Response to Request for Information (RFI), Docket Number 130208119-3119-01

U.S. Department of Commerce

National Institute of Standards and Technology

Diane Honeycutt
National Institutes of Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899
cyberframework@nist.gov

Submitted by:

SafeGov Inc

6074 Wynn Jones Rd E

Port Orchard, WA 98366

www.safegov.org

Purpose

The purpose of our response is to advocate that NIST in the development of a Cyber Framework for critical infrastructure adopt specific concepts outlined in the Organization Cyber Risk Management Framework. SafeGov.org developed and released this framework in conjunction with the National Academy of Public Administration on March 26, 2013. As originally constructed, the Organization Cyber Risk Management Framework applies to the management of government information systems, as well of those of supporting contractors, but the information security and risk management principles upon which the framework is founded apply equally to the private sector.

Given the shared importance of information security and risk management for critical assets across both the public and private sectors, SafeGov.org is encouraged that NIST is considering critical infrastructure in both the public and private sectors.

Introduction to SafeGov.org

SafeGov.org is a forum for IT providers and leading industry experts dedicated to promoting trusted and responsible cloud computing solutions for the public sector. By fostering a more comprehensive understanding of cloud technologies, including their benefits, capabilities, and limitations, SafeGov.org works to empower government users to make well-informed procurement choices from the growing universe of marketplace offerings.

Background

This response focuses on the second major area for consideration outlined in NIST's RFI on developing a framework to improve critical infrastructure cybersecurity: the "Use of Frameworks, Standards, Guidelines, and Best Practices." As stated above, SafeGov.org views the establishment of a secure baseline; the Organization Cyber Risk Management Framework; and the Organizational Cyber Risk Indicator as critical inputs to the development of a Cybersecurity Framework. The Organization Cyber Risk Management Framework promotes the creation of an adaptable, threat- and vulnerability-oriented approach to cyber risk management that is equally applicable to the public and private sectors, including critical infrastructure. This framework was first released in a report titled *Measuring What Matters: Reducing Risk by Rethinking How We Evaluate Cybersecurity.*

The Organization Cyber Risk Management Framework was designed to provide a new way for government to improve and evaluate the maturity of information and information systems in compliance with FISMA. It encourages the creation of an improved risk management feedback loop involving senior agency leaders and IT managers, Inspectors General, and third-party certification and accreditation organizations. In developing this framework, the SafeGov.org team consulted the U.S. Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), as well as numerous government and industry stakeholders.

The use of this risk management framework rests on the establishment of a secure baseline, which includes Critical Security Controls and automated continuous monitoring, diagnostics, and mitigation, as well as the creation of a threat model. In evaluating risks to information and information systems above and beyond this security baseline, the framework also calls for the evaluation of information security capabilities across ten domains of information management. These domains acknowledge the interconnections between technical capabilities, organizational policies and processes, and personnel capabilities. They include:

