NIST RFI ON DEVELOPING A FRAMEWORK TO IMPROVE CRITICAL INFRASTRUCTURE CYBERSECURITY

SAIC NATIONAL SECURITY OPERATIONS

APRIL 8, 2013

NATIONAL SECURITY • ENERGY & ENVIRONMENT • HEALTH • CYBERSECURITY

SAIC

INTRODUCTION

Science Applications International Corporation (SAIC) appreciates the opportunity to participate in the review of the questions posted in the RFI titled "Developing a Framework to Improve critical Infrastructure Cybersecurity", Docket Number 130208119-3119-01. Our response is primarily focused on four areas.

RECOMMENDATIONS ON FRAMEWORK, STANDARDS, AND PRACTICES

The development of a Framework to codify cybersecurity guidance will be of great benefit to both critical and non-critical infrastructure providers. Different sectors and providers are at different levels of maturity in developing processes and procedures to respond to the cybersecurity challenges. Sharing the lessons learned within the information technology industry can shorten the learning and response timeframe. Use of a Capability Maturity Model (CMM) in implementing the Framework will allow individual sectors to develop tailored responses to their unique challenges while providing an overarching structure to share common problems and solutions. A CMM-integrated Framework will also provide mechanisms to measure progress made over time towards increasing security. The Capability Maturity Model Integration (CMMI) program is a well-recognized standard that could be used within the Framework. The National Initiative on Cybersecurity Education (NICE) CMM with its three main areas of focus: integrated governance; process and analytics; and, enabling technology, also provides a flexible organizational structure adaptable to the requirements of the Framework.

GENERAL STRUCTURE AND GUIDELINES

The cybersecurity industry has numerous organizations that have developed standards, guidelines and best practices. They have a variety of focus areas and varying levels of adoption. Many of these standards are focused within information technology areas that are very specific to the security challenges within their sectors and are not generally adopted by others. Compounding the wide variety of standards with uneven adoption, what is widely published and used currently is not broad enough of a framework to work across sectors. Ideally a Framework would be sufficiently broad to be acceptable across sectors but still enable sufficient specificity to achieve sector-specific results.

The Framework should serve as both a set of guidelines to meet and develop towards, but also an opportunity to educate, collaborate, and ensure common understanding across sectors. To further promote usage, each sector would be able to adopt the Framework through the development of sector specific standards that leverage each industry's knowledge, expertise, and current regulatory requirements to develop applicable solutions to their common risks and threats. The Framework would encourage each sector to develop compliance or audit mechanisms to conduct cybersecurity conformity assessments to ensure that no individual company attempts to gain a competitive advantage by ignoring sound practices. It is not recommended that the standards body conduct the assessments themselves, but to create the mechanisms and rely on a 3rd party assessment model. The Payment Card Industry Data Security Standards (PCI-DSS) Council has a model that could be referenced. The PCI-DSS model supports an industry lead self-enforcement model that focuses on their primary threats and risks. The assessments are not carried out by the rule making body, but by 3rd party assessors that meet the industries requirements. If the industry is reluctant to participate it would be incumbent on regulatory bodies to mandate these processes. The Framework should also consider adoption of an expanded FedRAMP program. FedRAMP's governance process program, combined with the use of independent third party assessors, provides a consistent, transparent methodology with established technical security controls that could be applied by all sectors.

A challenge posed by this model is that each sector may interpret the intent of Framework recommendations differently. To achieve unity of purpose and be workable the Framework should accommodate both general and specialized requirements. A clear delineation of common goals versus sector-unique requirements must be observable in the Framework. Sector-specific cybersecurity information can certainly be included in the Framework. A great value of the Framework is that different sectors will be able to leverage security solutions originating outside their sector. Effectively the Framework serves to showcase components of sector-specific information that could become cross-sector solutions. The North American Electric Reliability Corporation's (NERC) model for development and enforcement of reliability standards may serve to provide lesson's on how to engage an entire sector towards the common good.

