April 8, 2013

National Institute of Standards and Technology (NIST)
Diane Honeycutt
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Subject: Request For Information (RFI) # 130208119–3119–01
Developing a Framework To Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt,

PricewaterhouseCoopers LLP (PwC) is pleased to submit to the National Institute of Standards and Technology (NIST) our RFI response to assist NIST with developing a framework to improve critical infrastructure cybersecurity. Our response represents the insights that PwC possesses from having delivered cybersecurity services to many of the largest firms in the world across a breadth of critical industry segments along with many government agencies.

PwC is part of one of the world's largest professional services networks with more than 2,500 professionals based in the Washington Metro Area. PwC is a leader in providing advisory and assurance services to the Federal Government. PSP helps government agencies solve complex business issues, manage risk, and add value to performance through its detailed service offerings in financial management, risk and compliance, security and data management, operations improvement, and program management. PwC delivers comprehensive approaches to cybersecurity that helps government agencies adapt to changing environments; manage IT risks; select, design, build, and integrate comprehensive solutions; and respond to cybersecurity crises.

PwC has skilled professionals with cybersecurity, risk management, and program management experience to meet the U.S. Government's needs. We look forward to continued interaction with NIST to successfully support your Cybersecurity Framework development, implementation, and management needs. If you have any questions about our response, please contact me at (703) 918-3767.

Sincerely,

John Hunt
Principal

PricewaterhouseCoopers LLP, 1800 Tysons Boulevard, McLean, VA 22102
www.pwc.com/publicsector

Table of Contents

Section **Page**

List of Figures

Figure **Page**

1.0 Our Understanding

In the current context of asymmetric warfare and global economic instability, defending against cyber attacks on U.S. critical infrastructure has become a national priority. Fortunately, adversaries have not yet been able to significantly disrupt our critical infrastructure operations. However this is not due to lack of effort. Most cyber incidents to date have focused on denial of service or data exfiltration, resulting in the loss of sensitive data. However, the same access to our information systems that allows information gathering to occur also provides the access an adversary needs to disrupt those same critical infrastructure information systems.

The National Institute of Standards and Technology (NIST) has been assigned the difficult task of aligning policy, business, and technological approaches to standards. NIST, as directed in Executive Order (EO) 13636, will establish the methodologies and processes that provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. PricewaterhouseCoopers (PwC), as a cybersecurity, business operations, and risk management advisor to numerous commercial and public sector clients across the globe, possesses unique insights and has relationships that can assist NIST in establishing a practical framework to achieve the objectives of EO 13636.

2.0 PwC Insights and Capabilities

2.1 Who is PwC?

PwC is a network of firms in 158 countries with over 180,500 people. We are one of the world's largest professional services networks supporting a wide range of commercial and government clients with solutions to some of the most challenging technology and security problems. In fiscal year (FY) 2012 PwC firms provided services for 422 of the companies in the Fortune Global 500 and 439 of the companies in *The Financial Times* Global 500[1]. Our clients represent a broad spectrum of industries that include financial services, energy and utilities, aerospace and defense, information technology, and healthcare. PwC is a key element in the financial services critical infrastructure segment as we provide assurance to capital market investors and stakeholders for many of the world's largest companies. We also provide advisory service offerings in technology, financial management, risk, and compliance, security and data management, operations improvement, and program management to over a dozen major federal civilian, and defense agencies. Cybersecurity is an especially important topic to PwC's ability to protect our clients' sensitive information and data in highly regulated industries requires sound technology and processes, and diligent execution by our entire workforce.

With more than 2,300 PwC Technology Consulting professionals in the U.S., approximately 30% of which are dedicated security services professionals, PwC continues to address the cyber challenges that our nation's critical infrastructure owners and operators face. We take pride in our role as a trusted advisor to senior executives and information security professionals in organizations around the world. Our reach has allowed us to gain considerable insight into the challenging issues leaders face in their organizations. We have honed our cybersecurity approach to focus on strategy and governance, IT risk, security technologies, and cyber crime and breach response. By focusing on these four areas, we can provide a comprehensive approach to cybersecurity solutions that helps our clients plan and communicate to adapt to changing environments, manage IT risks, select, design, build, and integrate comprehensive solutions, and respond to the cybersecurity crises faced by our clients every day.

2.2 PwC's Viewpoint on Cybersecurity

Cyber attacks are increasingly frequent, aggressive, well-funded, and sophisticated. Our data highlights the growing challenges these threats could pose to commercial organizations. Our 2013 Global State of

[1] http://www.pwc.com/gx/en/about-pwc/facts-and-figures.jhtml

Information Security (GSIS) Survey[2] revealed that diminished budgets have resulted in degraded security programs, cyber risks that are not well understood or properly addressed, and new technologies that are being adopted faster than they can be safeguarded. Given that a successful attack on critical infrastructure sector organizations can result in grave damage to our national security and economic interests, it is important to take steps that will help ensure that the trends indicated in the GSIS survey do not carry over to the critical infrastructure sector.

Faced with these challenges, PwC feels that the framework that NIST is tasked with developing to improve critical infrastructure cybersecurity should incorporate the following concepts:

Organizations are only as secure as their weakest link. The global business ecosystem has changed the risk landscape. (see **Figure 1**).