1. Asset, Change, and Configuration Management;

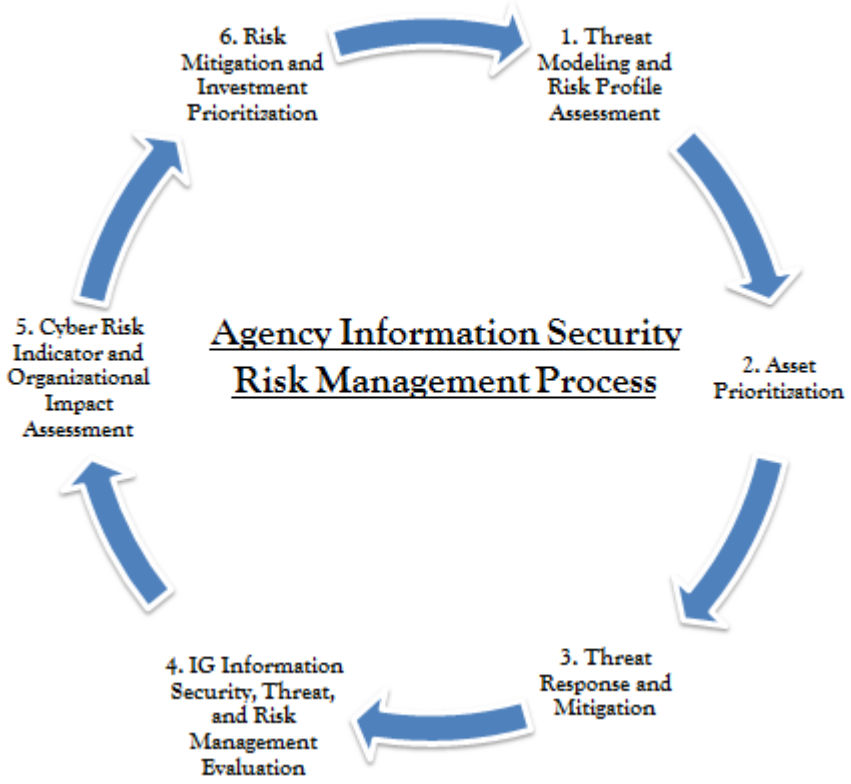
2. Access Management;
3. Identity Management;
4. Data Management and Protection;
5. Threat and Vulnerability Management;
6. Situational Awareness;
7. Information Sharing;
8. Workforce and External Dependencies Management;
9. Incident Response, Monitoring, and Continuity of Operations (COOP) Planning; and,
10. Program Management.

The framework promotes the use of independent third-party assessment organizations to verify the technical implementation of the secure baseline and other appropriate technical controls. The Federal Accounting Standards Advisory Board (FASAB) or a similar board could establish and agree upon generally accepted security principles for critical infrastructure in accordance with the above information security domains which would factor into the overall framework evaluation process.

Finally, the framework calls for the creation of an Organization Cyber Risk Indicator, a quantitative measure that would measure an organization's cybersecurity capabilities against known threats and vulnerabilities. When combined with robust cross-sector information sharing, this framework would enable a flexible and comprehensive means of addressing cyber risk management. The use of an approach that is broadly applicable across the public and private sectors would assist in protecting all critical national assets—public and private—and promote critical information sharing.

Summary of Organization Cyber Risk Management Framework
The framework is designed to foster continuous feedback among agency leaders, Inspectors General, and other oversight organizations. It does this by linking the central features of any comprehensive cybersecurity strategy (including agency threat assessments, risk mitigation action plans, information security management, and recommendations from IG information security evaluations) to agency cybersecurity investments and strategic management. This is easily transferable to critical infrastructure by substituting the company leadership, board of directors, and independent auditors for government personnel.

In order for agencies to transition to the risk management framework approach, the framework advocates that a fundamental set of capabilities (a secure baseline) must be in place that encompasses automated continuous monitoring, diagnostics, and mitigation, as well as the implementation of Critical Security Controls. Once these baseline practices are in place, agencies (and same in the case of critical infrastructure) should develop a clear understanding of the threats they face in their current operating environment, and how those threats could be realized. A strong threat model, which includes an agency's current and future operating environment, is critical to any effective risk management strategy. Once the threat model is developed and applied, agency leaders should identify key organizational mission priorities and map these priorities to critical assets and essential functions. Only by defining organizational mission priorities, known threats, critical assets, and essential functions can agencies determine their desired risk profile and the appropriate controls required to address those threats.



Different agencies and different sectors will face different threats and must, therefore, tailor their risk mitigation strategies to their individual needs. The public health analogy works here as well. Some of us need to do little more than engage in good personal hygiene (the baseline), while a few of us who are more at risk need to take additional steps to protect ourselves and the larger community.

In the second phase, IGs (or private sector auditors) will be able evaluate the maturity of the processes associated with information security, threat mitigation, and risk management based on the department or agency's chosen risk attributes and security controls. (NOTE: In the case of the private sector, the evaluation could be conducted in conjunction with internal audit groups and/or the external auditors.) External third-party audits may not be necessary or useful for all sectors and should not be universally required in the Cybersecurity Framework. The FASAB, to which companies already prepare statements in accordance with collaborative and voluntary standards, or a similar board could establish and agree upon generally accepted security principles for critical infrastructure. These principles would describe capabilities and risk attributes of critical infrastructure entities—not define processes or technologies used to achieve them.

