# Developing a Framework to Improve Critical Infrastructure Cybersecurity

Response to NIST's Request for Information

# Developing a Framework to Improve Critical Infrastructure Cybersecurity

**April 8, 2013**

**Presented by**

**Deloitte & Touche LLP**
1750 Tysons Blvd
McLean, VA 22102

**Technical POC:**
Carey Miller, Director
Tel: 571-882-6975
Email: caremiller@deloitte.com

**Contracts POC:**
Greg Anderson, Contracts Manager
Tel.: 703-509-2514
Email: gregranderson@deloitte.com

**Submitted To:**
Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-1640
*cyberframework@nist.gov*

**Error! Use the Home tab to apply Cover 2_Entity Name to the text that you want to appear here.** & Touche LLP
1750 Tysons Boulevard, Suite 800
McLean, VA 22102

Tel: +1 703 885 6000
www.deloitte.com

April 8 2013

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-1640

**Re: Request for Information on Developing a Framework to Improve Critical Infrastructure Cybersecurity.**

Dear Ms. Honeycutt:

Deloitte & Touche LLP is pleased to submit a response to the above Request for Information.

We have drawn upon the breadth of capabilities in our organization to provide suggestions to help mitigate challenges that NIST is likely to face as they develop the Cybersecurity Framework. In assembling our suggestions, we have leveraged our core competencies in cybersecurity disciplines, such as risk management, identity management, and privacy to address the technical challenges. In addition, we have drawn upon our experience in the public sector (particularly Department of Homeland Security) and private sector (with clients encompassing all sixteen of the critical infrastructure sectors) to address the business and operational challenges. We have drawn on this subject matter experience, matched with our infrastructure experience, and our capabilities in standards development and public private partnerships to provide this response to NIST.

We hope the ideas presented herein will assist NIST as they implement their mandate under the President's Executive Order. We would be pleased to offer support to NIST as they develop the Framework, based on our experience and client relationships across the critical infrastructure.

We are excited about the Cybersecurity initiative and are available to further discuss the ideas presented in this response at NIST's convenience. If you have any questions, please do not hesitate to contact me at 571-882-6975.

Sincerely,

Carey Miller, Director

Deloitte & Touche LLP

# Table of Contents

# 1 Introduction

Deloitte[1] is pleased to respond to NIST's Request for Information (RFI) regarding development of the Cybersecurity Framework (Framework) in support of the Executive Order (EO) and Presidential Policy Directive-21 (PPD-21).

NIST's initial mandate under the EO is the rapid development of a first draft of the Cybersecurity Framework. Further, NIST has comprehensive experience in assimilating material received in response to such RFI's, a process that it routinely uses to solicit points of view on work products such as the NIST Special Publications. At the same time, due to the diverse stakeholder base, the development of a Cybersecurity Framework for critical infrastructure poses some unique challenges, including: ensuring that key critical infrastructure operators are engaged; defining risk metrics in a way that allows them to be aggregated from diverse sources; deriving meaningful and pragmatic conformity processes; and ensuring that privacy rights are maintained by providing strong identity management and data protection, consistent with Fair Information Practice Principles and the Privacy Act of 1974.

Deloitte has drawn upon a breadth of capabilities in our organization to provide suggestions to help mitigate the challenges that NIST faces as they develop the Cybersecurity Framework. In assembling our recommendations, we have leveraged our core competencies in cybersecurity disciplines, such as risk management, identity management, critical infrastructure protection, resiliency, and privacy to address the technical challenges. In addition, we have drawn upon our experience in the public sector (particularly the Department of Homeland Security and sector-specific Agencies) and private sector (with clients encompassing all sixteen of the critical infrastructure sectors) to address the business and operational challenges. We have drawn on this subject matter experience, matched with our infrastructure experience, and our capabilities in standards development and public private partnerships to provide this response to NIST.

We hope the ideas presented herein will assist NIST as they implement their mandate under the President's EO. We would be pleased to offer support to NIST as they develop the Framework, based on our experience and client relationships across the critical infrastructure. We are available to further discuss the ideas presented in this response at NIST's convenience.

