Booz | Allen | Hamilton

8283 Greensboro Drive
McLean, VA 22102

April 8, 2013

The National Institute of Standards and Technology
Attn: Ms. Diane Honeycutt
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Request for Information—Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

As cyber threats grow and the lines between types of attackers, attack techniques, and motives continue to blur and evolve, the need for more innovative approaches to cybersecurity increases. The nation's critical infrastructure sectors and component organizations require a risk-based framework for measuring, managing, and maturing cybersecurity practices across the dimensions of people, processes, and technology. Organizations simply cannot protect all assets, systems, and functions, particularly when the threat landscape is constantly evolving. However, a clear understanding of business priorities can inform a well-crafted and proactive approach to allocating resources in a targeted manner. A well implemented framework of this nature should enable a diverse community of governments and businesses to more confidently push forward in attaining ambitious business goals and protecting infrastructure from potentially damaging cyber events.

We have shaped our cybersecurity viewpoint at Booz Allen Hamilton (Booz Allen) through decades of partnering with government and commercial organizations in the U.S. and around the world, to address the most challenging and sensitive issues related to protecting information, businesses, and missions. For example, we have been supporting the National Institute of Standards and Technology for more than 12 years and have supported efforts to develop foundational cybersecurity standards documents. We have also been working closely with Fortune 500 corporations to strengthen their cybersecurity programs through the adoption and assessment of foundational and enabling security practices. Our breadth and depth of understanding continues to evolve through our active engagement with industry (e.g., financial, energy, health), with sector leads, and with all facets of the federal government. As the National Institute of Standards and Technology (NIST) works with the Department of Homeland Security, the Sector-Specific Agencies (SSA), critical infrastructure owners and operators, and others to build the Cybersecurity Framework, NIST should consider the following principles:

- **Keep it Agile and Adaptive.** Cybersecurity practices within such a framework must be efficient and effective in dealing with current and future threats and vulnerabilities, cultural shifts, business needs, and technological advancements. At the same time, they must enhance the overall preparedness and resilience of critical infrastructure and reduce risk to a sector (and the nation). A one-size-fits-all "checklist" of controls runs counter to this idea and is limiting, as different sectors have different priorities. Instead, a framework that "adjusts" to the unique operating and risk environments of various business types—while still maintaining an overall common foundation—has the potential for enhanced cybersecurity at the sector-level as well as for the nation.
- **Enable Enterprise Risk Management.** The future of cyber risk management allows one to readily ascertain the maturity of an enterprise's security posture within the context of the business and across the dimensions of people, process, and technology. Enterprise-wide cyber risk management requires the ability to communicate the story of how effectively the cybersecurity program is protecting the business, as opposed to merely protecting information technology (IT) systems. Furthermore, providing this security maturity information to executives, middle managers, and operators throughout the organization—with the appropriate messaging and level of detail—empowers everyone to do their part in managing risk and continuously improving resilience as part of a collective and comprehensive approach.
- **Promote Repeatable Measurement.** The Cybersecurity Framework must enable organizations to assess the appropriateness and effectiveness of current security controls against identified threats (across multiple dimensions) within the context of a given organization's business goals, objectives, and risk tolerance. A thoughtful combination of qualitative and quantitative measures embedded into the framework should be clear and obvious to implementers and assessors; facilitate a common understanding of risk from the perspective of multiple stakeholders; and enable consistent measurement of controls in a manner that communicates to the business how effectively aligned the security program is to the greater enterprise. Tools and techniques that enable repeatable measurement allow an organization to report on progress and react faster to security challenges.

Booz Allen has a long history of working cybersecurity-related challenges across the public and private sectors, including information assurance, cybersecurity operations, cyber threat intelligence, data analytics, advanced malware detection, and communications security. We operate throughout the entire lifecycle of cybersecurity, partnering with clients in diagnostic and strategy-setting, designing targeted capability solutions, and finally, implementing and operating those solutions. We have and are continuing to evolve our cybersecurity practices based upon internal and external (i.e., client-based) lessons learned, all commensurate with the evolving threat landscape. The following includes Booz Allen's answers to the questions in the Request for Information from February 26, 2013.

