CSCSS CENTRE FOR STRATEGIC CYBERSPACE + SECURITY SCIENCE

Developing a Framework to Improve Critical Infrastructure Cybersecurity

Response to RFI

The National Institute of Standards and Technology
U.S. Department of Commerce

[Docket Number: 130208119-3119-01]

April 8, 2013

Contents

Summary

The Center for Strategic Cyberspace and Science (CSCSS) is pleased to submit comments in response to the Request for Information (RFI) as requested by The National Institute of Standards and Technology as published in the of the Federal Register dated 21 February 2013, notated FR Doc. 2013-04413 and Docket Number: 130208119-3119-01.

Points of Contact

Dr. Marc Gartenberg
Chief Operating Officer
marc.gartenberg@cscss.org
(571) 451.0312 x 501 (Office)
301.747.0717

Mr. Richard Zalewski
President & CEO
richard.zalewski@cscss.net
(571) 451.0312 x702 (Office)

About CSCSS

The Centre for Strategic Cyberspace + Security Science / CSCSS is a multilateral, international not-for-profit organization that conducts independent cyber-centric research, programs, development, and analysis

Providing Leadership / Research / Defence to Cyberspace, defence intelligence, cybersecurity, and science

CSCSS address threats, trends, and opportunities shaping international security policies and national cyberspace cyber security initiatives.

As a Strategic Leader in Cyberspace CSCSS:

- Works jointly and in collaboration with key partners to address, develop, and define cyber technologies, cyber defense force capabilities, information dominance, National Critical Infrastructure / NCI, cyber concept operations and national cyber security
- Delivers practical recommendations and innovative solutions and strategies to advance a secure cyberspace domain
- Provide to CSCSS connectivity to government, private – public sector, agencies and academia to address cyber science, and cybersecurity, cyber-based research and development, studies, programs and projects, and initiatives, working to find strategic insights and solutions for cyberspace and cyber-centric issues faced today. Just as importantly the
- Advisory as a whole will also be looked upon to deliver leadership and advice to the CSCSS Management Team for the Centers overall strategic direction

The Centre for Strategic Cyberspace and Security Science | CSCSS is an international revenue neutral organization that conducts research, development and education in the area of cyber security, intelligence and science, while analyzing the threats and opportunities shaping cyberspace and internationally security policy initiatives.

Vision:

Our vision is to ensure that cyberspace remains open to innovation and the free flow of ideas, information and expression.

Mission:

Our mission is to conduct high-quality, credible, independent research and provide innovative, focused, realistic recommendations and initiatives.

Goals and Objectives:

CSCSS is determined to tackle the threats internationally, in collaboration with public – private, inter-agency partnerships that focus on the international aspects of cyberspace and security. This will be achieved by leveraging the use of research and resources while driving cyber security to focus on key issues, infrastructures, and coordinated preventative and responsive activities. CSCSS is committed to:

Strengthening cyberspace at an organizational, national and international level

Protecting key elements of the information and critical infrastructure which are crucial to the continued delivery of essential services and national security by preventing loss, through espionage of intellectual property and/or of sensitive information that could damage national and economic security and well-being reducing the vulnerability of national critical infrastructure to cyber warfare, cyber-terrorism and other threats.

The Challenge

There is still no systematic effort at strategic cyberspace planning for national security that is inclusive, deliberative, and integrative and defensive. Almost all cyber warfare capabilities developed to date are offensive in nature. The cyber security industry(vendor), as a group that is entrusted for defense, is generally lagging behind offensive capabilities of cybercriminals, terrorist organizations, cartels and nation sponsored and corporate espionage.

How it will Work

The articulation of a vision that describes a purpose but describing a destination is no substitute for developing a comprehensive roadmap for how we can protect cyberspace will achieve our stated mission, goals and objectives. CSCSS will bring the collective voices to the cyber arena at an international level through collaborative partnerships. CSCSS will provide leadership on issues relating to cyberspace, cyber warfare, intelligence, situational awareness, law and privacy.