## 1.1 Developing a Framework to Improve Critical Infrastructure Cybersecurity

Cybersecurity was recently identified as the number one threat to national security by James Clapper, U.S. Director of National Intelligence[2]. Cybersecurity serves a critical dual role: both facilitating commerce and supporting our national security structure. Daily cyber-attacks are being made on the very infrastructure that operates the goods and services underpinning our nation's economy and defense apparatus. Attacks in the cyber domain resulted in approximately $300 billion in losses of trade secrets last year alone.[3] Pipelines, financial institutions, and government agencies have been victim to cyber-attacks that are reportedly executed by nation-states.[4]

---

[1] As used in this document, 'Deloitte' means Deloitte & Touche LLP, which provides accounting, internal control and financial management support services, and Deloitte Consulting LLP, which provides strategy, technology, and human capital consulting services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

[2] http://ivn.us/2013/03/15/cyber-security-not-terrorism-number-one-threat-to-national-security

[3] http://csis.org/files/attachments/131902_Cybersecurity_TS.pdf

[4] http://www.cfr.org/cybersecurity/secretary-leon-panettas-speech-cybersecurity/p29262

Furthermore, a recent Government Accountability Office study said that "reports of cyber incidents affecting both public and private institutions are widespread," and that the Office of Management and Budget reported that the U.S. Computer Emergency Readiness Team (US-CERT) received over 106,000 total incident reports in Fiscal Year 2011.[5]

Executive Order 13636 (EO) signed by President Obama on February 12, 2013, "Improving Critical Infrastructure Cybersecurity," creates an opportunity to break out of the cybersecurity "regulation/no-regulation" debate of recent history. The core principles of the EO - collaboration, coordination, and cooperation, as well as information-sharing, and the establishment of a voluntary program within the Cybersecurity Framework - create an environment that will enable tangible progress in cybersecurity without legislation.

To develop a response to this RFI of most value to NIST, we have considered some of the challenges that we anticipate NIST will face in its role of developing the Cybersecurity Framework based on Deloitte's experience with similar government-wide initiatives, our knowledge of the subject area, and our direct relationships with critical infrastructure owners and operators. To offer ideas on how to mitigate these challenges, we have addressed specific questions in the RFI that encompass critical factors that are imperative to the success of the Cybersecurity Framework. In responding to these questions, we draw upon our experience to highlight some common trends and challenges that we see across the critical infrastructure sectors. As NIST develops the Cybersecurity Framework, we also believe that lessons learned by Deloitte practitioners from similar initiatives, such as the Department of Homeland Security's Voluntary Private Sector Preparedness (PS-Prep) Program, will be highly valuable and instructive.

The development and adoption of the Cybersecurity Framework will involve many aspects of stakeholder consensus and public-private partnership. The types of processes used in consensus bodies, such as the World Economic Forum and the Identity Ecosystem Steering Group (IDESG) can be drawn upon for reference. We will provide some ideas to NIST based on our experience in these domains.

By focusing on several key questions relating to critical success factors, we believe that this response will assist NIST in successfully developing and sustaining the Cybersecurity Framework.

[5] http://www.gao.gov/assets/600/592008.pdf

# 2 Responses to selected questions

## 2.1 Question: What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

### 2.1.1 Response: Creating the Right Public-Private Partnership

We believe that one of the greatest challenges to improving cybersecurity practices through adoption of the Cybersecurity Framework will be the creation of successful public-private partnerships. In similar initiatives regarding smart grids and trusted identities, the Smart Grid Interoperability Panel and the Identity Ecosystem Steering Group were formed, respectively. As these groups were formed, Deloitte & Touche LLP found that the following five factors are most critical:

1) Create an environment where a broad range of stakeholders have a clear voice.

2) Resolve governance and management issues early so that work can commence as quickly as possible.

3) Ensure that a very transparent process for standards and frameworks adoption is defined.

4) Bring the right people to the table at the right times—subject matter experience and technical facilitation are essential to the process of establishing a viable framework.

