DEVELOPING A FRAMEWORK TO IMPROVE CRITICAL INFRASTRUCTURE CYBERSECURITY

In Response To:
National Institute of Standards and Technology
U.S. Department of Commerce
Request for Information
Docket Number: 130208119–3119–01

Prepared By:
The SI Organization, Inc.
15052 Conference Center Drive
Chantilly, VA 20151

Technical Point of Contact:
Thomas B. Ruffner
Systems Engineering Asc Mgr
The SI Organization, Inc.
720 Vandenburg Road
King of Prussia, PA 19406
Phone: (484) 681-7995
FAX: (484) 687-6294
Email: thomas.b.ruffner@thesiorg.com

Contracts Point of Contact:
Nicholas R. Cramutola
Contracts Negotiator Sr Stf
The SI Organization, Inc.
720 Vandenburg Road
King of Prussia, PA 19406
Phone: (484) 681-7276
FAX: (484) 687-6294
Email: nicholas.r.cramutola@thesiorg.com

08 April 2013

1.0 INTRODUCTION

The SI Organization, Inc. (the SI) is pleased to present our response to NIST's Developing a Framework to Improve Critical Infrastructure Cybersecurity RFI. Following are the SI's insights based upon the SI's experience dealing with standards, methodologies, procedures, and processes used by existing security frameworks, followed by responses to the specific questions in the RFI.

Perspective

There are several security frameworks available that provide guidance on different categories of security such as: checklists, governance, risk management, security engineering, and audit/assurance. However, there is no overarching framework that includes all of these categories which we consider common to all critical infrastructure sectors. Some of the more prevalent security frameworks are defined and maintained by the following standards development organizations: NIST, The Health Information Trust Alliance (HITRUST), The International Organization for Standardization and International Electrotechnical Commission (ISO/IEC), The framework standards for IT management, Control Objectives for Information and related Technology (COBIT), Committee of Sponsoring Organizations of the Treadway Commission (COSO), and Payment Card Industry Data Security Standards (PCIDSS or PCI). The Energy Sector also relies on a multitude of control system security standards from the Institute of Electrical and Electronics Engineers (IEEE), the North American Electric Reliability Corporation (NERC), and the American Petroleum Institute (API), among others.

To reduce risks to critical infrastructure, the Cybersecurity Framework should consider all security framework categories, including checklists, governance, risk management, security engineering, and audit/assurance. The best fit and best practice security concepts and capabilities that these frameworks provide could be merged and consolidated or at least evaluated for consistency and best practice emulation.

Our organization believes critical infrastructure can be categorized into three distinct areas that are vulnerable to a cybersecurity attack. The first area is the business infrastructure and IT systems that support the execution of day to day business operations. A successful cybersecurity attack against the IT systems may result in disruptions of business operations but would not likely impact the operation of the entire infrastructure. The second area is end-user devices for the industrial control systems. A cybersecurity attack against the end-user devices may result in skimming of services or minor financial impacts but likely would not impact the operation of the entire infrastructure. The third area is the control systems (for example, SCADA systems) against which a successful cybersecurity attack could cause a catastrophic failure. These control systems pose the most critical risks

Existing Framework Issues

A significant challenge with existing frameworks is that business concepts and security topics are treated separately and are not related in a way that allows business leaders to understand the benefits of technical solutions or technologists to understand the business processes that they are helping to enable. Security frameworks are often vague in defining specific artifacts or products that span the boundaries between business objectives and technical implementations. Framework artifacts need to clearly show a specific purpose, needed fidelity, relevant importance, interdependencies, and a clear value to the enterprise. The latter is perhaps the most important and

most difficult to present in tangible terms to decision makers who must ultimately provide funding and other support to implement and maintain a framework. Framework products and their relationships need to provide useful information to all business entities that benefit from the framework. The value of the Framework should be evident to all entities and stakeholders that utilize and support it to enable their business capabilities and ensure the success of their missions.

Desired Attributes

We believe the Cybersecurity Framework should clearly define a list of products/artifacts and also define the relationships between them. The Framework should promote traceability and relevance between the products/artifacts. The products should both facilitate and benefit from Configuration Management (CM) practices and be specific enough to allow a future tool-assisted Framework implementation. This is not to say that a specific tool needs to be used in the development of the Framework products. The Framework should stand on its own merits. However, if the Framework is developed with enough attention to quantitative and tangible constructs, such that a tool could be developed for the Framework implementation, then the Framework's usefulness will greatly be enhanced by having that level of quantification. A future tool can also facilitate the creation of reports, diagrams, and other artifacts, which promote usability and value to all cybersecurity stakeholders in the enterprise.