****

Current Risk Management Practices

Organizations must manage critical infrastructure cybersecurity risk with an eye towards protecting business processes and information from activity that could adversely impact confidentiality, integrity, and availability. Managing cybersecurity risk in critical infrastructure cannot be grounded solely in an asset-based, compliance-driven approach, because this limits the agility and flexibility needed for success. Compliance is important, but only to the extent that it has a demonstrable impact on reducing the potential risk to the business, and ultimately the sector and the nation. NIST should encourage a programmatic, risk-based approach to security that allows informed decision-making based on threat, vulnerability, and business impact—holistically tying elements of an enterprise together to ensure security is attuned to precise business needs and allowing critical functions and services within a sector to operate as intended. While the risk framework may allow organizations to drill down to the system or asset level, the framework must be able to characterize cyber risk in terms of operational risk or impacts to nationally-important functions and services that make infrastructure "critical."

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

The simple, yet challenging, stages in improving cybersecurity practices across critical infrastructure can be summarized as: "know what you have," "know where you're going," and "know when you're achieving success."

The initial challenge to improving cybersecurity is to "know what you have." Before critical infrastructure protections can be effective, it is essential to move beyond a system or component focus to a paradigm that accounts for all the major inputs to a security program—the people, processes, and technology. Adversaries are highly motivated to find the weakest link in a security system, whether it is untrained people, an insecure process, or a misconfigured piece of technology. Thus, "knowing what you have" must include each of these areas. The technology component is a challenging piece, as organizations must truly account for all network-connected technology assets and develop a full understanding of how these assets are accessing the network in today's always-on, ubiquitously connected, environment. Similarly, organizations must understand threats to its business processes that may come from the technology—either because of vulnerabilities in the technology; vulnerabilities inherent in how the technology is used; or inadequate knowledge, skills, or abilities within the workforce.

The next challenge for organizations is to "know where you're going." Developing appropriate target metrics for incremental and overarching improvements will provide another hurdle as organizations work to consistently describe risk tolerance and convey risk-based mitigation decisions. Finally, there is the challenge of "knowing when you're achieving success." In order to make improvements, it is necessary to first be able to make consistent measurements. Appropriately and consistently assessing the current baseline of cybersecurity practices within a given sector or across multiple sectors, and in turn, assessing the efficacy of those practices for a given operational environment will present a challenge.

Technology continues to bring vast amounts of sensitive data together in large repositories and new processes are linking new organizations together (e.g., personal health information in health information exchanges). However, traditional challenges, such as cost, feasibility, and state-of-the-art technology will continue to impact the degree to which security practices and techniques are implemented in the critical infrastructure. Interconnectedness of environments continues to introduce multiple new threat vectors and continuously expand the attack surface of organizations within the critical infrastructure. Innovative approaches and new thinking will be essential to stay ahead of the changing threat environment and provide the highest possible level of security for the nation's most valuable functions and services. In addition, we must look beyond technical solutions at the people and processes necessary to enhance security cost-effectively.

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

Through our work with various critical infrastructure organizations across multiple sectors, we believe a cross-sector standards-based Framework for critical infrastructure should be:

- Agile to address 80-90 percent of the risk situations facing critical infrastructure;
- Flexible to support tailoring to the unique needs of sectors;
- Specific (yet not prescriptive) to promote consistent characterization, assessment, and mitigation of risk across the sectors;
- Adaptable to adjust to technology innovation and the evolving threat environment for each sector; and
- Customizable and pertinent to critical infrastructure business models and operations, enabling the operational environment to drive and independently manage risk and investment strategies.

There are a number of challenges to accomplishing the goal of building a cross-sector standards based Framework. Building consensus on a standardized way of approaching cybersecurity and managing risk across multiple sectors will be difficult. Organizations and sectors have different missions, business imperatives, and risk profiles. For example, the Financial Services Sector recognizes the benefits derived from working together to strengthen the overall security of the sector. In other cases, such as the Oil and Gas subsector, a competitive spirit remains among organizations, making coordination on security practices less common. Finally, because sectors are at varying levels of maturity, it may prove challenging to gain a common understanding of the current landscape of effective practices, standards, and approaches, and elevate the discussion from system-level risk management to a programmatic view, which is focused on maturing an organization's cybersecurity capabilities in a dynamic threat environment.