5) Clearly define conformity requirements and assessment processes.

Throughout the drafting of the *National Strategy for Trusted Identities in Cyberspace* (NSTIC), Deloitte & Touche LLP, guided by the principles outlined above, helped to enable outreach, education, and interaction with a diverse set of more than two-hundred public, private, and international stakeholders. As a result of these efforts, the Department of Homeland Security created an inclusive and broad reaching strategy that has gained significant support across all sectors. As NSTIC moved into implementation via the Department of Commerce's National Program Office, we have continued to provide strategic, technical, and organizational support. The IDESG, a private-sector led organization responsible for administering the creation of the Identity Ecosystem Framework and its requisite policies and technical standards, was established in 2012. Led by a representative body that includes key government personnel, the IDESG was rapidly organized and has grown to include several-hundred member organizations from both the public and commercial sector in less than one year. We believe that a process that allows for such broad stakeholder participation is also crucial to the successful development and sustainment of the Cybersecurity Framework. Additionally, current NSTIC efforts will complement the Cybersecurity Framework, by providing a forum and organizational structure for the establishment of standards and solutions that promote the use of trusted identities throughout cyberspace.

On a global basis, Deloitte brought together a multi-national, cross-functional team to act as Project Advisor to the Risk Response Network (RRN) initiative within the World Economic Forum (Forum). The Forum is an independent international organization committed to improving the state of the world by engaging business, political, academic and other leaders of society to shape global, regional and industry agendas. The Forum launched the RRN to bring together stakeholders on complex, interconnected global risks. The network serves as a preparatory, analytical and highly practical framework for the global community to improve risk management through bringing together the relevant global decision-makers with compelling insights and suitable tools and services. Drawing upon the most experienced and knowledgeable opinions across a range of

industries and sectors of society, the project started by laying the foundations for a common framework to understand global systemic risks, and to identify the main stakeholders and their role in this eco-system. The first year of the initiative culminated in the presentation of Principles for Cyber Resilience (PCR) at the Forum's signature annual event in Davos, Switzerland. At a private session, leaders from industry and government discussed issues and many committed to the PCR on the spot. The project working group also released a final paper reporting the results of the first year of the initiative and laying out next steps to carry forward the agenda of making cyberspace more resilient.

As the Cybersecurity Framework is developed, and draft cybersecurity legislation is adopted in international regions, Deloitte believes that close international coordination is required, to ensure that the Framework can be capably implemented by global operators.

### 2.1.2 Response: Ensuring Appropriate Stakeholder Representation

Stakeholder engagement is critical in early phases of the development process for the Cybersecurity Framework. Deloitte's experience in brokering support for initiatives similar to the Cybersecurity Framework is that success of such initiatives is highly dependent on garnering the appropriate support and participation across sectors and industries, especially at the C-Suite level. We routinely see that executive level support is a pre-requisite for the success of our cybersecurity risk management engagements. Additionally, when initiating or transforming an organization's risk management strategies and processes, it is key to conduct outreach, identify business needs and requirements, and secure buy-in from organizational stakeholders. The same holds true for NIST's Cybersecurity Framework endeavor. The approach to cybersecurity risk management varies based on industry, existing guidance and standards, the particular Critical Infrastructure sector, and the Administration's perspective. Some organizations may follow the standards issued by Standards Development Organizations, such as ISO, while others may use industry leading practices to "conform" to NIST's approach.

Facilitating a cross-sector dialogue will be challenging and has the propensity to overwhelm both the process leaders and participants. As the facilitator of Framework development, the government must set the tone of these conversations by identifying examples, demonstrating cross-sector domain knowledge, and being open to feedback. This will allow the various risk metrics used across the Critical Infrastructure operators to be characterized so that they can be commonly used, as well as create meaningful and pragmatic conformance practices.