At a high level, the Cybersecurity Framework should have the following attributes:

- The Framework should provide an organization of related security elements that include operational activities and supporting system services/functions which may have both logical and physical components. These components should align to business policies, rules, requirements, and mission capability.
- All security elements should demonstrate their relationships to each other, the environment, business needs, security requirements, standards, and quantifiable risk assessment data, which govern cybersecurity development, implementation, and evolution.
- The Framework should provide a holistic view of the security controls relevant to defined security needs.
- The Framework should allow implementers to demonstrate how security controls are adequate for meeting the underlying requirements and identified risks.
- The Framework should provide artifacts that help identify gaps in requirements, risks, and other operational and system areas, to include areas that are not being adequately managed.
- The Framework should help identify duplicate security activities, services, functions, or components in order to consolidate them to reduce complexity, maximize efficiency, and promote system availability.
- The Framework should promote broad usability by being sector agnostic, yet provide associative connections that allow sector specific cybersecurity elements to be developed, measured, and managed.

In addition to the above attributes, the Cybersecurity Framework should be flexible enough to allow it to compliment and perhaps tie into security architecture and system architecture frameworks.

2.0 RESPONSES TO RFI QUESTIONS

2.1 Current Risk Management Practices

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

We see the cross-sector adoption of a consistent set of practices with related standards, training, and methods as one of the biggest challenges in improving cybersecurity practices across critical infrastructure. In order to overcome this challenge, a tangible value of migrating to new practices should be evident, as there have been considerable sector specific investments in current practices. Cross-sector consistency with practices will help create a strong synergy for analyzing threats, developing security solutions, mitigating risks, sharing threat intelligence, and increasing the speed of detection and response—strengthening the cybersecurity posture of our critical infrastructure.

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

We believe the greatest challenge in developing a cross-sector standards-based Framework for critical infrastructure will be addressing specific sector needs while achieving cross-sector commonality in understanding, process, and procedures. This will require disciplined architecture and development practices to create a Framework that is appropriate for all sectors. Common Framework product/artifact threads that apply to all sectors must be identified such that when these framework products are decomposed and refined to a level that applies to a sector specific set of solutions, those specific solutions can be implemented in the Framework without losing key constructs and cohesion with the remainder of the 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?*

Our organization uses a well-established risk management process based on identifying risks early and developing mitigation plans to proactively minimize the potential impacts of those risks over time. Our policies and procedures are consistent with industry best practices such as those defined by the Project Management Institute (PMI). We perform both qualitative and quantitative risk assessments to determine the probability and severity of each threat. We use Risk and Opportunity Management Boards (ROMBs) to provide governance, management, and control of risks and opportunities that are identified by any stakeholder within our organization as well as our customers' communities. We develop mitigation plans for every risk that is not within accepted exposure limits. Those plans are executed and periodically monitored and reported to the ROMB.

Our risk management procedures are integrated into our business processes and extend into our approach to mitigating cybersecurity threats. Our procedures are aligned with the Risk Management Framework (RMF), as defined in NIST SP 800-37 and we adopt specific cybersecurity risk processes from NIST SP 800-39 and NIST SP800-30 for managing and assessing information security risk. Our approach to cybersecurity risk is one of proactive behavior-based mitigation as opposed to identification and mitigation of threats after impacts have

occurred. Our senior management communicates the policies and procedures by making them available in a common repository accessible by all employees. Employees are educated on our policies through periodic compliance training and they are immediately informed when policies and procedures are modified. We have a Performance Excellence group that maintains our risk management procedures and ensures they are aligned to our business processes to achieve maximum efficiency while minimizing the burden to our business operations.

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

In our organization, the responsibility for executing our cybersecurity risk management program is assigned to our Chief Information Security Officer (CISO), who reports to our Chief Information Officer (CIO). Since our CIO/CISO office provides direct support to all of our customer-facing lines of business, this has been an efficient organizational location and has allowed us to quickly collect, adjudicate, and minimize threats as soon as they are identified.

