Developing a Framework to Improve Critical Infrastructure Cybersecurity

Response to National Institute of Standards and Technology
US Department of Commerce
Request for Information, Doc. Ref: 2013-04413
April 8, 2013

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

CIVITAS
GROUP

2020 K Street, NW, Suite 400
Washington, DC 20006
Phone: (202) 776 – 7354
Fax: (202) 776 – 7373
www.civitasgroup.com

Table of Contents

1.0 Introduction to Civitas Group

Civitas Group is an advisory services and strategy and management consulting firm serving private industry and government clients in the U.S. and across the globe. We provide a range of specialized strategic consulting services to senior corporate executive and government leaders and industry-leading due diligence support to sector investors. Our domain expertise in the national security, homeland security, and government services markets and policy domains allows us to advise our clients at the unique intersection between policy making and profit generation.

2.0 Civitas Group Corporate Data

This section provides the organizational information for Civitas Group

Administrative Data	
Company Name:	Civitas Strategy Group, LLC
Address:	2020 K Street, NW, Suite 400, Washington, DC 20006
Business Size:	Small Business
Point of Contact:	David White
POC Phone:	(917) 209 – 9284
POC Fax:	(202) 776 – 7373
POC Email:	dwhite@civitasgroup.com
Company Website:	www.civitasgroup.com

3.0 Capabilities & Experience Relevant to NIST's Needs

3.1 Background

Civitas Group occupies a unique position in the cybersecurity advisory services space. Our Cybersecurity practice combines our management consulting expertise, access to subject matter experts and former government officials, and strong cyber domain knowledge with our firm's agile market position. The diverse range of backgrounds, experiences, and expertise of our team members enables Civitas to integrate strong cyber domain expertise with corporate strategy and internal business processes analysis to view cybersecurity in a holistic, enterprise-wide manner. As a result, Civitas is able to identify security issues and organizational challenges that are overlooked if a singular, technology-driven, approach is taken to enterprise cybersecurity and overall risk management.

In addition to our team members, Civitas Group draws on an extensive network of advisors and partners. Civitas Group sits on the investment committee of Paladin Capital Group, a leading venture capital and private equity firm focused on security technology, cybersecurity, and the national security market. Our Advisory Board includes a former CIO at the CIA, a former Director of NSA, and a former senior DARPA official.

Civitas has reviewed approximately 200 technology assets in the last year as a member of Paladin Capital's Investment Committee. Additionally, Civitas has advised large organizations, including foreign-allied governments regarding cybersecurity and, as a member of SafeGov.org consortium of companies, developed Organization Cyber Risk Management framework for government (see Appendix)

Civitas Group's ability to combine our strategy and management consulting expertise with a deep understanding of the cyber threat environment and the existing risk enterprise management framework, while leveraging the market and technical expertise of our partners, is a key differentiator of the firm. We not only understand the current environment but have the ability to create cyber risk incentives to change the way organizations look at cybersecurity.

3.2 Subject Matter Experts:

3.2.1 David White

David White is an accomplished cybersecurity and business continuity strategy and management consultant with expertise in developing and using maturity models, benchmarking diagnostics, and training to support organizational improvement in cybersecurity and resilience. Mr. White was the Chief architect of Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and co-author of the CERT® Resiliency Management Model. He has experience in the federal, energy, and defense sectors.

3.2.2 Robert Liscouski

Robert Liscouski, former United States Department of Homeland Security Assistant Secretary for Infrastructure Protection, was appointed by President George W. Bush as the first Assistant Secretary responsible for cyber and infrastructure efforts. Mr. Liscouski is a recognized expert in risk management, Cybersecurity, and establishing the United States Department of Homeland Security's risk management framework.

3.2.3 Julie Anderson

Julie M. Anderson is the COO and a Managing Director at Civitas Group, a strategic advisory services firm in the national security markets. She also serves as an expert for SafeGov.org, an online forum focused on cloud computing policy issues. Recently, Ms. Anderson served as Acting Assistant Secretary for Policy and Planning and Deputy Assistant Secretary for Planning and Evaluation for the U.S. Department of Veterans Affairs (VA) in the Obama Administration. Prior to her appointment, Ms. Anderson worked for IBM's Public Sector Global Business Services practice in Washington, D.C.