Another challenge to the development of cross-sector standards-based Cybersecurity Framework is the frequently practiced wide distribution of risk management responsibilities based on functional alignment. For example, the responsibility of cybersecurity is generally delegated to the Chief Information or Chief Technology Officer, but other aspects of security are the responsibility of the Chief Security Officer. In a survey conducted by Carnegie Mellon University in 2012, the results show that the majority of Boards are still not undertaking key oversight activities related to cyber risks such as investment and budget, however there is an increase in companies that have established teams or risk committees focused on cyber risks. This is why it is important to engage Critical Infrastructure owners at the executive level, to ensure that execution of cohesive risk management strategies are harmonized across organizations. A common element across all private sector entities is the recognition that a key driver for the need for cybersecurity measures is the protection of sensitive corporate data, continuity of production and services, and the protection of reputation, confidence, and thus value for a company. Leveraging this common perspective as a point of departure for outreach would provide a focus that all Critical Infrastructure owners and operators could probably agree to regardless of which sector they belong.

Deloitte is committed to advancing capabilities around cybersecurity through outreach. We have sponsored a bi-annual study with the National Association of State CIOs to foster greater insight into the maturity of state cybersecurity programs. We also sponsor a quarterly Federal CISO roundtable to facilitate discussion around leading practices for cybersecurity. Deloitte supports private sector clients across all sixteen Critical Infrastructure sectors and we communicate with them on an ongoing basis to further the development of Critical Infrastructure protection. For example, our Silicon Valley-based research and development center (Deloitte Center for the Edge) helps senior executives optimize organizational performance from emerging opportunities on the edge of business and technology. We author and publish *Tech Trends*, an annual report examining technology and business use. Our themes for 2013 are analytics, mobile, social, cloud and cybersecurity and includes inputs from hundreds of stakeholders from Federal, commercial, and academia. We are eager to leverage similar activities and outreach efforts to help NIST conduct cross sector coordination and communication, identifying common themes and the mutual ground upon which the Framework must be built.

## 2.2 Question: What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

### 2.2.1 Response: Leveraging Lessons Learned from Similar Programs

It is clear that some of the biggest challenges to successfully developing a Cybersecurity Framework and Program relate to garnering tangible participation, both in the development of the Framework and in its promotion and adoption. Similar efforts have been attempted in the past and their lessons should be applied to the development of the Framework and Program under the EO. One such effort is the Voluntary Private Sector Preparedness (PS-Prep) Program[6] which was established by Congress in the Recommendations of the 9/11 Commission Act of 2007. The lessons learned from PS-Prep are directly applicable here.

Through the PS-Prep Program, DHS is required to work with standards-based organizations to designate a preparedness standard—or set of standards—that private sector companies can voluntarily certify themselves against to demonstrate their preparedness posture. Congress encouraged DHS to adopt standards currently used by industry which were focused on critical infrastructure. As such, the PS-Prep Program is analogous to the program envisioned under the President's EO because it is calling for voluntary participation and standards that are used by critical infrastructure. Standards were adopted a few years ago and the private sector may now voluntarily participate - just as it is intended under the EO. Due to these similarities, the structure, policies, and resulting effectiveness of the PS-Prep Program should be considered in the context of the development of the Framework and Program.

[6] http://www.fema.gov/ps-preptm-voluntary-private-sector-preparedness

Deloitte observed two key factors in the PS-Prep Program that will be critical to consider as the Cybersecurity Framework is developed:

1. A clear, consistent, public promotion of the Framework and Program among U.S. Government principals including, but not limited to, senior-level political appointees.

2. Early and robust engagement with private sector critical infrastructure owners and operators to develop the Framework and acclimate them with the resulting Program so that they are more willing to voluntarily participate.

Notwithstanding the PS-Prep Program's adoption of standards, the number of firms that have attempted to be certified has been small, with the first being certified only in March 2012. While many factors have contributed, the two listed above (discussed further below) have been the strongest inhibitors to success.