As the threats to national-international security and economic growth increase and become more complex and global, members of intelligence communities, government agencies, and industry are working more closely together than ever before. We will foster and promote these associations and provide CSCSS as a common ground and strategic platform for interaction on these relationships though:

- Summits and Conferences
- Executive Level Briefings on cyberspace, cyber security and the persistent threat
- Joint (sponsored) Projects with private-public, agency partners
- Academic and Research Partnerships

Opportunity/ Value Proposition

In the global forum, we are the only independent, bipartisan, revenue neutral, strategic cyberspace and security science group in operation, working to develop international strategies for cyberspace and scientific based research and development that clearly articulate strategic cyberspace security objectives, goals, and priorities. As a group CSCSS deliver a globally focused, well-defined strategic objective. We present clear cyber and cyberspace based security goals for government, the public-private sector and industry. We will develop a multinational strategy that clearly articulates strategic cyberspace security objectives, goals, and priorities; establishing coordinated cyber-leadership and promoting CSCSS as capable and respected operational leader in cyberspace, cyber-warfare, cyber-security and research and development.

Recommendations

Based upon the questions raised in the RFI, our senior leadership analyzed and developed a draft paradigm that aligns and enables the goals established in the Executive Order 13626. During our analysis it became increasingly evident that the best solution might in fact be the easiest solution, namely taking existing paradigms and honing them into a model of maturity which is clear and transparent. Taking this approach increases the likelihood of success by allowing personnel to maintain operational effectiveness with less likelihood of new required training, minimizing costs through an economy of scale.

Furthermore, we urge Federal Agencies to align with industry to form Non-Government Organizations (NGO) that will be useful to foster best-practices and spirited dialogue resulting in Rapid Prototype Solutions (RPS). These RPS can be expeditiously prototyped and outcomes would then become input to the next iteration of forward planning, enabling solutions that are “leading edge” in nature.

Through this evolutionary cycle, improvements can be built in rather than patched on after the fact, minimizing action time, thereby shortening responses to any zero-day exploitation. The key to success is making sure that communication channels are established, processes developed, and exercises put into place ensuring the effective use of those channels – with metrics captured along the way for analytical assessment as well as using them for reporting results to senior agency management officials through high-level rolled up “green, yellow, red” scorecard. Lessons learned and best practices can be instilled through continuous monitoring, resulting in a dynamic, flexible and resilient model.

The Basics of the continuous monitoring model is shown below in Figure 1.

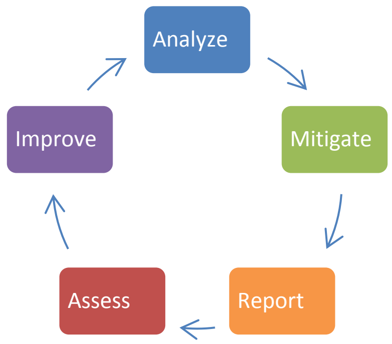
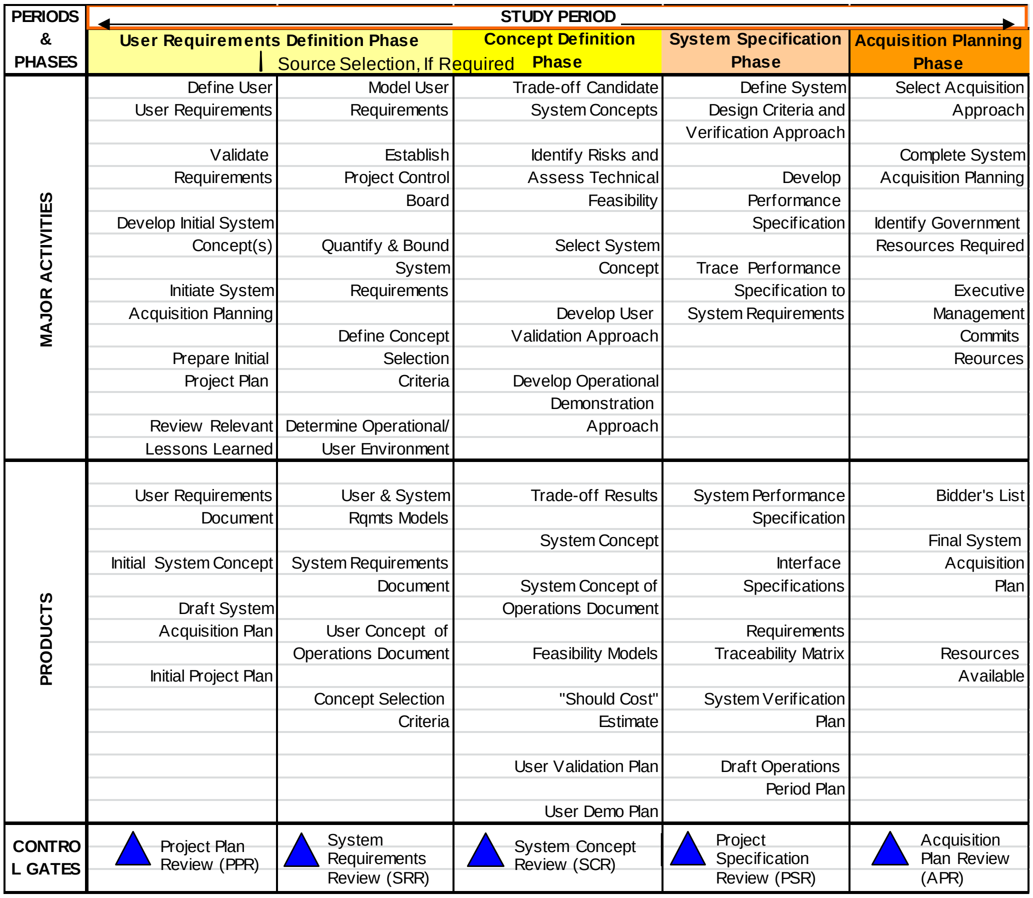