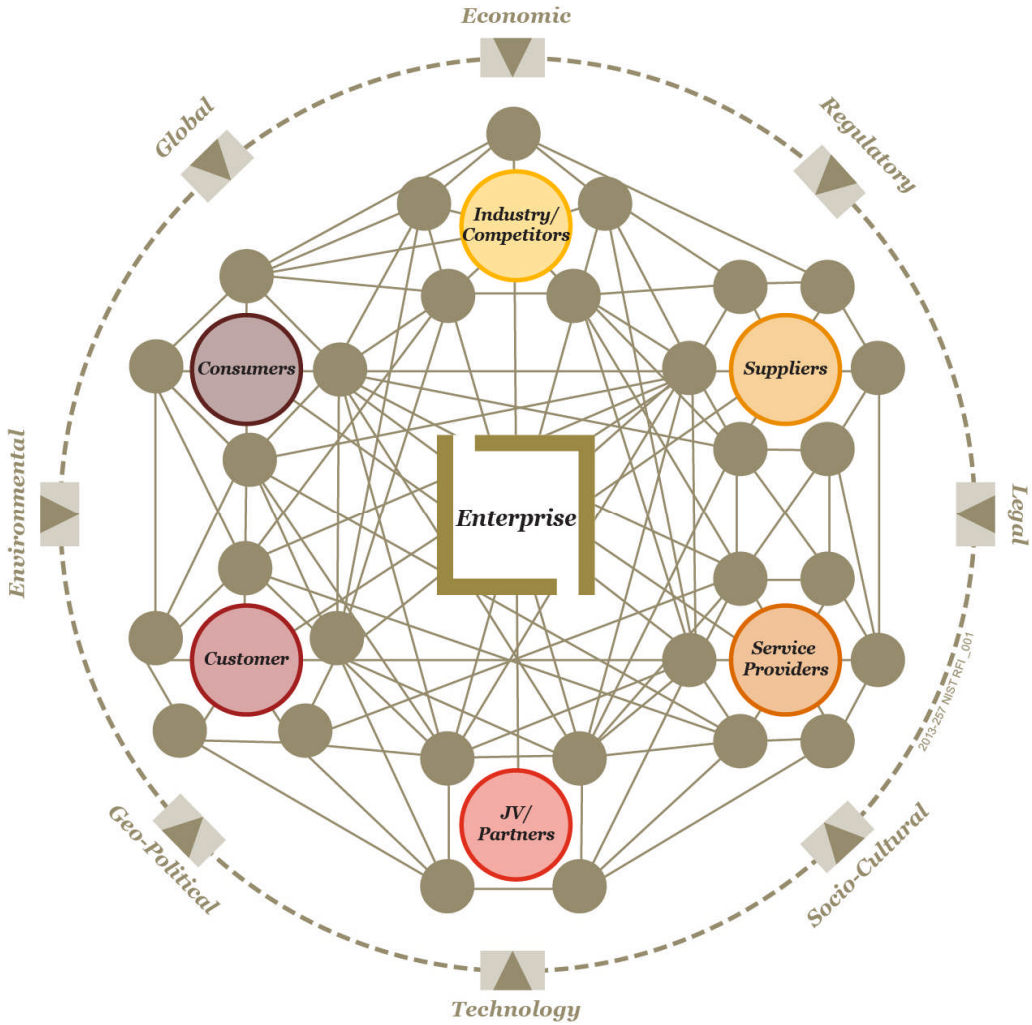

Figure 1. The Global Business Ecosystem

Critical infrastructure sector organizations depend on information technology and the information systems (e.g., financial transaction systems, healthcare record systems, industrial/process control systems, testing and calibration devices, etc.) to successfully carry out their business functions. Business

[2] http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml

models have evolved into an interconnected, integrated, and interdependent ecosystem that flows across sectors and industries. However, the security strategy currently in place has not kept pace. Critical infrastructure organizations today need a more dynamic approach to effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing business functions. NIST's cybersecurity framework should help organizations address the following questions:

- How do you monitor and manage vulnerabilities within your ecosystem?
- How have changes in your business model and/or strategic initiatives increased vulnerabilities?
- How has adoption of new technologies affected your level of vulnerability?

Focus on securing high value assets and protecting what matters. Not all assets are created equal; it is no longer efficient or effective for companies to protect everything in the same manner. Rather than securing everything equally, companies must now identify and protect their most critical assets. By determining what their most valuable assets are, where they are located, and who has access to them, executives and security officers will be able to effectively apply limited security and countermeasure resources where they are needed most throughout the system development lifecycle. NIST's cybersecurity framework should help organizations address the following questions:

- Have you identified your most critical (both physical and information) assets?
- Where do your most critical assets reside (in both physical and cyber domains)?
- Do you understand the impact/value of your critical assets, if they would become impaired?

Know your adversaries – motives, means, and methods. Recent cyber attacks and warnings from government, military, and intelligence leaders clearly indicate that critical infrastructure organizations are considered a target. Rather than waiting for an attack that one day may occur, businesses need to actively seek to understand their adversaries' motives and likely methods of attack. While intelligence organizations and their military counterparts are often limited in their ability to coordinate cyber defense for a number of significant reasons, sophisticated adversaries without such restraints are using cyber technology as an asymmetric tool to actively exploit weaknesses in the business ecosystem for economic and political gain. NIST's cybersecurity framework should help organizations address the following questions:

- Who are your adversaries? Where are they?
- Are you protected against threats? What do you do about them?
- How are methods/techniques being used? What do they do?

