U.S. Department of Commerce
National Institute of Standards and Technology
Request for Information (RFI)
Docket Number 130208119–3119–01
Developing a Framework to Improve Critical Infrastructure Cybersecurity

April 8, 2013

Prepared for:
Attn: Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop: 8930
Gaithersburg, MD 20899
cyberframework@nist.gov

Submitted by:
Northrop Grumman Systems Corporation
Northrop Grumman Information Systems Sector
Cyber Solutions Division
7575 Colshire Drive
McLean, VA 22102

Cage Code: 5YY61/NAICS Code: 541519, etc. / Business Size: Large
Federal Supply Schedule (FSS) GSA Schedule 70 Contract Number: GS-35F-0165Y

Primary Point of Contact (POC)
Melissa Corbin, Contracts Manager
Email: Melissa.Corbin@ngc.com
Phone: (571) 313-2226

Alternate POC
Tim Reese, Program Manager
Email: Tim.Reese@ngc.com
Phone: (310) 795-0717

Northrop Grumman Systems Corporation, a Delaware corporation, acting through Northrop Grumman Information Systems sector, Cyber Solutions Division (Northrop Grumman) is pleased to respond to the Department of Commerce (DOC) National Institute of Standards and Technology (NIST) Request for Information (RFI) Docket No. 130208119–3119–01.

Northrop Grumman is an industry leader in cybersecurity and understands first-hand how cyber threats pose serious risks to our national security, industrial base, and international economy. The rapidly evolving cyber threat spectrum demands persistent vigilance, constant awareness, and steady innovation to protect our critical information assets. Northrop Grumman is committed to working in partnership with the public and private sectors in the development and deployment of innovative and effective cybersecurity solutions to protect our nation.

We truly appreciate the opportunity to participate in this open public review and comment process to support NIST in developing an enhanced framework to improve U.S. critical infrastructure cybersecurity. Our response addresses areas of the RFI where we can provide the most helpful information in a public setting.

1 Overview of Northrop Grumman's Current Use of Frameworks, Standards, Guidelines and Best Practices and Risk Management Practices

Northrop Grumman is an important part of our nation's Defense Industrial Base, and as such, our company's assets are considered an element of critical infrastructure that requires cybersecurity protection. Over the past decade, Northrop Grumman has developed and enhanced cybersecurity best practices that we have effectively implemented within the company, through standardized corporate policy, procedures, and tools, and have used this experience to leverage these capabilities to also protect our customers' networks, systems and information. These best practices can be used to form the foundation on which NIST can create a defined and robust Critical Infrastructure Protection Framework. We utilize proven engineering approaches to cybersecurity and have established a framework of security standards and architecture approaches based on the guidance and standards of NIST and the International Organization for Standardization (ISO) Community as well as the Institute of Electrical and Electronic Engineers (IEEE) and the North American Electric Reliability Corporation (NERC). Our framework, reflected in our specialized cybersecurity visualization tools (Northrop Grumman's Cybersecurity Reference Framework titled The Fan™) and Northrop Grumman's Capabilities Framework (CyCape™), utilizes best practices from the SANS Critical Security Controls and the NATO Cyber Defence Capability Framework.

In addition to protecting our company and our customer's networks, systems and data, Northrop Grumman knows that effective cybersecurity includes continual enhancement of the technological security of the products we manufacture and the services we deliver. From unmanned aerial vehicles to satellites, we focus on to developing products that mitigate vulnerability to cyber attacks. Our methodology incorporates and demonstrates Northrop Grumman's commitment to a holistic approach to cybersecurity. Northrop Grumman's approach to effective cybersecurity means assessing and protecting