3.2.4 Gavin Long

Gavin Long is a Managing Director at Civitas Group. Mr. Long has founded and helped capitalize numerous businesses in the identity management, homeland security and intelligence markets, working with notable private equity groups including the Carlyle Group, TPG, MidOcean Partners and Golden Gate Private Equity. Two of those companies have grown to more than $300 million in revenues. In addition, Gavin was a seminal employee hired by BAE Systems to establish its Intelligence & Security line of business, which now amasses more than $2 billion of revenue.

4.0 Supplementary Information: Civitas Group's Approach to Developing a Cybersecurity Framework

Civitas Group believes that cyber-attacks pose the single greatest long-term threat to any organization. As a result, our firm supports the development and implementation of a cybersecurity strategy as part of an overarching, organization-wide risk management strategy.

The Civitas Group approach to the development and implementation of a cybersecurity framework is to develop a product that provides clients with both an overall view of their organization's health as it relates to cybersecurity and the identification of specific assets and processes that are most vulnerable and/or would cause the greatest harm to the organization if they were compromised.

To achieve these comprehensive analytical outcomes we take an strategy-driven (as opposed to an audit-driven) approach that, in the initial stages, forces organizations to take a step back from daily operations and view their organization as a whole, not by department or business unit. The Civitas approach leverages and adapts the CERT Resilience Management Model (RMM) enabling organizations to identify their business priorities, key stakeholders, and most valuable assets from a macro-view. Through these prioritization discussions we collaboratively identify the processes and resources that are most critical to the firm from a viewpoint that encompasses both the direct impacts of a potential cyber-attack (financial and productivity loss) and the more intangible aspects (reputational damage and shareholder value).

Using our existing analytical framework as a base, we mold the content to reflect each industry and/or company, creating a unique, client-specific framework to can be used for both the initial assessment and as a building block to develop and manage ongoing monitoring and evaluation processes.

It is our view that a mature organization has a consistent, repeatable strategy and evaluates both itself and the framework on an ongoing basis. Our approach facilitates the development of these important processes for our clients.

5.0 Civitas Group's Comments

Based on recent and current efforts, Civitas Group is pleased to submit the following ideas, suggestions, and comments for NIST's consideration as it develops its Framework.

5.1 Current Risk Management Practices

1)	**NIST:**	***What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?***
	Comments:	Organizations are challenged to determine what their cybersecurity needs are, how much to spend, how to identify risk, and how to measure success. Organizations are often paralyzed because they do not know where to begin. They don't how much to invest in cybersecurity practices or how to justify those investments. Reconciling quarterly financial goals and reporting requirements with expenses for cybersecurity improvements is challenging. Such improvements contribute to the overall mission and to the greater good, but their value is difficult to determine – organizations need the ability to value the cost of preventing a cyber-attack. Organizations face challenges in consistently identifying risks, quantifying their potential impact and/or measuring the efficacy of their approach. The framework could help by clearly identifying the practices that all organizations should implement as a starting point

2)	**NIST:**	***What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?***
	Comments:	Based on our experience, organizations seeking to implement the framework want a sector-specific view and are indifferent to whether the Framework is applicable across sectors. When developing a cross-sector standards-based Framework organizations find it challenging to balance the desire to customize the product to their specific needs while maintaining enough consistency of information and output that cross-sector comparisons can be made. Organizations are also very concerned about the Framework becoming a regulatory requirement and therefore may be hesitant to participate in the development of a cross-sector standards-based framework. However, appropriating a cross-sector framework within various subsectors in order to secure an insurance product could be an effective way of encouraging industry engagement.

3)	**NIST:**	***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?***
	Comments:	Our policies and procedures governing risk include an outsourced approach to cybersecurity risk management. We have engaged third party experts to direct and oversee our security controls, which largely address identity and access controls.

		At hire, background checks are completed to provide a basis of trust for new employees. All employees affirm their agreement in writing to information protection policies and information system use guidelines.

4)	**NIST:**	***Where do organizations locate their cybersecurity risk management program/office?***
	Comments:	From our experience, the cybersecurity risk management program/office is often located in the IT group, but this varies widely by organization. Our cybersecurity risk management program office is outsourced. The contractor reports directly to the President.