Embed cybersecurity into board and executive-level decision making. Cybersecurity is not a technology problem; its complexity and importance mean that it is an executive-level business challenge. PwC's 16th Annual CEO Survey[3] indicated that seven out of 10 Chief Executive Officers (CEOs) fail to view cybersecurity as a fundamental strategic issue. The disconnect between the reality of cyber threats and how CEOs currently view these risks means many critical infrastructure business models are vulnerable. Active engagement at the highest levels will signal a committed strategy to get in front of cyber threats and be prepared to respond quickly when attacks are successful. Executives should have a global security strategy approach, looking at their own internal policies as well as external factors. They should reinforce with their employees that everyone has a role in cybersecurity and ensure employees have the resources and training to do their part. In addition, Executives should equally assess the security practices of their suppliers and service providers to limit risks from those vectors as well. NIST's cybersecurity framework should help organizations address the following questions:

- Can I explain our corporate cybersecurity strategy to others?
- Are security investments aligned with critical business processes and mission priorities?
- Are human, cyber, and physical risks addressed adequately across all organizational lines?

---

[3] http://www.pwc.com/us/en/ceo-survey-us/index.jhtml?WT.mc_id=ba_Home+page_CEO+Survey+2013+home

- Do investments demonstrate that the overall security posture has improved? How is this measured?

This last concept of executive commitment perhaps exposes the greatest limitations of effective participation – namely incentive and liability, which is inherent in a voluntary framework such as the one the NIST is tasked with creating through EO 13636. Generally, boards and executives of companies are evaluated on financial outcomes rather than broader national security factors. NIST's framework should ultimately be accompanied by legislation that provides companies with financial incentives (e.g., tax breaks for cybersecurity investments or limitation of liability for sharing breach information) to participate. Financial incentives will lead to a greater chance for C-level attention and more wide-spread adoption. Throughout the development of the framework, NIST may wish to consider economic factors (e.g., industry cost models, competitiveness in foreign markets, etc.), in addition to the technical challenges associated with cybersecurity.

3.0 NIST Requirements Response

PwC is proud to advise clients across a wide range of industries and organizations deemed critical infrastructure. Many of our commercial clients are engaged in financial services, energy and utilities, aerospace and defense, information technology, communications, and healthcare industries. Furthermore, we value the opportunity we have to support federal, state, and local agencies and governments. Our relationships with all of these organizations have demonstrated that they are very concerned about the impact cyber threats could have on their ability to operate and provide services for to the critical infrastructures of the United States.

To give voice to our clients' concerns, we have collected and synthesized the professional experiences and insights of our PwC practitioners within these critical infrastructure segments in relation to the questions NIST provided. Our access to these security professionals, who are well-versed in cyber operations within their respective organizations and industries, provides us a unique perspective from which to answer the following Request for Information (RFI) questions:

3.1 Current Risk Management Practices

NIST has requested information about how organizations assess risk, how cybersecurity factors into that risk assessment, the current usage of existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a framework that identifies and includes common practices across sectors.

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

Industry leaders at the forefront of critical infrastructure security face a wide range of challenges in improving their cybersecurity practices. PwC anticipates that six key challenges will need to be considered:

1. **Mobility.** The push towards mobile technology, especially employers allowing their enterprise to "bring your own device" (BYOD), will be a challenge for any organization, due to the new threat landscape in which security is no longer just an internal concern. These technologies create a "boundless" network that is difficult to manage and secure, raising a number of privacy and security concerns. Connecting personal mobile devices to a corporate network creates additional challenges, given the growing capabilities of these devices. The key is to create policies that welcome and encourage the usage of mobile devices. Simultaneously, the organization must manage the inherent risks involved with permitting access to the corporate network, while not compromising critical infrastructure.
2. **Threat Intelligence.** Another key concern is the lack of useful threat intelligence, as well as a disconnect in the ability to apply current threat intelligence to new or existing technology. Industry security professionals routinely question whether all owners and operators understand who the adversary is, relying on the assumption that Security Content Automation Protocol (SCAP) -

compliant and Federal Desktop Core Configuration (FDCC) -capable tools for harnessing the National Vulnerability Database (NVD) is enough to fend off attacks. In fact, cybersecurity practitioners must be able to assess threats across a broad spectrum. This can only be achieved through increased data sharing and collaboration across industries.

3. **Executive Commitment.** Securing management buy-in and ensuring leadership is involved demonstrates the importance of cybersecurity and conveys a serious message to employees. This starts with educating senior management on the importance of enterprise security so they view it as a priority. This can be achieved by highlighting the potential impacts to business operations – specifically critical infrastructure. Shareholder buy-in is also a critical component and may be influenced by government incentives.
4. **Defining Risk.** Many PwC clients struggle to identify risk in measurable ways. Even when risk is adequately defined, differing risk tolerances across organizations make specific security standards difficult to prescribe. Cyber risk should be correlated to the performance metrics that are the most important for each business unit responsible for critical infrastructure operations. A well-developed continuous monitoring program can provide critical risk measurement and analysis and is especially beneficial if integrated within an enterprise risk management framework. This type of program should incorporate the capabilities of real-time data reporting and analysis, the ability to "drill down" at the individual host-level, historical/trending data to assess the effectiveness of the program, and scoring metrics/algorithms to provide a real-time risk score snapshot. Initial (and iterative) data analysis will help to establish acceptable risk thresholds. Real-time risk monitoring provides key stakeholders with actionable data to respond to risk proactively as well as a clear picture of the organization's cybersecurity readiness.
5. **Information Sharing.** Security collaboration and information sharing is generally limited due to the fear of sharing too much information with competitors, which negatively impacts competitive advantage. Many of our clients acknowledge the need for increased sharing of best practices, which in turn would lead to improved overall security within the industry. However, most are hesitant to volunteer that information.
6. **Supply Chain Security.** Because businesses operate in global ecosystems, cyber threats can impact a business' operations at any point in the operations process. Supply chains are particularly vulnerable because most businesses rely on them but, in reality, have no direct control over security processes, standards, or enforcement related to them. And because many businesses rely on supply chains that are owned and operated by foreign companies, many with questionable ties to aggressive foreign governments, U.S. critical infrastructure -related businesses are showing that they are amenable to discussions with the U.S. government regarding government-issued security practices.