First, the promotion of the PS-Prep Program occurred primarily at the program level; senior-level officials have not encouraged industry participation to the extent necessary. Because the private sector is being asked to do something which it does not have to do (or pay for) under PS-Prep, only senior-level officials, particularly political officials, can convince industry of the importance of their participation in the program. This executive buy-in and promotion demonstrates commitment to industry and without it, industry will not consider adoption and participation necessary. Designers of the Framework and Program should not forget this lesson and take every opportunity to ensure senior-level officials are soliciting targeted industry participation when they are meeting with such groups. If this effort appears to be a low priority for the Administration, the importance of the Framework and Program is automatically lessened.

Second, and concurrent with the first factor, a climate must be created where industry feels it can help shape the program while maintaining the overall cybersecurity objectives stated in the EO. If industry has this opportunity early and often, the likelihood of tangible private sector participation increases. Further, industry involvement must be both strategic and constant, and transparency must be a guiding principle. Simply put, the Cybersecurity Framework must not be treated as a traditional regulatory program, putting critical infrastructure owners and Framework developers on opposite sides of the table. If industry does not have consistent and frequent access to updates and opportunities to provide input into a non-regulatory program, then the chances of participation in the Framework development process dwindles, as does the probability of subsequent Framework adoption.

By building upon lessons learned from the PS-Prep Program, the designers of the Framework and Program under the Cybersecurity E.O. would face a greater likelihood of success and increased participation. Because NIST's Framework and the associated Program will include standards with which firms can voluntarily comply, it is imperative that these factors are addressed early and often by officials.

The following section further addresses these factors.

### 2.2.2 Response: Engaging Key Stakeholders in Critical Infrastructure Dialogues

A key element of the EO is the development of the Cybersecurity Framework that establishes voluntary, consensus-based standards for cybersecurity in the nation's critical infrastructure. Private sector critical infrastructure owners and operators may, however, be skeptical of participating due to a perceived sense of increased regulation and risk. To be effective, the public and private sectors must collaborate to develop a framework that enhances both cybersecurity and galvanizes private

sector participation. It is therefore crucial that an environment be created that encourages substantial participation by private sector operators. We respectfully suggest NIST's extensive background in galvanizing the Information and Communications Technology industry be augmented by the incorporation of three phases specifically designed to create future workshops that are highly inclusive of critical infrastructure operators. These recommendations were developed after extensive dialog with such operators over the last several months, and reinforce the importance of collaboration, communication and cooperation throughout development of the Framework.

Facilitated workshops could be implemented in three phases:

- ***Phase I: Education and Stakeholder Outreach***
  NIST has commenced these activities via its April 3rd workshop. A point of note at the workshop was that critical infrastructure operators need to be fully represented, in addition to Information and Communications Technology providers.

- ***Phase II: Convene roundtable discussions with private and Federal stakeholders to discuss development of the Framework***
  In addition to the NIST workshop process, we believe that there is significant value in capturing lessons learned from programs such as PS-Prep in smaller, more targeted, roundtable discussions including representatives from such programs and critical infrastructure operators. This phase should start immediately and continue through at least the initial draft periods of the Framework.

- ***Phase III: Socialize the progress and solicit continued input on the Framework***
  We believe that key consideration of Framework development and subsequent adoption is ongoing openness and transparency. We suggest that frequent, targeted, communications to critical infrastructure operators is required to enhance the nature of inclusiveness and to encourage tangible participation.

In addition to the types of public-private partnerships discussed later, such as SGIP and IDESG, Deloitte believes that the success of the Cybersecurity Framework is dependent on such very targeted and active phases of workshops. Early in the development of the NSTIC, the public-private partnership that characterizes the IDESG was catalyzed through the use of collaborative meetings and similar discussions. Key characteristics of stakeholder engagement during the development of NSTIC included:

- The use of large and small forums. Often times, the best information was gathered through targeted conversations with small groups. While time-consuming, these conversations (all conducted in full compliance with the Federal Advisory Committee Act (FACA)) yielded great results including key industry concerns and challenges; lessons learned on other analogous programs; and perspectives that drove adoption of the Strategy once published.
- Full Transparency: specifically, the widespread sharing of draft content through both formal and informal channels.
- The use of a wide range of collaboration technology.
- Repeated recognition and acknowledgement that this was an ongoing process that would require long-term industry participation. This particular approach galvanized the IDESG once it was developed.