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?*

Booz Allen has taken a proactive and aggressive approach to defining and implementing a set of cybersecurity best practices. Our approach is grounded in a philosophy of measuring, managing, and maturing. We have defined and deployed for ourselves and several of our clients a comprehensive and risk-based maturity model, which addresses functional (e.g., threat intelligence, application security, infrastructure & mobile security, etc.) and enabling (e.g., governance, policies, awareness & training, change management, etc.) controls in a balanced fashion. At Booz Allen, cybersecurity is everyone's responsibility. We formally communicate cybersecurity policies to employees and make them readily and clearly available. Cybersecurity awareness training on security policies, procedures, and associated risks expands and deepens the knowledge of our employees, enabling them to make appropriate decisions. Electronic enforcement of cybersecurity policies further assists in ensuring that user activities are in compliance.

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

Organizations locate their cybersecurity risk management program in a variety of offices including, but not limited to, the Chief Information Officer (CIO), Chief Information Security Officer (CISO), and General Counsel. Placing cybersecurity risk management within the Office of the General Counsel is becoming much less common and we have observed many forward-leaning organizations elevate the CISO role (and the associated cybersecurity responsibilities) from underneath the CIO to become a direct-line report to the Chief Executive Officer (CEO) or Chief Financial Officer. No matter where the cybersecurity program/office is located, a proven best practice is to establish strong linkages with the organization’s other risk management and security functions to holistically manage enterprise risks. Booz Allen’s own physical and cybersecurity risk management functions are linked with other enterprise risk management efforts (including financial and ethics risk management) to holistically manage risk. These principles are part of our maturity model that is rooted in the philosophy of *measuring*, *managing*, and *maturing*.

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

Organizations typically define risk differently based on the level of the organization and the industry type. At the lowest levels of any type of organization, most managers and operators view risk from an operational and detailed standpoint and in terms of confidentiality, integrity, and availability—with one of those factors given special preference depending on the industry type. For example, in healthcare patient facilities, availability concerns are paramount, as operational disruptions could result in loss of life. Employing a healthcare compliance lens, confidentiality of protected health information is critically important. At these same lower levels of the organization, there tends to be a narrow IT-focused view of the world. Risk is generally defined in terms of risk to operations while cybersecurity risk is defined in terms of controls implemented and potential impact to a given cyber asset or system.

At higher levels of an organization, executives and board members view risk differently, considering strategic, operational, compliance, and reputational types of risk. At this level, component risk registers are gathered from throughout the enterprise to provide a summarized view of risk—typically filtered through a true enterprise risk management function. These individuals look at a “Top 10” risk list (or something similar) and gauge how these risks could impact short, medium, and long-term business goals and objectives. Currently, cybersecurity risk is typically a small (but growing) component of this agenda.

At these higher levels of the enterprise, we see organizations taking a maturity-based view of capabilities as they relate to risk management—an approach that allows for cross-cutting performance assessments. For example, a maturity view can readily help answer the question, "How effective are we at monitoring insider threats?"

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

Within the strategic or enterprise risk management space, the agenda usually consists of five to ten risk types that the enterprise needs to manage (e.g., reputation, credit, fraud). Typically, cybersecurity risk is a subset of an "IT" risk type, but sometimes cybersecurity does stand on its own as an enterprise-level agenda item. Cybersecurity often rises to the forefront only in the event that the enterprise has experienced a negative cyber event. Often, the lack of executive-level attention is due to a broken process at a lower level in the organization, where security and IT organizations lack the skill, desire, or resources to integrate risk information with the business and subsequently pass that information up the organizational hierarchy in meaningful ways. Therefore, what is potentially valuable security-related information for executives, remains hostage at lower levels of the organization due to poor risk management and communication processes.

From an industry-specific standpoint, the financial services community has generally elevated the CISO to new levels of importance, so we see cybersecurity gain more attention at executive and board meetings. In the electricity subsector, there has been less of an evolution in cybersecurity risk prominence, as management is still hyper-focused on operational availability. While in healthcare, we see a trend in cybersecurity risk appearing on the enterprise risk agenda, especially with the mobile device movement and the push for electronic health records.