3.1.2 What do organizations see as the greatest challenges in developing a cross-sector, standards-based framework for critical infrastructure?

Key challenges to developing a cross-sector, standards-based framework includes:

Differing Risk Models. Differing risk models and tolerances across sectors hinder the ability to apply a single framework with very specific detail. The complex nature of the current regulatory landscape is a challenge that impacts critical infrastructure sectors in different ways. The lack of a central point of leadership or "standard bearer" in the Federal Government (i.e., Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) vs. Federal Information Security Management Act (FISMA)) for industries has allowed various alternatives to be established. Industries or organizations that work with more sensitive data and missions are likely to be extremely resistant to changes imposed upon their framework.

Differing Business Operating Models. Organizations, even within the same industry, may have very different operating models, which will also hinder the development of a single cross-sector model. Varying levels of global operations, suppliers and customers, and web-enabled applications will likely dictate cybersecurity priorities, vulnerabilities, and threats. For instance, in the healthcare and hospitality industries, which rely on a relatively higher contingent worker environment, they likely require a different approach to awareness and training than industries that hire mostly full-time employees.

Differing Cost Structures. Due to their ability to absorb costs or pass them along to their customer base, certain organizations and industries will be able to handle the increased costs associated with aligning to a new standards-based framework. On the other hand, a deployment of a single cross-sector framework could impose economic hardships on certain organizations or industries, limiting participation or overall effectiveness as other operating risks take the place of cyber risks.

Overlapping Regulatory Requirements. One of the concerns within the utilities industry, and quite possibly the healthcare and financial services industries, is the threat of having multiple, overlapping regulatory requirements. The utilities industry is particularly concerned with having to comply with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements in addition to the framework standards being considered.

NIST may seek to limit these concerns via a maturity model to help organizations gauge their current capabilities against a spectrum of increasing effectiveness within the confines of the framework. Ultimately, some organizations with lower maturity may be unable or unwilling to meet what the framework suggests based on the current state of their security program. Organizations that have a specific plan of action in place to meet the various framework elements over time (with a step-by-step maturity plan) will be better-positioned than organizations that simply reject the framework from the onset.

3.1.3 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?

Cybersecurity risk should not be evaluated separately from business operations; rather, policies should be all encompassing and consider all facets of the organization when defining and evaluating risk. Many organizations find themselves still in the planning stages of cyber risk management, or even enterprise risk management as a whole, having created strategies that quickly become outdated. Policies and procedures must be dynamic "living documents" and be constantly reviewed and revamped to account for the ever changing ecosystem. Apart from developing policies and procedures, organizations should consider actively testing the operating effectiveness of controls to validate whether security and risk mitigation mechanisms are operating as expected.

In addition, organizations should shift away from the "check the box" mentality regarding cybersecurity risk and risk assessments. Assessments often uncover a long list of findings that are either never addressed or sit stagnant for a long period of time. Merely identifying risks it not sufficient. To overcome these challenges, organizations often develop a risk assessment methodology to identify, evaluate and prioritize, monitor, and remediate risks. In this case, leadership and key stakeholder buy-in and understanding is critical to understanding that a strong risk management program can provide them with a competitive advantage and increase industry confidence in their cybersecurity and overall risk practices.

Specifically with regards to cybersecurity risk, we have observed the need to move from a control model that seeks to prevent cyber incidents to one that incorporates prevention along with a stronger emphasis on detecting and correcting vulnerabilities and incidents. In the global business ecosystem, this requires a balance between an internal and external focus, as well as the risk responsibility assigned to the business rather than to the IT organization.

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

Our view is that no matter where the cybersecurity risk management program or office is located, the organization should understand the overall risks to the organization and how cybersecurity risks relate to the overall risk posture. The cybersecurity risk management office should be positioned to be able to affect the business and technical aspects of operations.

The cybersecurity risk management program/office has been viewed as an Information Security responsibility. To highlight the importance of cyber risk management, we recommend that cybersecurity risk be assigned responsibility at the CEO, Chief Risk Officer (CRO), or Chief Operating Officer (COO). It should be business- aligned and owned, not just operated by an IT department, as is often the case. A

centralized cybersecurity risk management office with senior-level management involvement is critical to obtaining stakeholder buy-in and to help ensure the allocation of necessary resources to keep the program/office running properly. However, depending on the size of an organization, a specific risk management office can exist with liaisons into IT, Operations, Management, Human Resources, and Financial Services. An organization may also consider assigning cybersecurity oversight responsibility to a board member to ensure that adequate governance and resources are applied to cybersecurity in alignment with corporate strategy and compliance. Internal audit organizations should also assume responsibility for assessing cybersecurity practices as part of its risk assessment portfolio.

3.1.5 How do organizations define and assess risk generally and cybersecurity risk specifically?

Risk is generally categorized, assigned, and assessed based on the impact to the business, while cybersecurity risk is viewed as reputational or regulatory. Risk assessments, such as a Business Impact Analysis (BIA), are typically performed on a periodic basis as necessary; however, cybersecurity risk assessments are starting to gain more exposure as a result of internal and external pressure.

PwC recommends assessing cyber risk using a traditional risk equation (threats X vulnerabilities X impact)/controls and countermeasures) with an evaluation approach that scores each variable with a current view of the cyber landscape.