These events not only garnered the information necessary to develop the NSTIC, but solidified the initiative as a direct output of collaboration between the Federal Government, private sector entities, nonprofit organizations, and others. In addition to our experience on NSTIC, Deloitte has, for some time, been developing such workshops for operators of critical infrastructure.

## 2.3 Question: Which of the Cybersecurity core practices do commenters see as being the most critical for the secure operation of critical infrastructure?

### 2.3.1 Response: Mission/system Resiliency Practices

We live and work in a world that is increasingly interconnected and interdependent as well, which means we are more vulnerable to systemic and catastrophic impact if our critical infrastructure is attacked or compromised. If we are to protect ourselves against these vulnerabilities, then strong resiliency practices are a necessity The vulnerabilities of an aging infrastructure and the threats of extreme events, ranging from natural disaster to acts of terrorism and cyber-attacks, can create long-lasting and complex disruptions to the government's mission critical functions, as well as introduce significant disruptions to our everyday life. Malicious cyber activity can affect any component of our nation's infrastructure, many of which we are unaware of as being "critical infrastructure," take for granted and rely upon every day including: telecommunications, emergency services, food warehousing and distribution, mass transit, financial systems, power, water, and sewage systems.

Organizations may not be able to control natural disasters or cyber terrorist attacks, but they can mitigate the impact of occurrences by identifying and understanding their vulnerabilities and associated risks, and proactively developing integrated resilience strategies. Resilience strategies should not focus on a single element of an organization's infrastructure, but must take a systems-wide approach to integrate the core elements that make up that infrastructure including physical assets, personnel, operations, and technology. One of the related challenges in the private sector is the increasing virtual nature of the workforce and the reliance on various modes of communication to "stay connected". This ability and freedom to work from anywhere also introduces complexity into an organization's network security efforts. The conduits for network access have increased to include wireless, email, mobile devices, and portals for vendor and executive access, thus exponentially increasing the potential for unauthorized logical ***and*** physical access which ultimately puts all of an organization's assets and data at risk.

It is Deloitte's belief that the following principles are paramount in ensuring that system resiliency is maintained:

- Provisions to promote continuous development of innovative approaches to proactive information sharing related to cyber threats and resiliency.

- Inclusion of standards, processes and procedures in the Cybersecurity Framework that incorporates all phases of the resilience lifecycle: strategy, risk management, governance, policy, business intelligence and data analytics, geospatial technology, human capital, and crisis communications.

- Development of cross-sector guidance within the Cybersecurity Framework focused on sharing of lessons learned about cyber threats , while still allowing for conformity to industry-specific regulation and prescribed guidelines. The intention would be for entities to continue operating within industry-specific guidelines and standards while encouraging voluntary information sharing to support early warning and detection across critical

infrastructure, which could greatly impact the ability to employ emergency resilience protocols and maintain operational status.

- Enhancing the usage of interoperable resources and a government-wide decision making process for prioritizing the allocation of those information technology resources, This could build off the progress already being made to increase the availability of approaches such as Federal cloud offering and shared services, but also involves reevaluating the individual agency and private sector response processes to identify where cross-agency/private sector decisions would be more effective. Increased inter-organization (public and private) exercises should then support the validation of these approaches and provide opportunities for these disparate organizations to make improvements.

- These efforts should have a primary focus on the data given that today's advanced cyber threats pose a direct threat to data integrity. These threats have demonstrated a tendency to employ tactics that are "low and slow" meaning professionals may not discover their existence for months if not years. After the discovery or realization of these threats, it may be challenging for incident response teams to restore or uncorrupt the vital records that support the Nation's Essential Functions. A structured approach and capability for recovering from a known good point of historical data helps address these challenges.