There is great opportunity to evolve the status quo. For example, more mature integration of cybersecurity and business organizations—to the level of embedding representatives within business units—is an effective start, from Booz Allen's experience. Once better communication and security-to-business integration is happening, more ideal risk management dialogue typically takes place.

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

A myriad of sources are available to manage risk at different levels of the organization. The unfortunate history of these guidance documents is that no one framework or standard is universally valuable and applicable to managing risk at all organizational levels—management, operational, and technical. Another concerning trend we see is that controls-based "checklist" standards are substituted for robust risk management processes. Such an approach reflects the fact that many leaders view compliance or certification as equal to security, when in reality, security must go beyond compliance.

At the management level, there are several guidance documents that advise on programmatic constructs and high-level controls that are required for comprehensive cybersecurity. The most overarching and flexible guidance comes from International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC)

27001 and 27002. Many other national and international standards have adopted this framework outright or used it as a basis for additional customization. Several others exist for management purposes (e.g., Control Objectives for Information and related Technologies, COBIT, NIST Special Publication (SP) 800-39), but they are designed more for devising programmatic constructs and cannot readily permeate into operational and technical parts of security activities. A seemingly endless set of guidance exists that blends the operation and technical levels (e.g., NIST SP 800-53, Health Information Trust Alliance (HITRUST) Common Security Framework, Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) standards, and many others). All of these are largely targeted below the management level, and many are sector-specific.

In addition, Booz Allen has developed a comprehensive, maturity model that leverages the best attributes from the most well-known cybersecurity standards from across sectors. Our approach is designed to enable organizations to measure, manage, and mature their cybersecurity capabilities and enhance overall threat preparedness and resilience. The maturity model addresses functional (e.g., threat intelligence, application security, infrastructure & mobile security, etc.) and enabling (e.g., governance, policies, awareness & training, change management, etc.) controls in a balanced fashion and is deployed using a risk management approach. We have been using this maturity model with a variety of critical infrastructure sectors and through continued collaboration and partnership with industry have continued to tailor and refine the methodology to meet the unique needs of sectors and organizations.

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?*

A variety of existing regulatory requirements exist (e.g., Health Insurance Portability and Accountability Act, Sarbanes-Oxley, Gramm-Leach-Bliley, Chemical Facilities Anti-Terrorism Standards, State data breach laws, and several others), which impact a variety of critical infrastructure sectors. Compliance with this vast array of regulations is not only complex, but organizations often—due to lack of resources, confusion, and regulatory fatigue—do not achieve intended results. Existing regulations, which promote a checklist approach, do not necessarily enhance cybersecurity, as they lack the flexibility and adaptability necessary to meet current and future cyber challenges.

An inventory and review of current cybersecurity regulatory requirements can enable the identification of common themes, unique requirements, and potential gaps, which the Cybersecurity Framework should address. Such an activity would also help to ensure that regulators are able to incorporate the Framework into existing regulatory regimes, thereby reducing the cost of compliance and enabling critical infrastructure to focus on improving their cybersecurity posture.

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

Much work remains to be done around the identification of cyber-related risks that have impacts across multiple sectors and may be magnified when realized in more than one sector. Infrastructures are closely intertwined and interconnected with ecosystems within ecosystems within ecosystems. Cybersecurity risks in one sector can translate to operational risks in other sectors and can ultimately introduce systemic risks to the nation. The highly diverse, distributed, virtual, and interconnected nature of the critical infrastructure and the constantly evolving threat landscape limit the effectiveness of traditional, bottom-up asset-based approaches to cybersecurity. An ecosystem approach to security is needed, which considers the whole enterprise (and multiple enterprises within enterprises) and the interdependent nature of business operations and functions. Such an approach makes cybersecurity a business-as-usual activity and ensures that cybersecurity is embedded in the organization's culture and is used to drive innovation and business growth through governance and risk management.