- Threats are dramatically evolving, are more numerous, and more targeted.
- Vulnerabilities are exacerbated through the ecosystem across people, process, and technology dimensions.
- The depth and breadth of impacts internally have increased due to targeted attacks on critical assets, and impacts are now felt across the enterprise and ecosystem.
- More tailored control and countermeasure designs based on prioritization of assets, intelligence-based approaches to assessing threats, and increased implementation of detective and corrective mechanisms are required.

Many organizations are conducting regular Attack and Penetration (A&P) tests as part of their periodic risk assessments in order to more actively view the enterprise from an adversary's point of view.

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

Many large organizations have incorporated IT risk within their Enterprise Risk Management (ERM). However, smaller organizations are less mature and focus more on traditional information security operational responsibilities. Every organization, no matter the size, can benefit from incorporating cybersecurity risk into their overarching ERM. Before doing so, though, an organization must establish their baseline for risk tolerance. This baseline will vary based on the sensitivity of the data and mission and will require different approaches if risk tolerance is generally low versus organizations that decide to accept a higher level of risk in their operating activities. This baseline will also help determine the organization's priority systems and data in order to direct efforts and funds to those areas first. We generally recommend incorporating cybersecurity risk management into an organization's overall ERM approach. We see this approach as a potential for an organization to take on a more proactive stance towards risk management – including actively developing countermeasures and procedures to anticipate and mitigate risk – with the mindset that it is not a matter of *how*, but *when* their systems will be compromised.

PwC's GSIS survey results from 2013 note that "diminished budgets have resulted in degraded security programs, risks are not well understood or properly addressed, and new technologies are being adopted faster than they can be safeguarded" within the public sector. Integrating cybersecurity risk management into overarching enterprise risk management practices can achieve efficiencies and greater senior leader visibility, thereby providing additional resources to address issues. Additionally, PwC healthcare industry practitioners note that many organizations incorporate cybersecurity through an internal information security risk management group responsible for managing and directing an organization-wide information protection program, mainly due to industry regulatory requirements.

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

There are many risk management standards that serve as general guidelines to help organizations in addressing their risks. Below is a list of the more popular risk management frameworks that we have observed our clients using:

- ISO 3100: Risk Management – Practices and Guidelines
- OCEG "Red Book" 2.1: GRC Capability Model
- BS 3110: Code of Practice for Risk Management
- COSO: Enterprise Risk Management – Integrated Framework
- FERMA 2002: A Risk Management Standard
- SOLVENCY II: Risk Management for the Insurance Industry
- ISACA frameworks of COBIT 5, Risk IT, and Val IT
- NIST Risk Management Framework

Often, general standards for managing risks from a management, operational, and technical aspect start with an understanding the organization's critical mission area and the supporting elements. Not knowing what is most critical to the mission leads to a poor definition of fault tolerances, resulting in misappropriation of scarce resources to address the most high-impact risks to the organization.

PwC has also observed that companies often create hybrid risk management frameworks that are based on general guidelines established by standards organizations like ISO or NIST, coupled with industry-specific best practices from various guidelines and regulations. Generally, the management of an organization's risk will take into account the operational needs of that organization rather than assuming that a single framework provides one specific answer on how to manage risk in that organization. PwC has conducted many engagements where we apply our proprietary frameworks and methodologies to a client's specific business model. PwC's Risk Management and Mitigation Planning (RMMP) services have attained Department of Homeland Security (DHS) Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act designation and certification, which supports the use of such hybrid risk management approaches in securing critical infrastructure.

3.1.8 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?

From PwC's viewpoint, the FISMA and the Comprehensive National Cybersecurity Initiative (CNCI) directed by the January 2008 National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) both drive the regulatory and regulatory reporting requirements for the public sector. Other regulatory requirements within the private sector address elements of cybersecurity such as privacy (e.g., Health Insurance Portability and Accountability Act (HIPAA)). Other notable regulations with or without reporting requirements include:

- Electronic Communications Privacy Act (ECPA)
- Stored Communications Act (SCA)
- Computer Fraud and Abuse Act (CFAA)
- Defense Industrial Base
- State Breach Notification Laws (state specific)
- Payment Card Industry Data Security Standard (PCIDSS)
- Gramm-Leach Bliley Act (GLBA)
- 2002 Homeland Security Act
- United States Computer Emergency Readiness Team (US-CERT)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards
- Nuclear Regulatory Commission (NRC)

Additionally, individual states, particularly California, have existing or emerging security and privacy requirements related to electric grids and customer information.

Generally, these regulations address specific elements of cybersecurity but do not provide the basis for a full cybersecurity framework.

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

Dependencies between critical physical and information infrastructures, such as telecommunications, energy, financial services, water, and transportation, to an organization's operational status, is largely dependent on their mission. In general, most organizations have information systems or network enterprises that have a dependency on telecommunications and energy. "Back Office" operations for any organization are dependent on these two critical infrastructures. Facilities that house the operational environments for an organization's workforce are dependent on water and energy. The critical dependencies of these infrastructures are associated with the risk to people and property. For example, a lack of running water means that living domiciles get backed up with sewage, causing health concerns to the people housed there. Ultimately, PwC practitioners across multiple industries have an anecdotal knowledge base on the interdependencies to critical infrastructure; however, there is not a cross-industry macro view of interrelated infrastructure.