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

Our organization defines risk generally as a measure of the potential inability to achieve our objectives within defined cost, schedule, and technical constraints. We assess risks generally by identifying and prioritizing risks to our business objectives. Specifically, we define cybersecurity risk as the probability of successful exploitation of vulnerabilities in our information systems that cause negative impact to our business operations or our customers' missions. We assess cybersecurity risk by qualitatively identifying the threats to specific asset classes and quantifying the probability of any vulnerabilities being exploited along with the severity of impact of a successful exploitation. Effective risk mitigation measures are then put in place to reduce vulnerability and/or the impact of successful vulnerability exploitation. The defensive measures we put in place are security controls such as those defined in NIST SP 800-53. We use specific guidance on risk assessment from NIST SP 800-30 and procedures consistent with industry best practices such as those defined by the Project Management Institute (PMI).

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

Cybersecurity risk is fully incorporated and integrated into our organization's overarching enterprise risk management processes. Risks to the critical infrastructure that our business relies on to operate could result in damage to the relationships we have established with our customers as well as loss of our intellectual property. Therefore, cybersecurity risk is a key consideration during our evaluation of new Information Technology (IT) systems or cloud based services. Cybersecurity risk management flows from strategic organization risk management through a tiered and traceable hierarchy. Strategic cybersecurity risk management starts at the organization governance tier, incorporating high level business process and is then subsequently decomposed into tactical risks and risk management at the business information and cyber operations tiers. Enterprise and security architectures along with related requirements also tie into the cybersecurity risk management process and a risk management database. All related sub-processes and information are disseminated, measured, controlled, and acted upon throughout the relevant enterprise entities, as coordinated by the CISO.

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

Some good foundations for standards, guidelines, and practices include the "Guide for Applying the Risk Management Framework to Federal Information Systems", as defined in NIST SP 800-37 along with its associated standards (NIST SP 800-30, NIST SP 800-39, and NIST SP 800-53), the (ISC)$^{2®}$ (International Information Systems Security Certification Consortium) Common Body of Knowledge Domain for "Information Security and Risk Management", and the PMI common body of knowledge. Models or tools that exist include: Capital asset pricing model, which helps determine the appropriate rate of return of an asset; and Probabilistic Risk Assessment (PRA) (also called Probability Consequence or Probability Impact Model), where estimates of probability of occurrence are related to the consequence of occurrence.

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?*

Our organization is required to comply with the reporting requirements defined in paragraph 3 of the National Industrial Security Program Operating Manual (NISPOM), specifically paragraph 1-302b which states, "Contractors shall report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee." Paragraph 1-301 in the NISPOM requires that "contractors shall promptly submit a written report to the nearest field office of the FBI regarding information coming to the contractor's attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of its locations".

We are currently not aware of any mandatory reporting requirements at the State or Local levels for privately owned organizations. The majority of our organization's efforts are focused on supporting the Federal Government and our reporting is done directly to the government agencies we support as well as those defined in the NISPOM. Our corporate policies and procedures are tailored to support the reporting requirements defined in the NISPOM as well as any of our existing customer's unique reporting requirements.

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

Our organization's most critical assets are our people who help our customers execute their missions on a daily basis. In order to execute these missions, our people are interdependent upon critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation. Impacts and interruptions to the telecommunications, energy, and financial services sectors could represent the most immediate risks to our organization's business operations. We conduct risk mitigation activities and plan contingencies to offset the impacts of disruptions in each of the sectors.

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

Our organizational performance goal is to maintain nearly 100% availability of our network to provide essential services to meet our business objectives and our customers' missions while we proactively manage cybersecurity risk. Outages associated with routine maintenance are not counted as downtime for this availability. We manage business continuity in alignment with

methods defined in the (ISC)$^{2®}$ common body of knowledge for the Business Continuity and Disaster Recovery Planning Domain.

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?

Our organization is currently not required to report to more than one regulatory body. In the event of a cybersecurity attack impacting our customers' networks, we are required to report the impacts directly to them immediately after the incident(s) is remediated in accordance with the NISPOM. In the event of a cybersecurity attack impacting our own organization's network, we are not required to report to any regulatory body.

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

We believe organizations that develop national/international standards should establish and sponsor an environment that would allow private, state, local and federal entities to collaborate on information sharing and standards development. Organizations that develop the standards should establish a forum(s) where participants are vetted and trusted. They should establish rules that define how data can be used and should define strict rules on data sharing. The Federal Government should work in partnership with these forums to ensure standards and best practices are being developed effectively to meet the needs of all critical infrastructure sectors.