The evaluation process will be outcome-oriented, draw upon live and scenario-based tests of information systems, and result in a prioritized list of recommendations for risk mitigation. These tests could be performed by independent third-party assessment organizations to maximize efficiencies and fill existing skill gaps in the case of certain types of critical infrastructure entities. Together, this approach is intended to facilitate communication within agency management, especially among CIOs and the IGs, to address the identified deficiencies. The evaluation will be conducted across ten separate

domains of information management to acknowledge the interconnections between technical capabilities, organizational policies and processes, and personnel capabilities.

In the final phase, security officials will calculate an organization cyber risk indicator by using a formula that aggregates the measured outputs of the IG evaluation process. The cyber risk indicator reflects the capacity of an agency to manage threats based on their existing operating environments and organizational priorities. Agency leaders can then use this cyber risk indicator alongside a list of prioritized risk mitigation recommendations to address ongoing vulnerabilities and improve how they manage risk and implement information security controls. By making agency leaders more aware of the evolving threat environment and their own risk mitigation capabilities, these processes will help them make better operational decisions, more effectively target their information security investments, and plan for the future more strategically.

Applications of the Framework for Critical Infrastructure

As conceived, this framework identifies key concepts and processes that are applicable for both private and public sector entities. In creating a Cybersecurity Framework for critical infrastructure, NIST should first identify a secure baseline that all designated critical infrastructure providers, as well as critical government assets, should meet. The Organization Cyber Risk Management framework suggests that these baseline requirements include the implementation of automated continuous monitoring and mitigation and the Critical Security Controls. To eliminate vulnerabilities above and beyond these requirements, specific standards and capabilities pertinent to the ten information security management domains could be developed and implemented. In some cases, these standards already exist and would not need to be developed. Desired risk attributes and corresponding information security management capabilities could be determined on a sector-specific basis or, in some cases, on a more tailored basis according to the type of entity or essential functions in question.

The framework also advocates that organizations develop a threat model as a foundation for risk management decisions and improvement to existing information security protections. This threat model could identify sector-specific threats, as well as acknowledge broader threats across the national security ecosystem. Finally, the Organization Cyber Risk Management Framework calls for the use of an Organizational Cyber Risk Indicator, which is intended to help an organization's senior leadership evaluate existing vulnerabilities and risk management decisions against known threats.

Beyond these elements, it is important that the Organization Cyber Risk indicator incorporate consequence information in order to prioritize the types of infrastructure and contextualize threat and vulnerability information. In addition, a cohesive information sharing construct should also be created to facilitate the communication of threats across and within sectors. The nature of this system is outside the scope of the Organization Cyber Risk Management Framework, but should be included in the further development of a cyber risk management approach.

Recommendations for Stakeholder Outreach

The Organization Cyber Risk Management Framework was developed using an iterative and collaborative approach to leverage the input of more than 20 senior government and industry IT leaders. We began by creating a draft framework that identified key themes by drawing from the work of multiple entities, including NIST, DHS, DOE, GSA, and OMB. The draft framework was shared with key

stakeholders, including government policymakers and technical experts, private industry experts, association representatives, and subject matter experts working in non-governmental organizations.

More outreach around the Organization Cyber Risk Management Framework should be conducted. Other stakeholders can provide invaluable input to help refine the framework as well as ease implementation of the new approach. For instance, additional Inspectors General, members of Congress, state government officials, and, in the case of the private sector, owners and operators of critical infrastructure, sector-based organizations (Information Sharing and Analysis Centers (ISACs) and Sector Coordinating Councils (SCCs)) and audit organizations and associations should be consulted as the framework evolves. State governments and their CIOs, in particular, are a vital stakeholder group given their role as implementers of federal government programs, many of which are covered by federal statutes, policies and guidelines including the Federal Information Security Management Act (FISMA).

The CIO Council, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and sector coordinating councils such as Electricity Sub-Sector Coordinating Council will be important entities to help orient stakeholders to the new approach, and offer technical assistance to support implementation of the framework.