Education will be critical to ensure that each sector understands there is a significant level of shared risk that all participants must accept, and the Framework is meant to support development of a cybersecurity community of interest. In other words, if there is a cybersecurity event that impacts a particular provider in the nuclear sector, this event will impact all providers in that sector from either a tangible or perceived standpoint. The establishment, participation and maintenance of this Framework will serve to enforce and codify this concept.

There are several Maturity Models available, which could be applied to the Framework. CMMI is probably the most recognized one. Originally developed for evaluating the development and quality of software and systems, CMMI has since become a well-recognized architecture for a maturity model and has been applied in other parts of organizations to evaluate business processes.

The NICE CMM (draft) is designed to help develop the cyber workforce. Use of this CMM would have several advantages because of the way it is structured and evaluated. Its structure is broken into three segments:

- Creation of a governance structure that would apply to all sectors;
- Sharing of process and analytics methodologies that could be optimized by sector;
- Introduction of enabling technologies at a sector level with application across sectors as appropriate.

This structure provides flexibility in implementation and focus on Framework-level, individual sector, and cross sector issues. The NICE CMM identifies three levels of maturity (Limited, Progressing, and Optimizing) that lend themselves to a broad undertaking such as the Framework.

In order to achieve tangible security improvements, the Framework should be maintained at a broad consensus level. The Framework should provide the platform to develop and publish sector-specific scenario guidance that would be vetted at the Framework governance level. Each sector would be responsible for identifying a number of common scenarios for their sector. These scenarios would be grown into scenario bundles that illustrate the application of the Framework to the specific scenario. This could include sample applications, scripts, checklists, cost/benefit information, network diagrams and tutorials. This would enable organizations to better understand the purpose and benefits of the Framework, how it can be leveraged, what the common sector level baseline approach is, and a reduction of shared risks. Again, looking to NERC's process and compliance model may provide good guidance.

The Framework must be implemented in a careful manner to ensure this approach will not lead to a significant increase in compliance or regulatory burdens. A descriptive rather than a prescriptive approach is needed. It is important that each industry and sector take positive steps towards securing their infrastructure. Increasing the compliance burden will not necessarily reduce risks and may hinder implementation of improved security practices. Careful review of existing compliance and regulatory requirements should be part of the standards development process. Identifying commonality and differences in requirements along with a cooperative review process will support streamlining any compliance issues. A unified approach to these

requirements must be outlined to clearly identify all of these scenarios. A number of organizations have already attempted to find alignments and gaps in the standards currently available. Sharing their approaches such as the Unified Compliance Framework (UCF) for lessons learned could be beneficial to the development of the Framework. Other examples include Information Systems Audit and Control Association (ISACA) samples of alignments with their COBIT Framework, NIST provides mappings to ISO standards, and the UCF has attempted to align a large set of security and legal requirements.

A governance board and process must be developed as a first step in completion of the Framework. The Framework will require updates on a periodic basis. A governance body can manage the updates required as best practices and new threats are identified. A potential model for this is for representatives to be provided from each sector's standards development body. This ensures that each sector is included, and that as the standards bodies develop their sector standards, there will be common understanding of intent at the Framework governance level. New content and updates should be enabled at the grassroots level, so organizations can share their ideas and experiences.

The Framework body must also undertake a review of the critical infrastructure's inherent interdependencies. Borrowing from social network analysis, it would be valuable to identify bridges, centrality, and distance between each of the critical infrastructure nodes. An additional element to add to the interdependency analysis is the duration of independence. For example, the wireless industry may be dependent on the electrical sector to supply power for their communication towers. These towers may only have sufficient battery backup to withstand 48 hours of outages. Understanding these time based interdependencies will be important in prioritizing the critical infrastructure and evaluating the cascading effects of service loss. A new tool that should be considered when analyzing risk dependencies is the Open Group's Open Group Dependency Modeling (O-DM) standard.