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

1. What additional approaches already exist?

Many of our government customers adhere to various federal standards, frameworks, and directives such as Intelligence Community Directive (ICD) 503 for direction on Risk Management, Certification, and Accreditation. Additional approaches are detailed in the NIST SP 800 series of documents for information technology security, as well as in multiple DoD directives and instructions. Significant works have also been created or adopted by the Department of Defense Cyber Crime Center (DC3), the National Cyber Investigative Joint Task Force – Analytical Group, and the DoD Industrial Base program.

2. Which of these approaches apply across sectors?

The NIST SP 800 series documents apply across multiple federal agencies, including derivations that are used within the Intelligence Community potentially impacting the critical infrastructure sectors that those agencies work with.

3. Which organizations use these approaches?

All federal agencies use the NIST SP 800 series documents or a derivation of the documents to tailor their own unique approach. For example, the Department of Defense uses similar approaches outlined in their various directives and instructions, but customized to their own organizational structure and culture.

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

Due to the complexity of cybersecurity, the scope of the approaches can lead to a large amount of program overhead cost required to implement an overwhelming number of standards,

maintenance practices, and compliance measures consistently across an organization. Due to this overhead cost, smaller agencies and businesses cannot typically utilize many of these approaches or can only utilize portions of the approaches. This in turn can lead to inconsistent application of cybersecurity controls, even within programs that are run within the same agency.

Another limitation of shared approaches is that even when common standards are shared and fully implemented, those standards are still not always applied consistently. Different entities can employ the exact same standards approach, but interpret and implement it in different ways. The differences in interpretation and implementation of standards can be attributed to a number of factors including, but not limited to budgetary constraints, risk appetite, lack of proactive compliance verification programs, and internal agency dynamics.

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

Most of the approaches applied today have a greater focus on risk management rather than risk avoidance. The strong emphasis on risk management is sound in a world of ever-evolving landscape of technology and threats. However, risk management inherently requires risk assessment. Performing an objective assessment of risk can be a difficult task for organizations to perform uniformly and consistently. Threat evaluation, a key portion of a risk assessment, is still a largely subjective endeavor. The resources that typically analyze risk and document the risk assessments are not always aware of or able to incorporate all of the risks because the threats are often deemed sensitive. The resources responsible for developing the risk assessment need to be made aware of all risks, including any sensitive threats in order to be able to document a comprehensive risk landscape.

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

Most of the approaches utilize similar security "best practices". However, the Federal Government, Intelligence Community, and Department of Defense have applied specific variants to these practices in order to account for the policies, environments, users, information sensitivity, and other factors within each of the sectors.

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

We believe there should be a sector-specific standards development process, since each sector has a unique set of needs. Those standards should contain clear compliance measures that can be regularly tested and should be designed to align with a common overarching framework. In our experience, voluntary compliance programs encourage shortcuts to be taken and can financially reward non-compliance.

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 related sector coordinating councils can guide the sector-specific standards to help ensure that those standards adequately address their sector-specific cyber security concerns without negatively impacting their ongoing government or business operations. Sector-specific approaches, when combined with sector-specific compliance measurements, typically benefit the entire sector by aligning controls and control auditing across all sector participants.

Promotion of this and other benefits by sector-specific agencies and coordinating councils will help drive adoption of and compliance of these common approaches across a sector.

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

We believe outreach efforts that identify specific areas of standards conformance to each sector and the implementation of conformance measurements would be helpful. These outreach efforts should identify the constraints that each sector has in meeting certain conformance criteria and promote collaboration on plans that will help mitigate those constraints.

2.3 Specific Industry Practices

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

Yes, the practices outlined in the RFI are widely used throughout critical infrastructure and industry, especially as they relate to U.S. critical infrastructure. However, it is sometimes difficult to ensure the separation of business from operational systems due to the inherent lack of continuity between business and technical solutions in some existing frameworks. This may cause technical implementations to hinder business agility due to inappropriate tight coupling of a security solution to a business capability.

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

There are a multitude of standards that relate to most of the practices mentioned. The most authoritative standards development organizations related to our industry sector are NIST, IETF, IEEE, and ISO/IEC.