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

Performance goals vary greatly, depending upon the sector. The simplest viewpoint is to understand goal-setting and risk management decisions in terms of confidentiality, integrity, and availability. Of essential note is the need for the core business function, rather than the cybersecurity program/office, to define the specific goals and their relative importance. Only then, can the organization work together to meet both the mission of the critical infrastructure and the related security needs. For example, in the payer-provider component of healthcare, we see a rigorous focus on integrity for claims processing. Within the patient care part of healthcare, the acute delivery of services is vital—thus, availability is a top goal. Similarly, availability is a top focus in upstream and downstream operations for oil and gas companies. The idea of "convergence" is becoming increasingly prominent in balancing and setting business performance goals and cybersecurity risk management. As business leads integrate with the technical sides of the enterprise in establishing confidentiality, integrity, and availability goals, the cybersecurity and business continuity organizations can more readily serve these needs and meet stated performance goals.

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?*

As an organization we have a variety of regulatory reporting requirements (e.g., periodic filings with the Securities and Exchange Commission, the Defense Contract Audit Agency, the Internal Revenue Service), which we must meet. We have found that compliance with regulatory requirements is a necessary element of doing business and providing transparency into an organization's operations. At times, these requirements can be complex and resources must be dedicated to ensuring compliance. In addition, we have found that it is important to link our security practices together with our compliance efforts to enhance our overall ability to manage risk to the enterprise."

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

Standards organizations can play a key role in building consensus on levels of assurance and associated evidence sufficient for conformance acceptance. They can also provide a forum for reaching agreement on necessary and sufficient qualifications for assessors. This can be particularly helpful to level the field when business imperatives (e.g., strong competitive environment vs. a collaborative sharing environment) differ among organizations. In addition, development of an international standard, which presents agreed upon cybersecurity standards, has the potential to result in long-term cost savings by eliminating duplicative and conflicting requirements across multiple countries and a consistent baseline from which to understand risk across organizations.

<u>Use of Frameworks, Standards, Guidelines, and Best Practices</u>

Numerous cybersecurity guidance documents are currently in existence. A great deal of them are focused on system-level guidance and managing everything within the "IT sphere." Evolving the language and targeting this guidance towards a connection with the business will be an important step forward.

1. *What additional approaches already exist?*

Three cybersecurity frameworks in common use in addition to the NIST Risk Management Framework (RMF) are ES-C2M2, NERC-CIP standards, and ISO/IEC 27001 with ISO/IEC 27002. All provide a broad-based mechanism for evaluating the maturity of enterprise cybersecurity functions. ES-C2M2 and the NERC-CIP standards were authored by subject matter experts in both cybersecurity and the electricity or electric power subsectors respectively, and therefore reflect both cyber and operational concerns. All provide controls across a variety of security domains or families. ES-C2M2 measures maturity of process. NERC-CIP standards focus on programs and process. ISO/IEC focuses on process and technology. All, with differing levels of tailoring, can be applied to multiple critical infrastructure sectors (and subsectors, where appropriate). None have a maturity model that considers the interlinked dimensions of people, process, and technology. For each, the focus is either compliance to stated controls or adherence to guidelines and principles—without explicit consideration of threats and an ultimate objective of demonstrated risk reduction.

We have also developed an approach that helps organizations measure, manage, and mature their cybersecurity programs. The model encompasses not only technology and analytics, but also business process engineering and human capital development. It also factors in the role that large, systemically critical organizations play in commercial markets and the economy. As a result, it has yielded tremendous insight into the ways companies identify and manage threats at a network level. The model has also yielded a new approach that revolutionizes traditional perimeter-based security by building on dynamic, tiered network structures. Our maturity model, which is deployed using a risk management approach is helping organizations (e.g., large financial, energy, and healthcare institutions) transform their cybersecurity programs from the ground up—and implement key components across all three dimensions of people, processes, and technology.

2. *Which of these approaches apply across sectors?*

It is likely that any of these approaches has a good deal of cross-sector applicability. Our estimate is that between 50-80 percent of a given documented approach would work in a cross-sector format, with some tailoring. Some frameworks such as ISO/IEC 27001 and 27002 can be applied to multiple sectors without signification modification because the standard is high-level and represents a collection of guidance similar to that found in the NIST RMF. Models such as ES-C2M2 or the NERC-CIP standards could be tailored for sectors beyond those they were intended for, or the concepts readily leveraged.