5)	**NIST:**	***How do organizations define and assess risk generally and cybersecurity risk specifically?***
	Comments:	Risk is a common discussion topic and consideration of our management committee. Generally, risks are viewed in the context of their potential impact on Civitas Group's reputation. From a cybersecurity risk perspective, the management committee routinely reviews standardized analysis reports that cover networks and website access and activity from both within and outside the organizational boundary. In our experience, organizations tend to assess and evaluate cybersecurity risk qualitatively. We have seen some rare instances of quantitative evaluations and we believe that moving toward quantitative approaches will support financial justifications and risk transfer instruments for cybersecurity risk. The Civitas approach evaluates risk both quantitatively and qualitatively. We apply rigorous analysis to provide a weighted value to each asset based on its value, how easily it can be replaced, and mission criticality but also provide a qualitative analysis based on overall trends both inside the organization and in the external environment.

6)	**NIST:**	***To what extent is cybersecurity risk incorporated into organization's overarching enterprise risk management?***
	Comments:	Fully. Cybersecurity is a critical component of enterprise risk management. Lack of inclusion in overarching enterprise risk management fails to acknowledge cybersecurity's relationship to all aspects of organizational security and risk management.

7)	**NIST:**	***What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational and technical levels?***
	Comments:	From our experience, organizations reference multiple sources, some of which are: • CERT® Resilience Management Model (CERT-RMM) (http://www.cert.org/resilience/rmm.html) • Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) (http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model) • ISO 27001 (http://www.iso.org/iso/catalogue_detail?csnumber=42103)

		• NIST Special Publications, including specifically NIST SP800-53 (http://csrc.nist.gov/publications/PubsSPs.html) • SANS Institute 20 Critical Controls (http://www.sans.org/critical-security-controls/) • Payment Card Industry Data Security Standard (PCI DSS) (https://www.pcisecuritystandards.org/security_standards/) • FFIEC IT Examination Handbooks (http://ithandbook.ffiec.gov/it-booklets/information-security.aspx) • North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards (http://www.nerc.com/page.php?cid=2|20)

8)	**NIST:**	***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?***
	Comments:	Regulatory requirements are not consistent across organizations. Some critical infrastructure owners and operators are not subject to any type of regulation. For those that are, reporting requirements vary by regulator (by industry). In the appendix of this document we have included a report titled, "The Compliance Effect", which outlines major regulatory drivers for cybersecurity by industry. For publicly traded companies, SEC has issued guidance on reporting cybersecurity risks, but has not instituted a rule (http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm).

9)	**NIST:**	***What organizational critical assets are interdependent upon other critical physical and informational infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?***
	Comments:	Virtually all organizational critical assets are interdependent upon other critical infrastructures to varying degrees. From our experience, effective techniques for analyzing the extent of interdependency of operational assets are lacking. The CERT-RMM explicitly addresses four asset types that are critical to operations: people, information, technology, and facilities. A holistic approach to risk management and cybersecurity risk management should address all four of these asset types.

10)	**NIST:**	***What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?***
	Comments:	Asset availability is a key measure that underlies the ability to provide essential services. In the electric power industry, IEEE standard 1366 (http://standards.ieee.org/findstds/standard/1366-2012.html) provides defined measurements for Electric Power Distribution Reliability Indices. These standard measures are used to report frequency and duration of service outages: • **System Average Interruption Duration Index (SAIDI)** • **System Average Interruption Frequency Index (SAIFI)** • **Customer Average Interruption Duration Index (CAIDI)**

		• **Momentary Average Interruption Frequency Index (MAIFI)** • **Average Service Availability Index (ASAI)** • **Average Service Unavailability Index (ASUI)** Standard measures like these are valuable in reporting and comparing service availability amongst electric power utilities; similar measures may be useful in other sectors.

11)	**NIST:**	***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?***
	Comments:	We have no regulatory reporting requirements.

12)	**NIST:**	***What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?***
	Comments:	National and international standards can provide valuable guidance, such as: • Baseline/uniformity of reporting (to some degree) • Standard measures for reporting uptime (or outage) frequency/duration • Industry- and technology-agnostic evaluation approaches that can be used to consistently evaluate organizations within and across sectors.

