Initial Analysis of Cybersecurity Framework RFI Responses

1. Introduction

On February 26, 2013, NIST issued a Request for Information (RFI) on *Developing a Framework To Improve Critical Infrastructure Cybersecurity*.[1] The purpose of this paper is to describe the methodology used to perform the initial analysis of the submitted responses, and to identify and describe the Cybersecurity Framework themes that emerged as a part of the initial analysis. This initial analysis will serve as the basis for additional discussion and study at the Cybersecurity Framework Workshop #2 to be hosted at Carnegie Mellon University in Pittsburgh, Pennsylvania on May 29-31, 2013.

2. Analysis Methodology

NIST implemented a consistent and repeatable methodology to conduct its initial analysis of the RFI responses to Federal Register Notice 78 FR 13024.

a. Review and Categorize RFI Responses

Each submitted RFI response[2] was reviewed and analyzed by NIST.[3] The review of each RFI response included:

- Analysis of response coverage across critical infrastructure sectors and organization types;
- Identification of sections of text relevant to one or more of the RFI questions;
- Categorization of relevant text to category/sub-category, as shown in Appendix A; and
- Specification of terms and phrases that identify key points in each categorized section of relevant text.

The resulting categorization was then used to identify commonalities and recurring themes.

---

[1] Federal Register Notice 78 FR 13024, *Developing a Framework To Improve Critical Infrastructure Cybersecurity*, https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity

[2] http://csrc.nist.gov/cyberframework/rfi_comments.html

[3] Responses identified as spam or marketing and sales materials were not posted or reviewed by NIST.

b. Identification of Commonalities and Recurring Themes

Commonly used terms and phrases identified during the RFI response categorization helped identify commonalities and recurring themes among responses. Due to the variance in terminology and nomenclature across sectors, NIST identified and normalized terms that expressed key points. For example, the terms *security requirement*, *security measure*, and *security control* were often used interchangeably. To correlate these terms, NIST selected the term *security control* to label this concept. The selected term allows for consistency in nomenclature.

Examples of commonly used terms and phrases include, but are not limited to:

- *Cross-sector*
- *Sector-specific*
- *Incentive*
- *Performance Goal*
- *ISO 27000/ISO 27001*
- *Awareness/Training/Education*
- *SANS Top 20*
- *Challenge*
- *Supply Chain*
- *Metrics*
- *Not "one size fit all"*
- *Compliance*
- *Do Not Duplicate / Recreate*
- *Timely / Actionable Threat Information*
- *NIST SP 800-53*
- *Flexible*
- *Scalable / Adaptable*
- *Outreach*
- *Workforce*
- *Information Sharing*
- *Risk-based*
- *Maturity models*
- *Tools*
- *International / Global*
- *Risk-Management Approach*
- *Unambiguous / Actionable*
- *Situational Awareness*

NIST used the commonly used terms and phrases to group relevant text from RFI responses. These groupings identified recurring and common themes, which were then separated into three categories:

- **Framework Principles:** Characteristics and considerations the Framework must encompass.
- **Common Points:** Practices identified as having wide utility and adoption.
- **Initial Gaps:** For the purposes of RFI input analysis, initial gaps are those areas where RFI responses were not sufficient to meet the goal of the Executive Order.

CATEGORY	Framework Principles	Common Points	Initial Gaps
THEMES	• Flexibility • Impact on Global Operations • Risk Management Approaches • Leverage Existing Approaches, Standards, and Best Practices	• Senior Management Engagement • Understanding Threat Environment • Business Risk/ Risk Assessment • Separation of Business and Operational Systems • Models / Levels of Maturity • Incident Response • Cybersecurity Workforce	• Metrics • Privacy / Civil Liberties • Tools • Dependencies • Industry Best Practices • Resiliency • Critical Infrastructure Cybersecurity Nomenclature

Figure 1. Cybersecurity Framework Categories and Themes

The results of the initial analysis of RFI responses, including the description of each Cybersecurity Framework theme, identification of associated key terms and phrases, summary statistics, examples of RFI responses, and representative questions are included in the following sections.