COMMON LANGUAGE AND TERMINOLOGY

In addition to the scenario bundles, the Framework needs to create a clear taxonomy, or hierarchical categorization scheme and terms defined such as Standards, Guidelines and Best Practices. Clearly defining these terms and showing how each relates will allow for unambiguous regulations to be developed and applied. For example, after completion of the Framework, each sector will then develop sector specific guidelines. The guidelines can then be used by the industry to develop standards. This is not necessarily the hierarchy and definition that the authors are advocating, but an example of how to flow the process.

A secondary purpose for these definitions is also to limit industry confusion due to marketing terminology. It would be incumbent upon the governance body to develop a dictionary or taxonomy of security terms to ensure the common understanding. This should also include common acronym usage. In the event of multiple terms and acronyms in use, the dictionary would offer the alternative definitions, context, and sector relationships.

PRACTICES

The cybersecurity practices highlighted in the RFI are often associated with industries knowledgeable about information technology security, either as a core business process or by leveraging outside expertise. This awareness may not be as commonly implemented in sectors where IT is an enabler but not as a central component of the business. In these businesses, security practices are largely ad hoc when present and more difficult to maintain. Security practices are sometimes enabled as a result of a breach or scare, but not set up as a long term approach. Basic security practices must be initiated by all organizations. Fundamental guidance provided by the Framework will be important to help ensure baseline practices are in place. Good basic practices are important to ensure a common level of security hygiene is maintained by all organizations.

In some cases, these cybersecurity practices are implemented in sectors that have to show compliance with existing regulations (FISMA, PCI, HIPAA, etc.). While they do not inherently originate from a business or mission need, their successful implementation sustains the business and mission.

Defining "most critical" as being the one practice that stands out as the first step towards implementing a more secure environment, then **separating business systems from operational systems** is the most critical, first priority practice. Leaving these systems interconnected is akin to leaving the doors open to intruders. First close the door, and then worry about installing the best lock. The practice of separating business systems from operational systems effectively closes the open door.

The other mentioned industry practices are also extremely important. The following list establishes a further relative priority and explains the reasoning behind this ranking. The priority can be viewed as an "order of encouraged implementation". In other words, these security practices, should be implemented in the following order:

Rank	Industry Practice	Reasoning
1	Separation of business systems from operational systems	See above. This is a critical activity that serves as a baseline to further systematic analysis of organizational assets and relationships.
2	Incident handling policies and procedures	Personnel must be trained to ensure they can respond in appropriate ways to unpredictable events. This is comprehensive training that includes all system users as well as IT specialists. The NICE CMM offers a model that could be followed to identify and achieve needed skills.
3	Identification and authorization (I&A) of users (and processes) accessing systems	A baseline level of control regarding the verification of identities of users (and processes) accessing the system is important because: (1) it encourages responsible behavior, since users recognize that their actions will be monitored; (2) it enables auditing of system usage for malicious activity; (3) it eliminates the single point of failure involved with username/password sharing, or an entire lack of identity verification; (4) it increases system stability because users cannot access exposed functions that are not necessary for their particular work activity.
4	Asset identification and management	To effectively protect and manage security, the organization must have a current view of their assets including associated metadata such as location, purpose, accessibility, backup or failover system, etc. A key metadata element is the relevant priority of the asset compared to all the other assets in the organization. This ranking enables dynamic risk and response management when prioritizing future security investments, identifying important vulnerabilities, and impact analysis during attack scenarios.
5	Security engineering practices	Incorporating security requirements into engineering designs and system requirements reduces lifecycle costs and improves efficient implementation of security functionality.
6	Use of encryption and key management	Ensuring secure end-to-end communications and protecting data at rest and in transit is a demonstrated effective measure that increases compliance and security.
7	Mission/system resiliency practices	This practice enables organizations to prepare for disasters and plan effective responses. Redundancy and failover measures can be improved as the organization's maturity in this practice increases.