3. *Which organizations use these approaches?*

Almost every private sector organization uses some semblance of ISO as a base construct, and then modifies from there. In sectors where there is a regulatory requirement for a specific standard, such as NERC-CIP, that standard would take precedence as the "approach" to security. We have found a variety of institutions across multiple sectors are embracing a maturity-based approach that is flexible, adaptable, and easily tailored to the diverse needs.

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

Security management standards are not leveraged to their fullest. Cataloging of vulnerabilities and security controls get high visibility without the required threat context. This can result in a drive towards compliance with a checklist of controls with weak ties back to the reduction of risk. The approaches referenced do not effectively integrate people and processes with technology and hence security compliance is decoupled from security operations.

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

The greatest utility increase we envision is the creation of a means to consistently characterize cybersecurity risk in terms of business risk. This requires a better characterization of the relationship between operations or mission, secure engineering and secure processes, including the humans that run and/or seek to disrupt the processes. Another key aspect is a means to consistently measure and demonstrate "sufficient" risk treatment in terms of the business rather than solely in terms of the state of the system. This requires having the ability to express risk tolerance in terms that go beyond IT system level metrics that deliver actionable data to system owners, and instead, build actionable metrics for business leadership. Finally, building consensus around mapping operational security or observable security to security engineering and compliance (e.g., agreement on factors that characterize current threat activity and whether or not the security plan is sufficient to meet organizational needs) is needed.

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

The base control types—identity and access management, training, policy, etc.—have a common foundation, but the sector-specific needs typically come out in the language that reflects the assets that need to be protected and the people that need to perform the activities. For example, in the NERC-CIP standards, "bulk electric system," "transmission operator," and "generator operator" are assets or roles unique to Energy Sector operations, and thus, that level of specificity would not be appropriate in healthcare cybersecurity guidance.

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

Sector-specific standards of practice are needed when using an existing risk management approach to ensure ease of use and maximum adoption by each sector. Risk profiles vary across the sectors and each sector has unique attributes, which must be considered. For example, the Electricity Sub-sector is highly concerned with the resilient operation of their control systems environment, whereas the Financial Services Sector is more concerned about information leakage and denial of service through their IT environment, and the healthcare sector is focused on working to reform operations and respond to mandates related to meaningful use.

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

SSAs and Sector Coordinating Councils (SCC) are essential to ensuring that approaches are developed in a collaborative and consultative way, take advantage of existing efforts, methodologies, and approaches, and tap into sector-specific expertise necessary to ensure that approaches are relevant to sector operations. SSAs and SCCs can help in a variety of ways including:

- Ensuring that a variety of subject matter experts from across a sector are identified and involved in developing and promoting the use of risk management approaches,
- Defining appropriate cybersecurity practices, which take into account the types of services and functions provided by the sector,
- Determining a sector-specific current state of practice and target state of practice, and desired sector risk profile,
- Building consensus on expressing sector-specific cyber vulnerabilities and risks,
- Assessing the efficacy of mitigation strategies, given a sector's unique challenges (e.g., legacy infrastructure, interdependence on external systems),
- Identifying or creating requirements, which appropriately balance the need for security with other customer needs (e.g., accessibility), and
- Protecting the sector collectively rather than as component parts through the development of a macro view of the sector's implementation of security practices to include "snapshots" of overall cybersecurity "health" of the sector.

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

NIST should continue to engage directly with critical infrastructure owners and operators to understand business drivers, current and emerging threats and vulnerabilities, risk management practices and limitations, and current performance measures. By working to understand the current landscape, NIST will be able to meet critical infrastructure owners and operators where-they-are, and put cybersecurity practices in the context of business goals and objectives. In addition, public and private sector efforts to expand cybersecurity awareness and training programs to include business partners and end users of critical infrastructure would be helpful. Each employee and decision maker in an organization has a role to play in enhancing the cybersecurity of the critical infrastructure and they need access to information regarding the importance of cybersecurity and actions they can take.

Specific Industry Practices

There are quite a few commonalities among industry practices. There certainly exists a base set of requirements that could and should be applicable across industries, and the future Framework should keep this as a principle. Based on what Booz Allen has seen across various sectors, it is very apparent to us that that framework must exude agile and adaptive characteristics that allow for each sector to make it uniquely conform to their needs.