the mission functions the cyber infrastructure supports (business protection and continuity); the applications and data executing the mission (or business) processes; and the information technology infrastructure connecting the people, processes and functions necessary for organizational success. A key component of Northrop Grumman's cybersecurity practices, particularly related to risk management, is our commitment to timely and effective information-sharing. We drive innovation and enhance the capabilities of our cybersecurity tools and countermeasures by actively collaborating and sharing threat information with numerous organizations similarly committed to robust Cybersecurity protection, including the Transglobal Secure Collaboration Program (TSCP), Defense Industrial Base, Internet Security Alliance, National Infrastructure Advisory Council and other government agencies and task forces. This collaboration reduces the risks of our architectures and frameworks becoming outdated and thus less effective to mitigate the impacts of a cyber attack and helps ensure we can continue to evolve cybersecurity measures to collectively align against the latest and ever changing emerging cyber threats.

Northrop Grumman knows the importance of deploying operational risk approaches and how those practices enhance existing approaches to risk management. For organizations across the Civil Federal Agencies, Department of Defense (DoD), and the Intelligence Community, we have proven capabilities for identifying adversaries and conducting operations to protect our customers' computing assets and networks. Northrop Grumman is an innovator in cybersecurity and was the chief partner in the development of the Continuous Monitoring (CM) solution that fulfills the continuous monitoring goals, as described in the SANS Critical Security Controls. Most importantly, these continuous monitoring solutions are consistent with NIST SCAP, CAESARS, and the DHS Risk Management Framework, making this experience relevant to the framework envisioned by NIST. In our role as the only United States Industry member to the NATO Information Systems Technology Research Task Group (IST RTG) 096, Information Assurance/Cyber Defence Research Framework (IA/CD Framework), we supported the development of the NATO Cyber Defence Capability Framework (discussed below) at the NATO Communications and Information Agency through the work of Hallingstad and Dandurand (2011).

2 Proven Security Frameworks

Northrop Grumman understands and employs several effective frameworks to better address our security requirements, technology implementations, and gap/capability analysis. We utilize multiple frameworks as design and evaluation tools to verify capture of requirements, capabilities, gaps, technologies and to provide consistent methods of communication of security architecture and solution deployment.

We recognize the strong need for education and training with respect to frameworks and how they impact security architecture considerations. In response to this challenge, Northrop Grumman developed our Cyber Academy to deliver effective training, including our Cyber Architecture Course for a Northrop Grumman Cyber Architect accreditation that includes framework adherence and application.

2.1 Department of Homeland Security (DHS) 4300A

DHS utilizes a NIST-based approach to system security policy development, specifically DHS 4300A, that can serve as a good starting point for developing enhanced security policies and practices required as the foundation for building an improved Critical Infrastructure Protection (CIP) framework.

DHS 4300A articulates a comprehensive security program, providing a baseline of policies, standards, and guidelines for sensitive systems. It also outlines policies relating to management, operational, and technical controls for ensuring the confidentiality, integrity, availability, authenticity, and non-repudiation for DHS system infrastructure and operations. DHS 4300A is a proven approach, implementing Federal Information Security Management Act (FISMA) and NIST requirements and guidelines.

2.2 Integrated Cyber Security Capability Maturity Model (iCScmm Trilogy)

The Department of Energy (DOE) developed the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) to measure cybersecurity capabilities, following the recent publication of the Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline. Similar in nature to the DOE ES-C2M2, the iCScmm Trilogy utilizes an interrelated security and economic model with the goal not only to increase cybersecurity preparedness at a granular IT infrastructure level, but also to support the evaluation of economic and financial benefits for prudent capital expenditures on IT infrastructure and cybersecurity controls within an enterprise architecture. Northrop Grumman employs a similar capability maturity model in house to guide and support our company's assets and customer programs.

2.3 SANS Critical Security Controls

The SANS Critical Security Controls were developed with input from over 20 individual Federal agencies and contain recommendations for a baseline security program. The SANS Institute (SANS) Critical Security Controls are effective and provide a predictable level of protection. Building from this framework or incorporating these approaches into the planned NIST framework will enhance future efforts in the risk domain.