Rank	Industry Practice	Reasoning
8	Monitoring and incident detection tools and capabilities	Key here is to monitor appropriate indicators and on a regular basis. Significant automation can be brought to bear in this practice. To protect critical assets monitoring must be coupled with an up to date vision of where vulnerabilities are, and how they might be exploited.
N/A	Privacy and civil liberties protection	This practice should not be "ranked" but should permeate the implementation of all other practices. We cannot write off privacy rights and civil liberties, even for the cause of critical infrastructure protection. Privacy requirements vary between jurisdictions. Key to successful enforcement of these requirements is understanding of the national and international requirements of geographic entities (EU for example).

The practices listed above are important and should be automated if at all possible. Any implementation is better than waiting for a “perfect” solution. Waiting for the optimal solution encourages paralysis and, significantly increases the required investment as well as the implementation time. Practices can be implemented at a baseline level, and the maturity of the practice increased with experience over time. In fact, this is better than conducting business with no implementation of the practice while you are waiting for the "perfect implementation". Implementation should also consider organizational capabilities. Small and intermediate sized organizations that are part of critical infrastructure sectors may not have the resources to implement all controls immediately or make use of automation. Guidance should be structured so that criteria are clear for making informed decisions on implementation priorities.

Among the noted practices, perhaps the most challenging to implement are identification and authorization (I&A) of users accessing systems, and monitoring and incident detection tools and capabilities.

The **identification and authorization (I&A) of users accessing systems** is difficult to implement because organizations may have to retrofit legacy systems that were not designed for user access management. Organizations may have to put another system in front of the legacy system. This will not be difficult if implementing a new system with identification and authorization capability built into the design.

Monitoring and incident detection tools and capabilities are difficult to do well because they are resource-intensive operations, and require tuning to ensure the right threats, or critical assets are being monitored. Monitoring must be coupled with an up to date vision of where vulnerabilities are, and how they might be exploited. Even if organizations are fully aware of these things, monitoring may not be possible or realistic due to limits in resources and personnel.

In addition there are significant challenges with: asset identification and management, and mission/system resiliency practices.

Asset identification and management is a foundational area that requires systematic, well-resourced processes. If assets are unknown and lack a documented security baseline they are a threat to an organizations security posture. Creating automated, scalable configuration management processes is a significant challenge.

A common, sector specific set of **resiliency requirements** requires a clear understanding of critical processes. The Framework needs to identify basic resiliency requirements for all information systems. Identifying critical business processes would be a logical first step to achieve these requirements.

INTERNATIONAL APPLICATION

The relationship of practices to international standards will be sector dependent. Sectors that are already subject to international compliance requirements will be able to identify high level practices that may be applicable across sectors. Sectors with a more national focus such as Healthcare and Power would not be as concerned with international standards and practices. Many sectors follow standards and practices (ISO, IEEE, etc.) because they make good business sense. Compliance may be voluntary but forms a basis for identifying "best practices."

National and international standards should be considered in any cybersecurity conformity assessment. In order to create a viable Framework that is accepted between sectors a phased approach is needed. National standards should be the starting point within each sector. Where a sector such as Finance is already involved with international standards, Framework development should proceed with the ultimate goal of alignment with existing international standards.

INFORMATION SHARING AND LIABILITY

The Framework should work through the Sector Coordinating Councils (SCC) to establish procedures for establishing best of breed cybersecurity practice guidance. Incentives can be established by the Framework to encourage participation. Raising awareness of efforts like the Energy Subsector Capability Maturity Model (ES-C2M2) will provide a starting point for collaborative development efforts.

Currently some of these practices are not shared by companies because they are considered a component of their competitive advantage. Sharing of some of this information may also be limited by a variety of legal concerns. Mechanisms must be created to permit sharing of this information, with some protections, that limit liability. These could be akin to “Good Samaritan Laws” that are in place to encourage participation and provide protections.

Overcoming industry's hesitancy about documenting vulnerabilities is another challenge. Companies and sectors still view identification of critical infrastructure shortcomings in a Framework as an admission of persistent inadequacies. The Framework needs to address this challenge and demonstrate that population and management of this information in a Framework in a not an “admission of guilt” but a mechanism to prioritize and handle cyber security threats, as well as learn from each other about the best means by which to overcome them.