### 2.3.2 Response: Privacy Protection Practices

As stated at the April 3, 2013 NIST workshop, the maintenance of business confidentiality and individual privacy is expected to play a central role in the Cybersecurity Framework, alongside risk management. In related programs, such as US-CERT[7], the Protected Critical Infrastructure Information (PCII) Program is used to prevent inappropriate disclosure of proprietary information or other sensitive data. Established in response to the Critical Infrastructure Information Act of 2002 (CII Act), the PCII Program enables members of the private sector to voluntarily submit confidential information regarding the nation's critical infrastructure to DHS with the assurance that the information will be protected from public disclosure.

We believe that strong privacy protection will help the adoption of the Framework by assessing the privacy risks at agencies and adequately safeguarding the information voluntarily submitted by companies as part of Federal law 6 U.S.C. Sec. 133, Protection of voluntarily shared critical infrastructure information. Based on our experience with similar deployments, Deloitte believes that a comprehensive "pre-assessment" of the Cybersecurity Framework for potential privacy implications and disclosure risks will minimize the perceived risk to the critical infrastructure operators and thereby increase adoption. We understand that the DHS will be tasked with assessing the privacy risks of agency's actions and programs and developing a publically available report outlining recommendations for mitigating those risks.

To support the development of a privacy-enabled Cybersecurity Framework and assist DHS in assessment activities, Deloitte recommends that the following steps are undertaken:

- Conduct an analysis of OMB guidance, NIST Standards, organization specific policies, and leading industry privacy practices to identify and rationalize a set of common privacy requirements.

[7] http://www.us-cert.gov/

- Work with DHS to develop a streamlined and automated process for collecting privacy assessment data and developing the assessment report in order to increase efficiency

- Identify processes and mechanisms for organizations to share critical infrastructure information that limit the risk of breach or disclosure

- Implement policies to mitigate privacy risks during information exchange

- Provide privacy training and specific guidance to all operators

As an example of this type of implementation, Deloitte Consulting LLP worked closely with the National Information Exchange Model[8] (NIEM) to help develop a privacy-enabled framework to facilitate secure information sharing. NIEM is a community driven, government-wide, standards group that focuses on sharing mission-critical information between federal, state, local and even international and commercial organizations.

To support the development of a privacy-enabled framework for NIEM, Deloitte Consulting LLP conducted an analysis of applicable privacy laws, OMB guidance, NIST Standards, organization specific policies, and leading industry privacy practices to identify and rationalize a set of common privacy requirements. As a part of the engagement's effort to provide privacy framework standards, the NIEM PMO will make available information on how to implement policies to mitigate the privacy risks during information exchange.

Deloitte Consulting LLP developed an internal framework which outlines recommended policies and practices. The framework outlined "Privacy by Design" principles and requirements, and described how NIEM can normalize privacy across their membership through the use of standardized PII classification and privacy tagging. To achieve this, we reviewed Information Exchange Package Documentation (IEPDs) and integrated leading privacy practices into NIEM's privacy framework by improving the existing IEPD guidance.[9] The NIEM PMO is preparing to make this privacy protection guidance available for member organizations.

Privacy considerations of the Cybersecurity Framework will span both private and public sectors, and it is essential that deep subject matter experience from both sectors is brought to bear on the development of the Framework. We have found that, in addition to the requisite privacy and security experience, extensive involvement with multiple stakeholder groups to identify and refine requirements and facilitate consensus building is required to develop an effective information sharing framework. These cross-disciplinary skills are essential for the development of a comprehensive data sharing Framework that protects critical infrastructure while safeguarding business confidentiality, individual privacy and civil liberties.

[8] https://www.niem.gov/Pages/default.aspx

[9] IEPDs are the final product of the NIEM exchange development process and are created from business requirements and technical artifacts that define the information exchange taking place between two organizations.

# 3 Conclusions

Deloitte is excited to participate in this important RFI by providing our perspectives in support of the Cybersecurity Framework. We have drawn upon our experiences in the public and private sectors to provide some suggestions of areas that we believe are critical to the success of the Cybersecurity Framework. We respectfully submit these to NIST for their consideration and would be pleased to follow up with a discussion at any time.