2.4 North Atlantic Treaty Organization (NATO) Cyber Defence Capability Framework

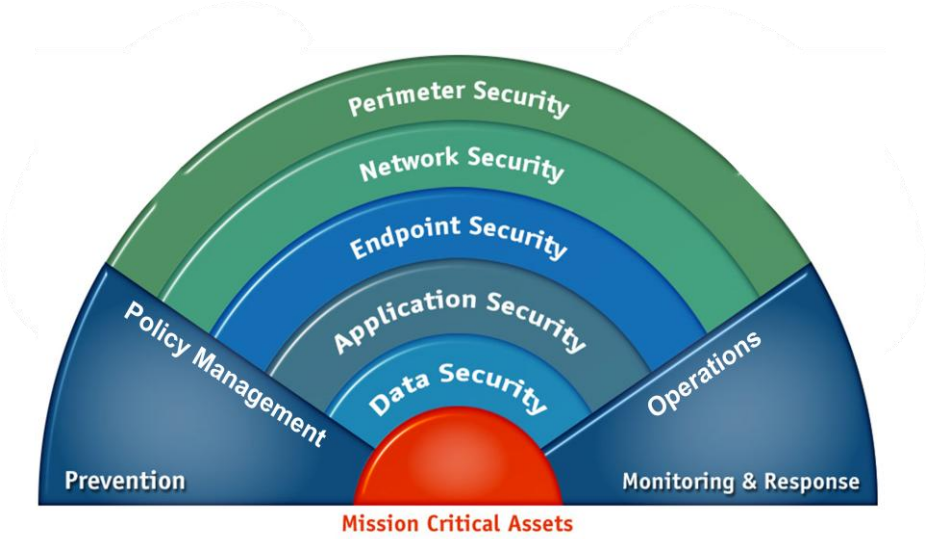
The NATO Communication & Information Systems (CIS) security capability breakdown is an international framework worthy of consideration by NIST. The objective of the NATO CIS security capability breakdown is to create a foundation for CIS security and cyber defense capability development within NATO and the NATO nations by clearly defining key terms and providing capability decomposition that can be used in a variety of ways. This approach should be carefully considered because it is dynamically risk-based in terms of developing key capabilities. These capabilities include, but are not limited to the following purposes:

- Establish the scope of CIS security and the capabilities needed to achieve a secure CIS
- Provide a common taxonomy and a structured reference for analysis of CIS security
- Provide a framework for multinational cooperation on the development of CIS security capabilities

- Provide a framework for establishing interoperability interfaces at various levels and for various capabilities, in order to facilitate CIS security in federated environments, and
- Provide a basis for assessing the maturity of CIS Security capabilities.

2.5 Northrop Grumman's Cyber Security Reference FAN™

Robust cyber defense requires proper architecting of technologies and processes at different conceptual layers of an enterprise which include the perimeter, the internal network, the various endpoints, the applications, and the data contained in the enterprise. This involves understanding which cyber technologies/processes can provide the maximum benefit, how these technologies/processes can support (or just as importantly, inhibit) each other, where it is best in the architecture to employ these technologies/processes and provide a consistent visualization of the results. The FAN™, a cyber defense-in-depth framework developed by Northrop Grumman, provides a picture of "what the defense is," illustrating technology placement and providing a visual architectural understanding how things "flow" within the network. This model provides a benchmark framework from which security architectures, and more importantly cyber security defensive architectures, can be assessed and evaluated. Although not directly a risk management tool, the FAN™ is used to consider alternatives in technology placement, product selection, and security control allocation. The FAN™ is proven and useful as a mechanism to communicate risk points and mitigation solutions.



2.6 CyCape™

CyCape™, a cyber capabilities framework developed by Northrop Grumman, provides the capability to analyze existing systems, requirements for new systems and provides a cybersecurity strength and weakness assessment. This cyber capabilities mapping is based on years of cyber work on numerous projects from small deployments to over a million users. CyCape™ provides a lexicon and a repeatable process used to perform requirements analysis, capability and gap analysis; and includes a cyber reference architecture framework that renders instantaneous representation of the analysis into visualization.