Organizations typically have processes in place to respond to attacks, new threats, or changes in alert status. These processes are normally implemented at a technical level with reporting mandated on a sector or higher basis. Framework guidance in this area needs to be generic and emphasize compliance with reporting requirements. The Framework should provide a forum for exchange of ideas on sharing of technical threat information.

USE OF METRICS IN COMPLIANCE AND RISK MANAGEMENT

The Framework should create a set of metrics that can be used across sectors. These metrics need to be defined in standardized terms that are recognized by national and international bodies and accepted for use by sectors. The metrics should focus on business risk and trends. The Framework can be of significant benefit by codifying the threats and likelihood measures. Each sector would be responsible for articulating the impact of each threat for their industry. These impacts should also be evaluated over differing durations, during the dependency analysis. The results presented in “Measuring What Matters” released in March 2013 by SafeGov would be a good starting point. A strength of the SafeGov approach is that it bases its assessments on common standards and

methodologies. While focused on use by IGs within federal agencies the methodology could be generalized for use by the Framework.

Cybersecurity risk is generally managed reactively, rather than proactively. "No news is good news" has been the historical norm. Organizations set up their cybersecurity (perimeter) defenses, conduct their monitoring, and generally wait to see if their network is attacked, or a machine is compromised. Organizations have trouble quantifying and defining cybersecurity risk because they often cannot identify their most important IT assets, or assign a relative priority to IT assets across the organization. Data loss is difficult for most people to measure because they cannot place a dollar figure on it.

One of the questions that the Framework should address is, "What to measure?" Many enterprises collect a great deal of data from multiple sensors. This data is not converted into intelligence (useful information) because analysis is not keeping pace with collection. More focus is needed on how to quickly create intelligence from the multiple data feeds available. One approach would be to put more emphasis on threat intelligence so that sensor data indicative of attacks would be given priority in analysis and shared throughout the Framework.

In most organizations cybersecurity risk and enterprise risk are managed separately. The IT security profession historically has not done a good job articulating cybersecurity risk to the business side of the organization. This is not surprising because IT security investments are also not directly tied to business needs. To be considered together, cybersecurity risks need to be translated in terms of costs. Consider the following scenario: if we implement email security system X it will cost $250,000 per year, but will reduce the number of compromised machine incidents by 5 per month. Each compromised machine costs $10,000 to fix. 10% of the compromised machines will result in maintenance costs of $50,000.

Item	Amount
Costs	
Purchase and monitoring	($250,000 / yr.)
Benefits	
Avoid machine compromise (5 x $10,000/month = 50,000 per month x 12 months	$600,000 / yr.
Data loss prevention (6 incidents per year @$50,000 per incident)	$300,000 / yr.
Net gain (loss)	$650,000
Payback Ratio	2.6 to 1

Payback ratio identifies value but there are limitations to this approach that need to be explained. For example, cost avoidance is still accomplished even if a new type of e-mail attack is successful against the organization. The investment in up-to-date software indicates an appreciation by management of the existence of a threat and appropriate due diligence.

The Framework should identify metrics that apply to multiple sectors. Some, such as training, could be standardized and measured with relative ease. Others would be more complicated and might involve sector specific inputs that are normalized to a common measure such as cost of outages.

Current metrics primarily center on easily automated functions. These are typically related to inventory and patch management functions carried out via automated scans of configuration files. This is often used as a compliance metric to gauge the performance of patch management systems, but is rarely used in a true risk management program. There are no defined processes or recommendations on how compliance metrics handle specific threats, which may be extremely beneficial in this Framework. A group that has invested in mapping of various risk management and compliance standards is the Unified Compliance Framework. They have tools that

map a variety of controls and standards to provide common understandings of compliance requirements. The Framework could leverage their work to promote cross sector definitions of cybersecurity terms and requirements. As recommended by SafeGov in "Measuring What Matters," NIST should develop a threat model as a part of the Framework to build a foundation for risk management across Sectors.