Assets in critical infrastructure sectors are increasingly becoming interdependent with one another. Disruptions in one sector are likely to adversely affect the operations of others. Interdependent effects occur when an infrastructure disruption spreads beyond itself to cause an appreciable impact on other infrastructures, which in turn causes more disruptive effects on the other infrastructures. When an infrastructure system suffers an outage, it is often possible to estimate the impact of that outage on service delivery. These are the consequent effects of an "outage". Due to business operations' strong dependency on information flow and connectivity, it is not a surprise that electricity, utilities, and telecommunications are critical services. As a result, we expect adversaries to target critical infrastructure assets through secondary and tertiary interdependencies that may be less understood and/or protected.

For example, during our work with healthcare practitioners, PwC recognizes that there is a strong organizational dependency on all infrastructures due to their direct impact on human life. Hospitals are a general community aggregated into one location that houses and/or affects both stakeholders and users. Hospitals depend on electricity to run life-saving equipment, water to provide critical fluids, telecommunications to run the interconnected personal medical records systems that support diagnoses and proper patient care, and financial systems to ensure connectivity with the insurance companies and financial organizations that run the "business" of a hospital.

In addition, during our work with the financial industry, PwC has noted the strong dependence upon telecommunications and electricity due to the interconnectivity of today's commerce, from connections at stock market locations to e-commerce on the world-wide web. For example, if the New York Stock Exchange had telecommunication issues, no trades could be executed outside of the market itself, which could bring down the entire financial industry and cause significant financial impact around the world.

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

During our work with a variety of business types and government agencies, PwC has observed that most organizations' performance objectives do not integrate business performance with cybersecurity performance. While organizations' performance goals, which measure the "health" of the organization and its mission, have evolved to include metrics that have dependencies on information systems, there are rarely executive-level measures of the security performance of those information systems. To address this, organizations may wish to develop cybersecurity performance measures based on the following:

- Security process effectiveness goals
- Business continuity and disaster recovery
- Security communication, training, and human capital activities

- Regulatory compliance goals

Cybersecurity must be embedded into critical infrastructure board- and executive-level decision making. Active engagement at the highest levels will signal a committed strategy to get in front of cyber threats and be prepared to respond quickly when attacks are successful. A successful cybersecurity framework will incentivize businesses and operators of critical infrastructure to view security as a differentiator in its business. If shareholders, boards, and CEOs do not view cybersecurity as a priority, then it will be difficult for the cybersecurity framework to gain wide-spread acceptance.

3.1.11 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?

Generally, every organization has multiple regulatory compliance requirements it must meet within its industry to continue operating effectively. We have seen that organizations in critical infrastructure segments like telecommunications, financial markets, and utilities are governed by a broad swath of regulations from international, national, state, and local industry authorities. For example, PwC, as an audit and accounting firm, is subject to multiple regulatory bodies just in the U.S., such as the Securities Exchange Commission (SEC), the American Institute of Certified Public Accountants (AICPA), and the Public Company Accounting Oversight Board (PCAOB). Organizations that span multiple industries or perform more complex or risky activities will likely be regulated by multiple regulating bodies. Ultimately, PwC has found that leading organizations strive to find ways to establish regulatory compliance as a market differentiation. For example, consumers may place a premium on conducting business with a financial institution that demonstrates above-standard performance and regulatory compliance related to cybersecurity. Regardless, it is beneficial for organizations to meet a certain minimum standard for protecting critical infrastructure information systems in order to establish some form of defensible liability stance should a cyber attack occur. However, most standards compliance is voluntary. Thus, an organization's adoption of that standard must be linked to a specific business need in order to act as an incentive for compliance.

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

Just as in the current environment of cybersecurity awareness and collaboration across international and national public and private sectors, industry leaders must determine a set of general guidelines to provide a uniform security posture across all critical infrastructures. Due to the global footprint of today's interconnected information systems, a consistent approach to protect all information systems is necessary to assure security of U.S. critical infrastructure systems. Standards committees, such as the International Organization for Standardization (ISO), the Security Industry Association (SIA), the Institute of Electrical and Electronics Engineers (IEEE), and NIST, must participate at Group of Eight (G8), North Atlantic Treaty Organization (NATO) and other international summits to reach agreement on cybersecurity standards.

These bodies should focus on understanding and addressing macro-level cybersecurity issues and developing the common definitions and taxonomies from which more specific industry-focused solutions can be developed. This will allow tailoring to specific organizational and industry considerations while maintaining alignment to broader national and international objectives. PwC recommends conformity assessment to be performed by qualified, independent third parties similar to financial statement assurance or current NIST compliance assessments within federal agencies. These third parties are more likely to be able to assemble the necessary resources and develop innovative methods to assess performance against various standards.

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

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions. NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations. NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage.

3.2.1 What additional approaches already exist?

While there are many approaches to standards, frameworks, and guidelines, the following is a sampling of the approaches our clients use to establish cybersecurity best practices:

- National Institute of Standards and Technology (NIST)
  - SP 800-53
  - SP 800-12
  - SP 800-14
  - SP 800-26
  - SP 800-37
- Information Technology Infrastructure Library (ITIL)
- International Society of Automation
  - ISA-99
- Information Systems Audit and Control Association (ISACA)
  - Control Objectives for Information and Related Technology (COBIT)
- Information Security Forum (ISF)
- Business Model for Information Security (BMIS)
- Established Security Maturity Models
- International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC):
  - 17799:2000 Series– Code of practice for information security management
  - 17799:2005, Information technology – Security techniques – Code of practice for information security management
  - 27001: Information security management systems
  - TR 13335-3 (Guidelines for the Management of IT Security: Techniques for the Management of IT Security
- Public-Private Partnerships
  - Department of Homeland Security (DHS) – National Cybersecurity & Communications Integration Center
  - U.S. Computer Emergency Readiness Team (US-CERT) Domestic Security Alliance Council (DSAC)
  - Common Vulnerabilities and Exposures Program (MITRE)
  - National Coordinating Center for Telecommunications
  - Defense Industrial Base (DIB)