2.7 Electricity Subsector Cybersecurity Risk Management Process (RMP)

Northrop Grumman provided subject matter expertise to the Department of Energy (DOE) in the development of the *Electricity Subsector Cybersecurity* RMP guideline, developed to provide a consistent cybersecurity risk framework to all organizations in the electricity subsector, irrespective of the organization's size or mission. The RMP incorporated existing cybersecurity standards from NIST and the International Organization for Standardization (ISO) with regulatory standards from NERC, the Nuclear Regulatory Commission (NRC) and others to create a repeatable model for risk-based decision making.

Northrop Grumman supported the National Electric Sector Cybersecurity Organization Resource (NESCOR), a public-private partnership established to serve as a focal point for the electric sector's cybersecurity priorities. NESCOR works collaboratively with NESCO, DOE, and other federal agencies to:

- Enhance cyber security of the bulk power electric grid and electric infrastructure, including the security of legacy, current, and emerging technologies for the electric generation, transmission, and distribution domains
- Assess security features
- Specify security solutions and mitigation strategies
- Focus cyber security research and development priorities, and
- Identify and disseminate best practices.

Collaboration and information sharing will be critical to risk management, as the electric power industry is fragmented. This sharing of threat and response information will help organizations better identify and manage the risks to their enterprise.

3 Current Risk Management Practices

The development of the Framework should be informed by industry best practices and approaches, particularly in the area of Security Governance. Cybersecurity best practices and good governance transcend enterprises, infrastructure and components. Good governance should:

- Underscore the importance of operational risk assessments and use results to drive investment decisions to more uniformly protect infrastructures
- Directly support and be tailored to the organization's principle mission and functions (i.e., the security approach needs to fit the organization vs. fitting the organization to security). This implies the resultant Framework will have to be adaptable, flexible, and scalable, while still providing the designated level of security
- The security environment should be risk management based driving security policy, processes and procedures and including measures of effectiveness to understand and provide some level of quantification of security, and

- The Framework should not be limited by an appliance, a single vendor specific tool, or a technology specific based approach. The Framework should encourage the continual development and adoption of best practices that can evolve and take root within the Framework confines.

3.1 Are these practices widely used throughout critical infrastructure and industry?

In general, these practices are not widely used in either a formal or informal sense. This is true, in particular, for cybersecurity and security engineering practices. Security (or cyber) engineering is not as defined a discipline as either systems engineering or enterprise architecture (Urbaczewski & Mrdalj, 2006; Pereira & Sousa, 2004). In fact, security is still struggling to be considered a science in the sense of being able to conduct and, most importantly, to repeat experiments in the cyber domain. Guidelines have been developed providing some level of risk mitigation, most notable of which is the SANS Consensus Audit Guidelines. SANS provides a framework that can be used to evaluate risk, is crowd-sourced by Federal and DoD Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs), and represents effective defensive measures against results of actual attacks.

3.2 How do these practices relate to existing international standards and practices?

The SANS Critical Security Controls are directly related to NIST 800-53 and by default, ISO 27000 series. The NATO CIS Security Capability Breakdown can also be related to both NIST 800-53 and the ISO 27000 series. The Electricity Subsector Cybersecurity RMP was developed to meet the NERC and NRC standards. NERC standards cover Canada, the U.S. and Mexico's Baja Peninsula. Many of Northrop Grumman's manufacturing and laboratory facilities both domestically and internationally take consistent approaches to protecting our SCADA systems by utilizing these international standards and practices.

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

There is no consistent approach, but applying baseline solutions and resilient architecture approaches are important. At a minimum, the recommendations from the SANS Critical Security Controls can provide a standard and measureable approach to cyber defense and risk mitigation. The SANS Critical Security Controls are a risk management framework and a tool providing a consistent approach to the protection of networked systems. One other area for concern is application software, particularly those within the CIP boundary. If applications are not properly secured, specifically the code within applications is not secure; then applications remain extremely vulnerable to specific classes of threats.