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

The majority of the practices referenced in the RFI are universally implemented within the Financial Services Sector, where there is increasing maturity in the processes and technologies needed to implement such practices. The Oil & Gas Subsector also demonstrates increasing sophistication in employing these practices, likely due to its status—just like Finance—as being a top tier target. The convergence of security (cyber, physical, and business continuity) and the practice of "resilience" is still relatively immature, as organizations still struggle with historically siloed operations and lack of impetus for true integration, but rather focus on meeting or maintaining compliance for regulatory and/or audit purposes. Other industries (e.g., Water, Healthcare) are generally recognizing the importance of these security topics, but due to legacy mindsets, unawareness of the threat landscape, or funding realities, broad adoption or mature implementations are not as visible.

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

Several of these areas—particularly dealing with access, assets, monitoring, and response – are explicitly covered by a large cross-set of well-known standards (e.g., NIST SP 800-53, ISO/IEC 27001 and 27002, HITRUST). The degree of depth (e.g., implementation guidance) provided by any one of these standards varies, depending on the level of flexibility and precision intended by the standards' authors.

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

In our experience, the most critical factor in ensuring the overall success of a cybersecurity program is to structure the organization in a way that addresses cybersecurity from a proactive, enterprise risk perspective, not a system or asset-focused perspective. Booz Allen uses our dynamic defense model to organize security programs around five dedicated cybersecurity functions:

- **Prepare –** Develop threat scenarios, assess threats and vulnerabilities, and conduct simulated exercises
- **Prevent –** Reduce day-to-day incidents by addressing known vulnerabilities and exercising strong security fundamentals

- **Detect –** Perform proactive security monitoring at multiple collection points (e.g., servers, desktops, network devices) and aggregate data for analysis
- **Respond –** Mitigate incidents through an agile and coordinated response
- **Recover –** Integrate investigation, forensics, and continuous improvement functions

Using this construct, an organization can align staff to day-to-day operations, while other functions are dedicated to more strategic preparedness and prevention of future attacks. Once organized in this manner, measurement frameworks are applied to ensure each function is operating effectively against their specific mission in the areas of people, process and technology.

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

Organizing a security program around a proactive set of cybersecurity functions is critical for all sectors. Within each function, specific practices may be more applicable than other for a particular critical infrastructure sector. For example, under the "Prevent" function, a financial institution may pay particularly high attention to its secure software development practices, while a water utility may produce relatively little custom software. Additionally, some practices are applicable, but may not be implementable because of the lack of cybersecurity capabilities being offered by the vendors. For example, use of encryption and key management may be extremely difficult within industrial control system (ICS) environments due to the lack of built-in security features and low processing power. In these situations, other mitigating controls must be in place, such as physical segregation of an ICS network from an Internet-connected network. Booz Allen's approach when assisting our clients across a broad spectrum of subsectors is to leverage a cybersecurity maturity model that allows us to tailor a client's security controls and target maturity in a way that is specific to the risks they face within their sector.

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

Those that are typically centralized (e.g., monitoring, setting encryption standards or other foundational controls) pose less of a challenge. Those practices that are typically owned in a federated model (i.e., must be implemented by different parts of the business) pose the greater implementation challenge. Business units have unique needs that they need to customize or tailor practices to support or enable. If there is no incentive model for uniform adoption, this becomes problematic when looking at the aggregate implementation and created exposures. An example challenge practice is asset management, where a business may need to deploy a large scale of mobile devices or "beyond the corporate perimeter" technology—getting a central view of all business unit assets and the data that those assets use is very difficult. Identification and authorization of users accessing systems is harder for larger organizations typically since they have built up so many accesses over time. Asset identification and management is difficult for large organizations because many of their operations and systems are siloed and no repository identified as the system of record.

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

Most standards/guidelines within a company are based on a well-known construct (e.g., ISO/IEC 27001and 27002) and are tailored from there. We see extreme variability in the "level" of guidance. Some organizations simply have a high-level ISO-based capstone policy with little "how to" or "next layer down" knowledge associated with it. Other organizations have a plethora of detailed system configuration guides, but no organizing construct for tying it all together. In regulated industries (e.g., healthcare), we see standards implementation being driven by a desire to focus on mapping to regulatory requirements and successfully completing required audits.

