic model to identify new threats, assess their impact, and implement changes to controls/protective measures to mitigate their effects on a near real time basis. These changes can be assessed against the risk baseline established within the authorization package.

- Movement to commercial data centers and the cloud – National policy is to reduce the number of Federal and duplicative data centers to reduce costs. There are efforts to move current data centers to collocated sites in commercial centers and to leverage cloud technology. Agencies have identified lessons learned and approaches to increase cybersecurity during transition to the cloud. They have also has developed cloud procurement requirements, as well as processes that leverage external efforts such as GSA's FedRAMP process, and a process to evaluate the security of different classes of clouds.

System 1 looks forward to providing input into this important effort. If you have any comments or questions, please feel free to contact me at (301)792-4581 or jabeles@syst1.com.

Sincerely,

John

John M. Abeles
President and CEO