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

The cyber domain is similar for all of us – the natural implication is that risk management concerns are similar, if not identical, across business or missions in different environments. Some attack vectors are liable to be more prevalent in certain sectors opposed to other sectors. For example, within the financial

sector denial of service attacks are more likely to occur than in the aerospace sector. Identifying and understanding the threat vectors will be important to aid in proper and focused cyber security controls. Even though the confidentiality, integrity, and availability requirements may differ across sectors, the controls implemented are similar. NIST has provided significant guidance in other sectors, and that same guidance will apply across critical infrastructure.

3.5 Which of these practices pose the most significant implementation challenge

All do, to some and varying degrees. Several of the practices are addressed below, as challenges are more pervasive in those areas.

For encryption and key management, the major impediments to wider use are issues concerned with cost and implementation. However, this impediment can be overcome particularly in cases where the key management is owned by the organization and not managed by a third party. For asset identification and management, the fully real-time knowledge of whom or what is on a given network is limited from a technology readiness standpoint. Although more straightforward to implement and use, most entities have not yet implemented robust incident handling approaches. Automated and semi-automated recovery and continuation technologies have not been fully developed nor integrated into mission systems. Some investigations into resiliency were carried out at Air Force Research Lab (AFRL) 13 years ago, but not much has been done in the interim.

Security engineering is not an exact science, so rigor and practice are still lacking. Carroll, Manz, and Greitzer (2012) pointed out that cybersecurity and security engineering suffers from a lack of more scientific methods, in particular cyber related experiments and the ability to reproduce experiments (confirming a scientific approach to security engineering). The Sherwood Applied Business Security Architecture (SABSA) (Sherwood, Clark, & Lynas, 2005) is a methodology for developing risk-driven enterprise information security and information assurance architectures, and for delivering security infrastructure solutions supporting critical business initiatives and leveraging work done in enterprise architectures by Zachman. These approaches utilize stakeholder and architectural perspectives to provide frameworks to analyze, select, and incorporate the many detailed approaches to security. Northrop Grumman has worked on using cybersecurity architecture views to decompose system security requirements and provide design templates that are useful for developing specific security solutions. These views include the SANS Consensus Audit Guidelines, the Fan™ (a Northrop Grumman defense in depth security view that concentrates on technology deployment across the layers of cyber defense), CyCape™ (a Northrop Grumman approach to categorizing cyber capabilities and is used for requirements, gap, and maturity analysis), and the NATO Cyber Defence Capability Framework (a risk based approach to examining cyber capabilities).

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

The standards and best practice approaches used are most often selected by organizations based on their ability to implement within cost and time constraints as prioritized by the operational risk factors. Formal measures of security effectiveness have not been developed; however, there is an effort within NATO and

NATO member nations to apply risk based measures of effectiveness against security practices. NIST's *Performance Measurement Guide for Information Security*, SP 800-55, Revision 1, provides a guide to assist in developing, selecting, and implementing measures to be used at the information system and program levels.

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

Not consistently. Maintenance of internal standards and best practices is based mostly on need and is addressed when there is demand for a standard or the modification of an existing standard. For those organizations that lack standards, their selection and implementation can be more based on events that drive (or point out) the need for a particular standard.

In many Electricity subsector organizations, for instance, lack of internal/comprehensive/resource standards results from a lack of understanding of cybersecurity and related risks. Adding to the challenge within this subsector, there are many of different types of organizations. The Electricity subsector is comprised of 3200 utilities, including 200 large companies, 1700 generating or transmitting power, 3000 municipals or co-operatives (CO-OPs), and more than 50 public utilities. Similar issues exist in other Critical Infrastructure (CI) sectors and drive the need for a comprehensive understanding of operational risk factors at the organizational level.