This information represents an *initial*, high-level analysis of the inputs NIST has received to assist with the development of the Framework. Stakeholders are asked to evaluate the themes identified by NIST, determine if these themes are reflective of the comments received through the RFI, and assist in those areas where additional stakeholder engagement will be needed to develop a sufficiently robust Framework. To assist, NIST has provided a series of representative questions to encourage discussion on these key themes.

3. Categories and Themes

a. Framework Principles

Characteristics and considerations the Framework must encompass

Flexibility The Framework can apply across multiple sectors and across the diverse group of stakeholders (size, business needs, etc.).	
Associated key terms/phrases: • Not "one-size-fit-all" • Adaptable, non-prescriptive • Ecosystem approach	**Statistics:** Discussed in 87 out of 243 responses (35.8%).
RFI Response Examples: • "Cybersecurity risk is dynamic-we face a constantly evolving threat landscape, and we must develop best practices to help mitigate those shifting risks. CI/KR (Critical Infrastructure and Key Resources) Owners and Operators from divergent critical infrastructure (CI) sectors will be more apt to utilize a flexible risk management-based Cybersecurity Framework. This Framework allows companies to prioritize and focus on the most serious threats to the most critical assets, systems, and processes based on their particular industries and businesses-there is no "one size fits all" approach or "check-the-box" model that will work for everyone in all circumstances." • "A cross-sector critical infrastructure framework that is too flexible may fail to provide standards that effectively protect all critical infrastructure adequately. On the other hand, a cross-sector framework that is too rigid may require some sectors to implement standards that may not be applicable, or worse, detrimental to their mission. Meeting the needs of all critical infrastructure sectors with a single, balanced, real- world framework could become a costly, resource-intensive endeavor; there is no existing "silver bullet" on this matter. It is a challenge in which future technology will continue to play an important role in resolving. It should also be noted that life-cycles for control systems (such as water) are 15-30 years, and thus running under legacy control systems. These legacy systems have proven to be highly reliable, and requirements to comply with a cross-sector standard must be balanced with the challenge of replacing billions of dollars in aging infrastructure, not to mention the increasing regulatory compliance cost.**"** • "One-size fits all approaches fail to appreciate differences in unique business models, risk profiles, and resources and expertise between and within sectors. It also doesn't work for the dynamic nature of cyber threats; flexibility and agility are essential when managing cyber risks. On a practical level, this means that the Framework must establish desired outcomes and identify relevant global standards that are cost-effective and may help to achieve those outcomes, rather than defining a list of specific standards, controls, or measures that must be applied. Specific controls and measures may face difficulty in cross-sector	

implementation and would be outpaced by cyber threats."

- "Because cybersecurity is a shared responsibility in an interconnected world, the Framework should include all ecosystem stakeholders in its consultative process. A broad ecosystem approach, which includes various types of service providers, equipment manufacturers, software developers and end-user customers, is essential to developing effective cybersecurity strategies and responses that can be adopted across sectors through the existing sector coordination process and implemented in specific sectors through the existing Sector Specific Agencies (SSA) and Sector Coordinating Councils (SCC)."
- "Any Cybersecurity Framework must be both highly structured, yet, nimble and flexible enough to adapt in real time as threats emerge. In addition, standards or guidelines that amount to a static set of "checklists" without an initial risk-based approach may result in institutions being "compliant" without being effectively secure. There is also the risk to common standards developing within and across sectors, which prevent or limit a firm's ability to innovate in protecting its systems in a way that is not used by others. By adopting a common framework we could open the sector and critical infrastructure more generally to the same risks and threats due to the lack of independent development."

Representative Questions:

- What does flexibility mean in context of the framework? (Provide specific examples of ways flexibility can be built in.)
- What are strategies to ensure the framework is sufficiently flexible to ensure it is usable to organizations of varying sizes?

Impact on Global Operations

Impacts of the Framework on global and international operations.

Associated key terms/phrases:	**Statistics:**
• International • Global	Discussed in 157 out of 243 responses (64.6%).