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

We believe the most critical practice for the secure operation of critical infrastructure is the "Security engineering practices". Security solutions must be designed and built correctly from the start. This practice must include architecture and design activities that satisfy business goals as well as mission needs. The following include some applicable engineering functions or security engineering areas:

- Security capability development aligned with business mission
- Security requirements development aligned with business needs, policies, and directives
- Security architecture development
- Technical security risk management tied to enterprise risk management
- Trusted platforms
- Network security
- Data security
- System/software assurance and application security
- Verification and validation relating to conformance, performance and interoperability

This represents only a brief outline of areas that need to be covered in Security engineering.

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

We believe that all of these practices are applicable for business and mission needs within all critical infrastructure sectors.

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

We believe that the "Monitoring and incident detection tools and capabilities" practice poses the most significant implementation challenge because of the lack of standards that provide a common syntax for communicating security intelligence and enabling effective event correlation. Continuous monitoring capability such as described in the Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) architecture per NISTIR 7756 and NIST SP 800-137, and the Security Content Automation Protocol as defined in NIST SP 800-126, are still relatively new. An increasing threat environment makes it increasingly necessary to implement continuous monitoring, define a common syntax for reporting incidents, provide policy continuity, and correlate security events.

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

Technical standards are referred to frequently when ensuring interoperability of functions or systems in the procurement and development process. These standards are also used in verifying conformance and performance against stated claims and requirements. Guidelines and process standards are scrutinized for pertinence to specific operational activities related to business functions and mission in our organization.

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

Our organization does have a methodology in place to properly allocate business resources to invest in, create, and maintain IT standards. Other organizations are beginning to realize the full impact and importance of standards to enhance interoperability, effectiveness, and competitiveness. In other organizations, a value to investment has not been realized yet, due to the lack of training, identified economic incentives, and perhaps a viable framework that identifies tangible business value to these investments.

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

Our organization does have a formal escalation process to address cybersecurity risks that suddenly increase in severity. We have a Computer Incident Response Team (CIRT) that is easily accessible by everyone in our organization, and through which any employee can quickly and easily escalate unforeseen risks. Our CISO customizes and implements mitigation plans for risks that suddenly increase in severity in accordance with our established risk management processes.

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

The application of any effective Cybersecurity Framework has the potential to create risks to privacy and civil liberties interests. The collection of information related to or derived from monitoring IT system activity, internal and external, could capture sensitive information, including

personally identifiable, protected health or other information in which an actor may have privacy or civil liberties concerns. The nature of a cybersecurity event may involve or require the government and private industry to share such information in order to respond to the event, whether in a remediation or preventative context. Resolving these concerns will require attention to legal (including with respect to transnational law) and regulatory strictures on the access, use and dissemination of such information, understanding that such limitations may vary depending on the nature of the information (e.g., protected health information).

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

As noted in the response to Question 9, certain transnational legal regimes (for example, the 1995 EU Data Protection Directive and its recent amendments) could have implications on any organization that transacts business outside the United States. The Cybersecurity Framework should be structured in a manner that provides sufficient internal controls to ensure compliance with non-U.S. privacy and civil liberties requirements.

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

Risks to privacy and civil liberties can be managed through a thoughtfully designed information sharing program with appropriate (i.e., legally compliant) limits on the scope and nature of the information to be shared, and the circumstances in which such information is to be shared, including appropriate limits on downstream use of that information

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

Assuming that the listed practices are comprehensively decomposed, we believe that this list of practices is complete. The only recommendation we would make is that "Privacy and civil liberties protection" could be a sub-practice under a law and regulations practice, which would include more than just one aspect of law. The organization of practices and sub-practices will likely be refined as the Framework development evolves through more detailed sector-specific analysis.

3.0 ABOUT THE SI ORGANIZATION, INC.

The SI is a leading provider of full life cycle, mission-focused systems engineering and integration capabilities to the U.S. Intelligence Community, Department of Defense and other agencies. Its scalable systems engineering platform for modeling, simulation and analysis helps customers baseline requirements, optimize resources and manage risk. The company has 40 years of experience successfully delivering complex, system-of-systems technology solutions. The SI employs approximately 2,000 people, with major locations in Chantilly, Va.; Denver; Laurel, Md.; Los Angeles; and Valley Forge, Pa. For more information, visit www.thesiorg.com.