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

Organizations with robust and executable incident handling plans usually have a formal, and more importantly a tested escalation process. Many organizations are considering dynamic risk management (as technologies mature) as a means of remaining agile.

The Electricity subsector has escalation guidelines identified in NERC standards. These standards only cover electricity generation and transmission. Electricity distribution, operations are regulated by the state/local/TT government.

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

Compatibility with current and potential international standards should be considered by NIST. Northrop Grumman has supported the development of the NATO CIS Security Capability Breakdown and has used this on several occasions to evaluate capability and risk. Additionally, the European Union recently published a draft network information security (NIS) directive that is applicable to private industry and ultimately aimed at improving information-sharing and cybersecurity. These international efforts can help inform the development, particularly as to international compatibility, of the final NIST Framework.

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

A final Framework that helps improve network and information security for critical infrastructure can also serve to better protect privacy and civil liberties. Current Government standards and processes provide sound principles for safeguarding privacy and personally-identifiable information. These standards and

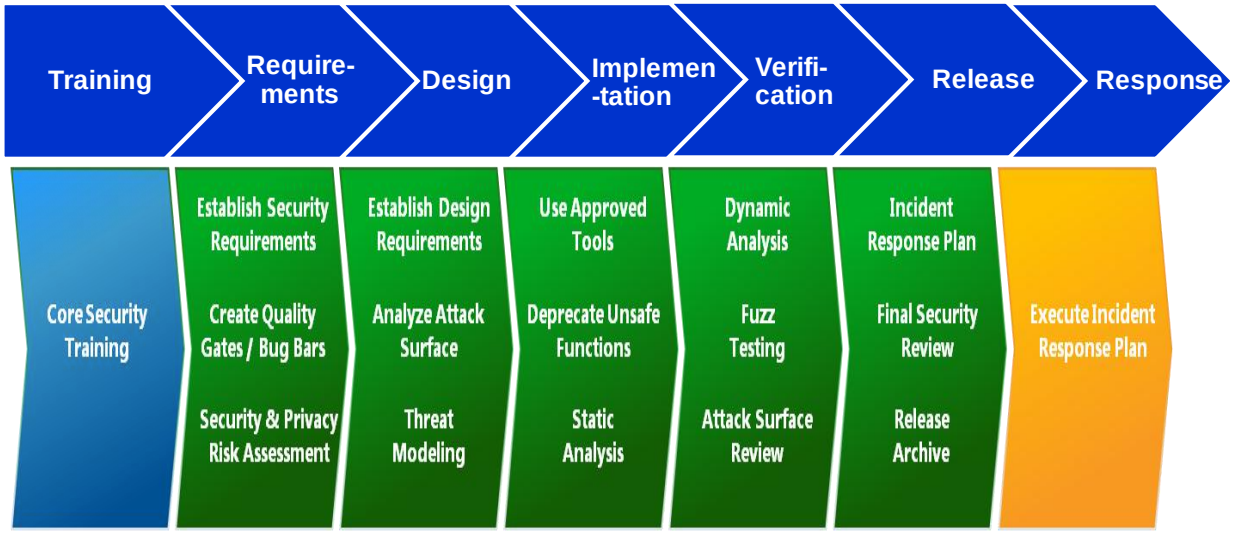
processes should be considered and appropriately incorporated with new legislative and regulatory efforts. Additionally, increasingly-available redaction tools can serve to enhance cybersecurity measures, particularly cyber threat information sharing, while effectively removing data that implicates privacy concerns.

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

Adoption and adaptation of the framework for incorporation into training/learning courses at the academic and corporate levels are important practices that should be considered. This should be accomplished being mindful of the goals of the National Initiative for Cybersecurity Education (NICE).

New applications should be developed using a Secure Software Development Lifecycle (SDLC) where security is built into the software code from the very early stages of development instead of as an afterthought.