5.2 Use of Frameworks, Standards, Guidelines, and Best Practices

1)	**NIST:**	***What additional approaches already exist?***
	Comments:	Some additional approaches include: • CERT® Resilience Management Model (CERT-RMM) (http://www.cert.org/resilience/rmm.html) • Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) (http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model) • ISO 27001 (http://www.iso.org/iso/catalogue_detail?csnumber=42103) • NIST Special Publications, including specifically NIST SP800-53 (http://csrc.nist.gov/publications/PubsSPs.html) • SANS Institute 20 Critical Controls (http://www.sans.org/critical-security-controls/) • Payment Card Industry Data Security Standard (PCI DSS) (https://www.pcisecuritystandards.org/security_standards/) • FFIEC IT Examination Handbooks (http://ithandbook.ffiec.gov/it-booklets/information-security.aspx) • North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards (http://www.nerc.com/page.php?cid=2|20)

2)	**NIST:**	***Which of these approaches apply across sectors?***
	Comments:	Specifically, the following are sector-agnostic: • CERT® Resilience Management Model (CERT-RMM) • ISO 27001 • NIST Special Publications, including specifically NIST SP800-53 • SANS Institute 20 Critical Controls However, all of the approaches listed in response to question 1 could be applied to any sector with some interpretation.

3)	**NIST:**	***Which organizations use these approaches?***
	Comments:	We are aware of firms in the following categories that are using one or more of these approaches: intelligence communities, defense, and federal civilian agencies, electric power utilities, natural gas utilities, financial services firms (including banks), and defense contractors.

4)	**NIST:**	***What, if any, are the limitations of using such approaches?***
	Comments:	Effective cybersecurity strategies and approaches should be dynamic to the threat environment. Guidance on incorporating and using threat models and threat profiles are missing from most of these approaches. ES-C2M2 provides some guidance on incorporating a threat profile into an organization's cybersecurity program.

5)	**NIST:**	***What, if any, modifications could make these approaches more useful?***
	Comments:	Inclusion of guidance on • developing and using a threat profile • evaluating and justifying cybersecurity investment • quantifying cybersecurity risk • evaluating and securing meaningful risk transfer mechanisms

6)	**NIST:**	***How do these approaches take into account sector-specific needs?***
	Comments:	Some of them do not. ES-C2M2 provides electricity-subsector-specific language and examples. CERT-RMM was a significant source of the content in ES-C2M2. Therefore, ES-C2M2 may serve as an example of how to express a complex model like CERT-RMM in a language and representation that is more accessible and useful to a specific sector.

7)	**NIST:**	***When using an existing framework, should there be a related sector-specific standards development process or volunteer program?***
	Comments:	This should be left to the discretion of the stakeholders within a specific sector. In some sectors, a sector-specific approach or process may be necessary to secure widespread buy-in and adoption by sector participants or in the event that sector-specific standards are in the interest of National Security. When this is the case, a sector-specific development process should be deployed.

8)	**NIST:**	***When can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?***
	Comments:	These entities should convene sector participants in voluntary initiatives to support cybersecurity capability improvements within the sector. A successful example of this is DOE's role in convening electricity subsector participants to participate in the development and piloting of ES-C2M2.

9)	**NIST:**	***What other outreach efforts would be helpful?***
	Comments:	Cross-sector outreach efforts may be helpful for selected groups of related sectors. For example, oil and natural gas entities typically participate in two overlapping subsectors: Pipelines with DHS-TSA serving as the SSA and energy with DOE serving as the SSA. In this case, cross-sector collaboration would be helpful in improving cybersecurity posture across the oil and natural gas subsector.

5.3 Specific Industry Practices

1)	**NIST:**	***Are these practices widely used throughout critical infrastructure and industry?***
	Comments:	Based on our experience, the use of these practices varies widely by organization and in some cases, varies within an organization.

2)	**NIST:**	***How do these practices relate to existing international standards and practices?***
	Comments:	We have not performed a detailed analysis of these practices in comparison to international standards.

3)	**NIST:**	***Which of these practices do commenters see as being the most critical for secure operation of critical infrastructure?***
	Comments:	All of these practices are important in every sector. Specific comments on selected practices are provided below.

		Separation of business from operational systems: Effective architectural separation or isolation is an increasingly important practice to protect sensitive or mission critical systems from threats that may propagate through internet-connected assets. In sectors for which critical functions depend on industrial control systems (i.e., operations technology (OT)), isolation of those systems from IT-centric business systems (e.g., customer service systems, email systems, and financial systems) is critical to protect the OT from potential threats. Isolation and separation is also warranted to protect sensitive organizational information and intellectual property. **Identification and authorization of users accessing systems:** This is a critical practice for all organizations. In our experience, organizations often struggle with deactivating authorizations and access in a timely and complete manner upon employee departure or job change. **Asset identification and management:** This is an important practice for all organizations. Assets should be prioritized relative to their importance in achieving the organization's mission or delivering the organization's critical infrastructure functions so that protective and sustainment strategies can be appropriately tailored. Such prioritization also enables the organization to focus resources on protecting the assets that are of greatest importance.