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

Most are very ad hoc. The desire is there, but several realities interfere with standards generation. The first is the separation of business and the IT/cybersecurity organization. Legacy separation of these business units creates conflict and resource challenges when coming together to work on a standard, even if for the "common good." Second, there is a skillset shortage. Many organizations do not have experienced policy authors that articulate needs based on business-specific needs, nor for the realities of a complex business environment facing ever-increasing threat types.

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

Organizations that have a heightened awareness of the threat and risk environment often have formal escalation processes in place. Those organizations that take an enterprise approach to risk management seriously (and have IT/cybersecurity embedded as a key part of it) are typically better prepared to address cybersecurity risks. In addition, those organizations with a CISO (or CISO equivalent) that is near the top of the corporate hierarchy are typically better able to formally escalate and address severe cyber risks. Finally, formal incident response plans and playbooks at the organizational and Sector levels that are routinely exercised and used during real-world events further support and enable the escalation of cybersecurity risks.

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

Organizations have many goals and objectives beyond cybersecurity, one of which is to develop a positive workplace environment which contributes to attracting and retaining staff. Cybersecurity controls run the risk of eroding this environment when employees feel technology is being used to unduly monitor and control their actions and behaviors. Employees must continue to feel safe and comfortable in using IT for everyday business needs and (realistically) benign personal use without fear. In this light, it is particularly important that the organization communicates clearly to the workforce about the goal of the security program—protecting the organization from internal and external risks, as opposed to tracking employee behaviors as a personnel management function. It must be clear to the employees that the security program's mission is to protect the overall health of the organization, which directly benefits the employees themselves.

In addition, organizations have a responsibility to protect any information they must necessarily collect as part of conducting daily business. Whether it is employee or customer data, identification and authorization systems must uniquely identify individuals, typically using a database of personally identifiable information (PII). If breached, such a database can cause financial harm and/or embarrassment to the record subjects, with the organization potentially liable, particularly in industries such as health and finance.

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

Multi-national organizations often find that local laws and regulations differ greatly between countries and trade zones. These differences can directly impact the implementation and configuration of cybersecurity solutions. For example, European Union countries have very specific regulations protecting personal identities and associated identifying information (e.g. usernames, IP addresses), while the United States provides relatively fewer restrictions on data generated on an organization's business network. The Framework should build in flexibility regarding these differing international laws and regulations by not prescribing specific solutions, but instead should be a maturity-based framework that defines the expected security practices for a given maturity level, while still allowing development of custom-tailored solutions.

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

Like their missions, the privacy and civil liberty practices and obligations of critical infrastructure organizations vary wildly. A baseline approach aimed at creating organizational safeguard requirements and PII breach response requirements would allow organizations to properly allocate resources for privacy and civil liberty concerns. A baseline approach with a set of expectations for all PII data would also allow basic privacy and civil liberty protections to be engineered and integrated into the system development lifecycle. This approach should address the issues raised by the Fair Information Practice Principles (also see NIST SP 800-53 Appendix J). Transparency should be provided to record subjects defining what data is collected, how it is used, and for how long it is used. Organizations should provide mechanisms to allow record subjects a way to access records and correct inaccuracies. Organizations should minimize PII collections and uses, with a timeline for disposal. Finally, privacy incident responses should provide accountability and redress for individuals involved.

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

Globalization has brought a unique set of supply chain risk management (SCRM) challenges and threats to industry, especially with our ever-increasing reliance on technology products and services to meet mission and business needs. Threats to the information and communication technology (ICT) systems range from counterfeit items, intentional threats such as malicious code or hardware Trojans, to poor software development practices that create software vulnerabilities or hardware quality issues. ICT

SCRM seeks to manage and mitigate cyber and supply chain risk throughout an acquisition lifecycle for an element or a system. It is a multi-disciplinary challenge, which requires contributions and collaboration among many disciplines and should be addressed as a core practice.

****

Thank you for the opportunity to provide Booz Allen's views on cybersecurity. We look forward to continuing the dialogue with NIST and our partners in government and industry.

Very truly yours,

John Michael McConnell

John Michael “Mike” McConnell

Vice Chairman

Booz Allen Hamilton