There are multiple Secure SDLC approaches such as the one below:



Source: Microsoft Security Development Lifecycle, SDL Process Guidance, Version 5.2, May 23, 2012

Northrop Grumman also recommends that NIST consider leveraging the Open Web Application Security Project (OWASP) approach to secure software development as outlined on their web site: www.owasp.org.

We recognize NIST has an SDLC approach. Ultimately, the particular approach to Secure SDLC (NIST, Microsoft, Northrop Grumman, and OWASP) matters less than developing Industrial Control System (ICS) software code using a well-understood, consistently applied Secure SDLC model during code development to ensure security is built into the software.

3.12 Supply Chain

The sophistication of our enemies and their abilities to launch a cyber attack is growing, and their willingness to employ cyber attack is well documented as being persistent and relentless. Critical infrastructure supply chain systems will certainly be targeted by these cyber threats. The supply chain is a natural vector for an enemy to try to insert malicious functionality. This should be a key focus of NIST and industry in the development of the Framework.

4 Conclusion

At this juncture in our nation's history, Cybersecurity experts are being called upon to assist in the development of a fully functional framework to protect the nations Critical Infrastructure. Northrop Grumman is committed to partnering with the public and private sectors in the development and deployment of innovative and effective cybersecurity solutions to protect the nation's Critical Infrastructure. To this end, Northrop Grumman will support NIST in every dimension to advance the development of the NIST Critical Infrastructure Cybersecurity Framework to achieve a framework supporting protection of the nation's Critical infrastructure from cyber attacks.

As previously stated, the final Framework will benefit from thoughtful consideration of industry best practices and approaches, particularly in the area of Security Governance. On the cyber security playing field, best practices and good governance transcend across all areas that touch the cyber domain. Ultimately, our key recommendations include:

- Operational risk assessments should drive investment decisions to more uniformly protect infrastructures
- A baseline, minimal set of security controls needs to be recommended if not required to ensure a consistent risk picture and avoid a "weak link" in the critical infrastructure. We see significant value in beginning this discussion with the SANS Critical Security Controls
- The Risk Management Framework must include measures of effectiveness to understand and provide some level of quantification of security. There are industry best practices evaluating metrics. Results from a number of areas in including NIST, SANS, and NATO (for example) can contribute to this. Again, this will help to ensure a consistent and uniform lexicon and approach to measuring and reporting
- The Framework should not require an appliance, vendor specific, or technology specific based approach. This would encourage best practices to continue to evolve within the Framework confines, and
- The resultant Framework has to be adaptable and flexible, while still guaranteeing that minimal security profile.

Bibliography

5 Bibliography and References:

Carroll, T., Manz, D., & Greitzer, F. (2012). Realizing Scientific Methods for Cyber Security. In Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results (pp. 19–24). ACM.

Guinchard, A. (2011). Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy. *Journal of Strategic Security*, 4 (2): 75-96. http://scholarcommons.usf.edu/jss/vol4/iss2/6

Hallingstad, G., & Dandurand, L. (2011). Cyber defence capability framework. (NATO Reference Document 3060). The Hague, Netherlands: NATO Consultation, Command and Control Agency.

NICE. (2011). National Initiative for Cybersecurity Education Strategic Plan. Retrieved from http://csrc.nist.gov/nice/documents/nicestratplan/Draft_NICE-Strategic-Plan_Aug2011.pdf

NIST SP 800-39 (2011). NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.

Pereira, C. M., & Sousa, P. (2004). A Method to Define an Enterprise Architecture using the Zachman Framework. ACM Symposium on Applied Computing (pp. 1366–1371).

Sherwood, J., Clark, A. & Lynas, D. (2009) Enterprise Security Architecture: The SABSA White Paper. http://www.sabsa-institute.com/members/sites/default/inline-files/SABSA_White_Paper.pdf

Urbaczewski, L., & Mrdalj, S. (2006). A comparison of enterprise architecture frameworks. Issues in Information Systems, VII(2), 18–23. Retrieved from http://iacis.org/iis/2006/Urbaczewki_Mrdalj.pdf