Many organizations are adopting DHS's Federal Emergency Management Agency's provided incident response structure to better collaborate with each other, and government agencies in the event of a cyber incident. Some of our clients use approaches to standards and frameworks that are specific to their particular industry:

- Financial Services

  - Sarbanes-Oxley (SOX)
  - Gramm-Leach-Bliley Act (GLBA)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Federal Financial Institutions Examination Council (FFIEC)
- Healthcare
  - Health Information Trust Alliance (HITRUST)
  - Health Information Technology for Economics and Clinical Health Act (HITECH)
  - HIPAA
- Energy
  - North American Electric Reliability Corporation (NERC)
  - Nuclear Energy Institute (NEI)/Nuclear Regulatory Commission (NRC)

3.2.2 Which of these approaches apply across sectors?

Just as in the approaches that already exist, several of the approaches apply across sectors. Our clients have specified a few that apply:

- National Institute of Standards and Technology (NIST)
  - SP 800-53
  - SP 800-12
  - SP 800-14
  - SP 800-26
  - SP 800-37
- Information Technology Infrastructure Library (ITIL)
- International Society of Automation
  - ISA-99
- International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC):
  - 17799:2000: Series–Code of practice for information security management
  - 17799:2005: Information technology – Security techniques – Code of practice for information security management
  - 27001: Information security management systems
  - TR 13335-3: Guidelines for the Management of IT Security: Techniques for the Management of IT Security

Some approaches that are specific to the financial industry address risks in a way that could result in best practices for industries outside the financial industry. Two specifically named are GLBA and FFIEC.

3.2.3 Which organizations use these approaches?

While we are unable to indicate specific organizational usage of these approaches, our discussions with our critical infrastructure clients leads us to conclude that all sectors use one or more of these approaches as operational roadmaps for their CIOs, Certified Information Security Officers (CISOs), Security Officers, and Risk Officers in the defense and development of a resilient critical infrastructure.

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

The most significant limitation of using such approaches is that no approach will ever eliminate every form of cyber risk, nor should any approach be expected to ensure total security. Because the cybersecurity environment is in a constant state of evolution, proactive standards and approaches are continuously being developed to combat emerging threats and risks, which are also in a constant state of change. However, because the standards have not been thoroughly tested or implemented, their effectiveness in preventing cybercrime is uncertain, especially given new technological advances and developments.

A number of organizations struggle to implement broad, industry-agnostic standards in their particular operating environments. Two such standards are COBIT, which focuses on governance standards; and IOS 27000, which focuses on information security controls. Poorly aligned standards to actual operating

environments leave gaps and inconsistencies in specific sector's security approaches. In the energy industry, operations take place in an automation and control systems environment, yet many required standards are IT-centric. Even where industry-specific approaches exist, limitations on their effectiveness may exist. For instance, some frameworks used in the financial sector are difficult to obtain without costly membership fees.

Successful, resilient organizations recognize the absence of a mature integration model. These organizations adopt a "continuous growth" model that will enable them to be as smart and adaptive as their adversaries, constantly developing approaches and proactive measures to protect their IT environment. These companies see the Executive Order as an opportunity to strengthen cybersecurity, which will ultimately increase profits from a cybersecurity approach that drives value and enhances returns on their security investments.

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

A common taxonomy of cybersecurity capability terminology and definitions can provide a foundation from which to build standard sets tailored to specific industry segments and operating models (e.g., global operations, outsourced IT services, etc.). Standards should reflect the range of risk tolerances and recognize that one size does not fit all. There is a need for unambiguous, industry-specific approaches that include examples they can use to derive custom organizational policies, procedures, and tools. In fact, the very framework NIST is developing could provide a mapping of the standards to steer sectors toward the most applicable solution. Implementation guides should be created that discuss real-world applications and examples. Also, a comprehensive matrix or work program could help make the approaches more useful. Security professionals in the energy sector suggested creating standards that govern controls and procedures specific to the industrial automation and control systems environment within their industry.

Given the broad range of cyber threats and their increasingly adverse impact to business-critical functions, determining exactly where to integrate specific approaches within information systems is imperative to determine the appropriate level of organization risk, response, and capital investment.

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

To account for sector-specific needs, the best approach is one that starts with top-level standards that are more general and less sector-specific. With top-level standards in place, more detailed, sector-specific standards can be created that address definitive concerns. This approach is similar to the National Security Agency's Community Gold Standard that is comprehensive, yet provides the ability to define specific configurations at the individual Component level. If designed with owner and operator input, this top-level approach will provide greater insight into how leaders perceive the information that is of value to their organization, the risks that are prevalent, and the mitigation plan to reduce security exposures. Additionally, this approach promotes an industry-agnostic framework that provides a base of common terminology, definitions, and tools from which sector-specific entities can build more detailed standards.

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

In general, a voluntary program is not effective for sectors with immature security programs, practices, or approaches. Organizations in these sectors are unable to recognize the specific guidance or direction that is required to implement cybersecurity standards, especially when so many approaches currently exist. For more mature security programs, a voluntary program could be adequate but would have to include a strong incentive program for organizations to participate. Successful incentive programs could serve as a model for less mature programs to emulate, and draw in more organizations to participate voluntarily.