Time-based metrics should be developed based on the interrelated nature of critical infrastructure sectors. A recent example that shows the linked nature of sectors is Hurricane Sandy. Power outages caused an immediate impact on large population groups. Backup power supplies lessened the impact on individuals and families, institutions (such as hospitals), and cell-providers who had emergency generators. However, blocked transportation lines (roads) caused further outages when fuel could not be provided to generators as they exhausted their immediate fuel supplies. Disruption to transportation links also impacted other critical infrastructure sectors that rely on the movement of people and materiel. Time-based metrics would provide insight into the prioritization of critical infrastructure restoration.

PRIVACY AND CIVIL LIBERTY CONCERNS

Cyber security risks that suddenly increase in severity will require the organization to increase their security; for example, when implementing increased virus protection, encryption, and vulnerability scanning. These actions could lead to the individual losing some control over their Personally Identifiable Information (PII). This loss of control could lead individuals to feel less likely to share their information `over the Internet.

To defend against the insider threat, organizations are starting to search open source content on the Internet for information about their prospective and current employees. Some view this as a threat to privacy, a limitation on our right to free speech, and at a minimum a blurring of the line between work and personal life. Clear policy guidelines must be established by the Framework in accordance with regulations and laws to ensure employee privacy is preserved.

One area that requires extra attention by the Framework is mission and system resiliency. If system backup and recovery procedures are not properly designed there is an increased risk of PII being exposed or compromised because proper controls are not in-place and enforced.

There are a number of actions that can be taken to help ensure awareness and compliance with current privacy regulations. These include:

- Completing a risk assessment and weighing risks against laws and cost to contain and safeguard PII
- Public awareness of what the company privacy policies are regarding PII
- Security training for those handling the data
- Users having the ability to control what they are sharing
- Ensuring policies and business practices comply with laws and guidelines governing the privacy and security of PII
- Protecting PII through a strong compliance program
- Maintaining awareness of international laws on privacy/liberties
- Establishing policies and procedures to identify and review protected information that may be shared.
- Enabling participants to determine the nature of protected information that may be shared and any applicable legal restrictions.
- Designating a Privacy Officer
- Developing and implementing appropriate policies and procedures that provide protections
- Implementing a continuous monitoring program that includes privacy policy guidance

Risks to privacy and civil liberties can be managed through several different methods. To manage the risks to privacy, one first must identify the risks to accomplish this, then a risk assessment should be completed that weighs the identified risks against the costs to contain and safeguard the information of the individual. As part of this assessment, the organization will need to identify and review protected information that may be shared, review how this information is protected, ensure information is secure where it is stored, define and prioritize what the threats are, and define a way to neutralize those threats.

Organizations will also need to review their policies and business practices and ensure they are in line with, and comply with, both American and International laws and guidelines governing the privacy and security of an individual's PII. The use of encryption is an important tool in ensuring the privacy of PII on the Internet, however if the individual is dealing with an international firm, the personal information may not be as protected due to the laws regarding the exporting of some encryption keys.

The organization must have a strong compliance program in place and be able to demonstrate that when policies are not followed, corrections are made. Individuals must be assured that the incident handling policies and procedures in place will protect the information during an ongoing or closed incident investigation to any person who does not have an authorized need to know the information.

As part of a security/compliance program a Privacy Officer should be designated by the organization and on-going security training for those handling the data should be required.

It is important that the individual be aware of what the organization's privacy policies are regarding their protection of the individual's private information. This policy information should be readily available to all and easy to understand. By understanding what the organization's policies are, the individual can make a better decision as to whether they want to risk their privacy with that organization. Individual participants should be able to determine what protected information may be shared as well as any applicable legal restrictions. Some entities may separate their business systems from their operational systems, but without strong access controls or a strong firewall policy this practice has the risk that an outsider could remotely access and change or influence the operation of a system and the privacy of the individual could be at risk.