Figure 1

In addition, CSCSS strongly encourages utilizing the Managing Agency Program Methodology Model for process development and improvement, which lead to an enhanced Return on Investment and scales accordingly. This is depicted in Figure 2 below.



PERIODS & PHASES	STUDY PERIOD				
	User Requirements Definition Phase	Source Selection, If Required	Concept Definition Phase	System Specification Phase	Acquisition Planning Phase
MAJOR ACTIVITIES	Define User User Requirements	Model User Requirements	Trade-off Candidate System Concepts	Define System Design Criteria and Verification Approach	Select Acquisition Approach
	Validate Requirements	Establish Project Control Board	Identify Risks and Assess Technical Feasibility	Develop Performance Specification	Complete System Acquisition Planning
	Develop Initial System Concept(s)	Quantify & Bound System Requirements	Select System Concept	Trace Performance Specification to System Requirements	Identify Government Resources Required
	Initiate System Acquisition Planning	Define Concept Selection Criteria	Develop User Validation Approach		Executive Management Commits Reources
	Prepare Initial Project Plan	Determine Operational/ User Environment	Develop Operational Demonstration Approach		
	Review Relevant Lessons Learned				
PRODUCTS	User Requirements Document	User & System Rqmts Models	Trade-off Results	System Performance Specification	Bidder's List
	Initial System Concept	System Requirements Document	System Concept	Interface Specifications	Final System Acquisition Plan
	Draft System Acquisition Plan	User Concept of Operations Document	System Concept of Operations Document	Requirements Traceability Matrix	Resources Available
	Initial Project Plan	Concept Selection Criteria	Feasibility Models	System Verification Plan	
			"Should Cost" Estimate	Draft Operations Period Plan	
			User Validation Plan		
			User Demo Plan		
CONTRO L GATES	▲ Project Plan Review (PPR)	▲ System Requirements Review (SRR)	▲ System Concept Review (SCR)	▲ Project Specification Review (PSR)	▲ Acquisition Plan Review (APR)

Figure 2

Appendix A – General Questions from RFI

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

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

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?

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

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

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

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

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?

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

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

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?

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

Appendix B – Framework Questions from RFI

Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. What additional approaches already exist?

2. Which of these approaches apply across sectors?

3. Which organizations use these approaches?

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

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

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

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

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

9. What other outreach efforts would be helpful?

Appendix C – Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- Separation of business from operational systems;
- Use of encryption and key management;
- Identification and authorization of users accessing systems;
- Asset identification and management;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;
- Security engineering practices;
- Privacy and civil liberties protection.

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

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

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

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

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

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

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

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

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

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

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

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