PwC has found that when aligning sector-specific development processes to critical infrastructure organizations, several factors are instrumental for successful implementation. These include the size of the organization, the impact the security program can have on public relations, and the number and diversity of sector members. Organizations should have a hand in identifying which recommendations are most applicable to them, ensuring approaches that define solutions to a specific environment. We observed in the financial industry in particular that a sector-specific approach would probably allow for the consideration of the nuances of each sector's legal and regulatory requirements. This could yield a more targeted approach to controls and governance.

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

Sector-specific agencies and related-sector coordinating councils can benefit from sector-specific conferences, webcasts, or training around cybersecurity. The ability to document and share sector-specific cybersecurity measures with other sectors benefits everyone and could lead to cross-sector policies, procedures, and centralized actions. Benefits should be promoted as redacted case studies to demonstrate the advantages of successful adoptions. These organizations would also be able to help coordinate collaboration and information sharing, reducing some of the fear of directly providing competitors with valuable information. Using an agency outside of the industry to collect and distribute the information would help introduce more anonymity to the process.

Activities that develop and promote the use of cross-sector approaches to improve security standards could create more ubiquity in standards, helping professionals who move between sectors. These activities would serve as a foundation for prerequisite skills or experiences that are transferable regardless of the industry or sector with which the security professional is aligned. This cross-sector approach would reflect the distinct operational characteristics of each sector founded on the commonalities of industrial automation and universal control systems.

3.2.9 What other outreach efforts would be helpful?

Security conferences and trade shows could be useful outreach efforts but, we caution that if poorly managed, they could turn into marketing events that reduce the collegiality and collaborative environments they are meant to espouse. These events should be balanced with both large and small organizations in order to capture the full spectrum of experiences that can be brought together and shared. It would be important to include international organizations as well, especially since businesses increasingly operate in a global ecosystem. The availability of internationally-focused events will allow businesses to get in front of the broader cybersecurity program issues they already face. For the defense sector in particular, it may make sense to participate in NATO-level discussions. The G8 Summit is another example of an international-based event that would attract organizations from the financial sector.

3.3 Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry. NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

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

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

PwC has found that the security practices outlined in this section are used throughout critical infrastructure and industry, but vary in level of intensity from one type of information system to the next within organizations and throughout the critical infrastructure sector. For example, the separation of business systems from operational systems is common in industries which rely on industrial or process control systems, e.g., energy, utilities, and manufacturing. While privacy protection is a key focus for consumer information-based industries such as healthcare and financial services.

Performance Monitoring. Many organizations are struggling to develop a set of performance measures that adequately portray their cyber risk posture at any given time. Real-time monitoring of security controls can be a cost-effective method of managing compliance and helping to reduce security costs, making it more appealing to more organizations. Continuous monitoring methods are evolving and are expected to be a core element to an organization's cybersecurity program. Markets for "security intelligence" tools that provide risk status based on aggregated network operations and security tool event logs are growing as managers and executives seek the timely status of their cybersecurity. In addition, independent security audits can help organizations measure and validate compliance with specific security guidelines and provide assurance to stakeholders.

Automated Identification and Analysis of Users. Organizations are beginning to enhance the identification and authorization of users accessing systems via automated tools for baselining and tracking user access, privileges, and activity with an organization's network to help deter and prevent insider threats. The threat to U.S. critical infrastructure from a trusted insider has one of the largest potentials for impact and viability if a person with the right access and knowledge decided to act maliciously or even inadvertently by not following standard guidelines or security practices. This growing market for heuristic software should be monitored and used when appropriate to help alleviate some of the risk to an organization from an insider threat.

4.0 Conclusion

To counter today's cyber threats, cybersecurity must operate the way businesses operate: agile with interconnected processes that are able to recognize and respond to multiple threats with limited resources. These are the realities owners and operators face as they run their businesses and manage cyber risks. The Cybersecurity Framework should recognize that while businesses operate in industry or sector settings, each has distinctly different strengths, weaknesses, and capabilities. Critical infrastructure standards are encouraged, yet should have some flexibility built-in to allow for, and take advantage of, the different capabilities each owner and operator brings. This includes what specific components should be considered more critical than others. The Framework should identify and measure risk using consistent methodologies that do not favor one business model over another, and support dynamic and real-time risk analysis. The most effective cybersecurity practices consider adversary intentions and enable processes to share threat information.

Cybersecurity is much more than a technical issue. The successful development, implementation, and management of this Framework will require ideas in areas that include technical management, risk, performance measurement, organizational alignment, and program management solutions. Despite the hundreds of ideas that speak to many of these points, there will likely still be critical knowledge gaps. PwC has a vast amount of federal and industry experience to assist in applying a holistic approach to cybersecurity. Our relationships with senior executives throughout the security industry have matured our understanding of their concerns and viewpoints. We are available as a trusted advisor to assist with executive-level information gathering and pragmatic counsel.

Our breadth and depth of experience not only reaches across industries, but also most of the critical functions that will contribute to a successful Framework development. Supporting a critical component of the Framework, PwC has helped clients identify future risks, measure the impacts of those risks, and develop plans to mitigate these risks. Owners and operators are encouraging consistent performance measures, an area in which we bring significant proficiency having helped many organizations define and determine success. Considering the enormous task at hand to bring the Cybersecurity Framework to life, we have helped clients manage large-scale programs through our ability to define the scale and scope of work. Our security practice is well-known internationally for its expertise across all of these management functions. PwC looks forward to working with NIST, other government agencies, standards and regulatory bodies, academia, and our industry-client base to establish a cybersecurity framework in protection of our country's critical infrastructure.

www.pwc.com/publicsector