4)	**NIST:**	***Are some of these practices not applicable for business or mission needs within particular sectors?***
	Comments:	While privacy and civil liberties protection applies to essentially all organizations in some form, it does not typically apply to OT or industrial control systems environments. Therefore, in organizations that operate OT environments, the application of privacy and civil liberties protections would typically be limited to business and financial systems that contain employee, customer, or business partner personally identifiable information.

5)	**NIST:**	***Which of these practices pose the most significant implementation challenge?***
	Comments:	• Separation of business from operational systems • Identification and authorization of users accessing systems • Asset identification and management

6)	**NIST:**	***How are standards or guidelines utilized by organizations in the implementation of these practices?***
	Comments:	Typically, to inform the specifics of practice implementation and as a basis for evaluating practice implementation, which may include benchmarking both within the organization and across organizations.

7)	**NIST:**	***Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?***
	Comments:	In our experience, organizations are challenged to justify cybersecurity investments and to understand whether they are spending too little, just enough, or too much. Quantitative approaches to evaluate cybersecurity risk and to enable risk transfer mechanisms are needed. Such approaches would help organizations to better understand, plan, and justify their cybersecurity investment.

8)	**NIST:**	***Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?***
	Comments:	This is a good practice. In our experience, some organizations do have effective escalation processes in place. We recommend that organizations design predetermined states of operation that can be invoked in conjunction with such an escalation process (as described in ES-C2M2).

9)	**NIST:**	***What risks to privacy and civil liberties do commenters perceive in the application of these practices?***
	Comments:	**Identification and authorization of users accessing systems:** We advocate background checks (at hire and periodically) on employees and contractors prior to granting access to organizational assets. Such checks pose some privacy and civil liberties risk because of the information that must be collected to affirm an individual's identity and the information that must be accessed to conduct the background check. A permissions process is recommended to ensure that the employee or contractor is aware and agrees to such checks. Information security controls should be put in place to protect the information gathered in support of such checks. **Monitoring and incident detection tools and capabilities:** Monitoring practices may appropriately include network traffic capture and review, which may pose privacy risk to individuals using the organization's systems. Disclosure of such monitoring is advocated.

10)	**NIST:**	***What are the international implications of this Framework on your global business or in policymaking in other countries?***
	Comments:	Our business operations are constrained to the United States at this time. If successful, the Framework will likely inspire similar efforts in other countries.

11)	**NIST:**	***How should any risks to privacy and civil liberties be managed?***
	Comments:	Through • clearly-worded disclosures of practices that pose privacy and civil liberties risks, • carefully designed controls to protect relevant information assets, • timely disclosure of breaches or other violations of privacy or civil liberties, and • effective risk transfer mechanisms that cover the cost or remediations and reparations.

12)	**NIST:**	***In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?***
	Comments:	**Threat management** – including the development and routine update of organization-specific threat profiles that guide the cybersecurity program. **Situational awareness** – monitoring the organization's operational and cybersecurity state in the context of the risk environment and interdependent critical infrastructures. **Physical security** – a critical element of access control for the organization's assets. **Communications and information sharing** – collection and conveyance of appropriate and timely information from/to the organization's stakeholders. **Supply chain, procurement, contracts, and dependency management** – the supply chain is a source of cybersecurity threats and vulnerabilities. Organizations should perform implement practices to protect assets that are procured. **Secure software development** – software that is developed or procured by the organization should be managed to reduce the incidence and risk of vulnerability-inducing software defects.

APPENDIX A – Related Works

1. Anderson, Julie M., Karen S. Evans, Franklin S. Reeder, and Meghan M. Wareham; ***Measuring What Matters: Reducing Risk by Rethinking How We Evaluate Cybersecurity;*** *SafeGov,* March 2013. http://www.civitasgroup.com/mar-26-2013-measuring-what-matters-reducing-risk-by-rethinking-how-we-evaluate-cybersecurity/?p=1190.

2. Long, Gavin and Beaghan, Jay; ***The Compliance Effect: Changing the Face of Security Technology;*** **USBX Advisory Services, October 2007.**