RFI Response Examples:

- "This framework will likely become a global reference for cybersecurity policymaking. [Name removed] operates in over 60 countries and has customers using our products all over the world. It is important that the U.S. set a positive example regarding the essential role that global standards play for both industry and government. This framework presents an important opportunity to develop a product that many other countries can replicate and use in their policy environments. The U.S. could encourage global acceptance of this framework by seeking comments and support from other
  countries during its development. This adoption would be beneficial by creating consistent and cohesive approaches across those geographies as well as a commitment to the global standardization process.
  [Name removed] also recognizes there is a risk in developing this framework. Some governments might misunderstand the role of the framework and see its development as a sign that regulatory action is both necessary and warranted. To avoid this scenario, the U.S. government should conduct extensive outreach to educate other governments about the purpose and role of the framework and encourage similar approaches based on voluntary, global standards."
- "The relationship of practices to international standards will be sector dependent. Sectors that are already subject to international compliance requirements will be able to identify high level practices that may be applicable across sectors. Sectors with a more national focus such as Healthcare and Power would not be as concerned with international standards and practices. Many sectors follow standards and practices (ISO, IEEE, etc.) because they make good business sense. Compliance may be voluntary but forms a basis for identifying "best practices." National and international standards should be considered in any cybersecurity conformity assessment. In order to create a viable Framework that is accepted between sectors a phased approach is needed. National standards should be the starting point within each sector. Where a sector such as Finance is already involved with international standards, Framework development should proceed with the ultimate goal of alignment with existing international standards."

Representative Questions:

- What additional challenges are imposed globally in terms of privacy protection and the sharing of PII across borders?

Risk Management Approaches

The Framework should encourage the use of risk-based approaches rather than compliance-based approaches.

Associated key terms/phrases:

- Risk Management
- Approaches
- Metrics
- Controls

Statistics:

Discussed in 197 out of 243 responses (81.1%).

RFI Response Examples:

- "[…] has taken a Cyber Security approach that is rooted through the lens of Business Resiliency rather than a culture of compliance as compliance does not result in good security but good security does result in compliance."
- "Standards and approaches tend to become audit guidelines and the application of and attainment of these approaches becomes a goal in itself. This discourages innovative risk management and commits resources to compliance-based processes."
- "Cyber adversaries constantly change attack methodologies and tools so a compliance regime mandating specific controls across all critical infrastructures to manage threats and risks is doomed to fail as it precludes critical infrastructure providers from changing their practices quickly enough to address rapidly changing threats. Such mandatory, static controls would also make it simple for cyber adversaries to avoid the controls."
- "The IT Security budget is a zero-sum game, every dollar spent on compliance is a dollar not spent on risk-management. Therefore, balancing the need to deploy risk-appropriate security controls against deploying those mandated by regulatory or contractual obligations is one of the greatest challenges to improving cybersecurity practices."

Representative Questions:

- What are examples of effective risk-based approach?
- How is the effectiveness of a risk-based approach measured?
- How can implementation of the Framework be used to demonstrate compliance with existing regulatory requirements?
- What are other risk-based activities in your organization (ex, safety)?
- How do you implement, track, and measure the effectiveness of those activities?

Leverage Existing Approaches, Standards, and Best Practices

The framework should leverage existing risk management approaches, standards, and best practices. Owners/operators should not have to manage overlapping or duplicative approaches, dual standards and conflicting requirements.

Associated key terms/phrases:	**Statistics:**
• Regulations • Risk management approach • Standards • Duplicate • Conflict	Discussed in 81 out of 243 responses (33.3%).

RFI Response Examples:

- "Where there is an existing mandatory framework in place, like the electricity subsector's NERC-CIP, care must be taken in not forcing adherence to dual standards, or creating standards that might conflict with current requirements."
- "In developing this Framework, NIST should consider leveraging existing approaches and public-private cybersecurity partnerships and focusing on cost-effective risk management. We caution against developing new cybersecurity standards because they will likely overlap or duplicate the existing approaches already in use today."
- "When particular standards, approaches or aspects of an approach are followed, the decision is often the result of biased preference, consulting influence or on occasion overall ignorance of better suited alternatives. Providing clarity surrounding the existing dizzying choices of approaches and their suitability for application to an […] environment would be helpful."
- "A successfully-designed common framework will allow for better compatibility across industry and sector approaches. Modifications to harmonize existing standards into a common framework include: consolidating existing standards, broadening the scope of existing standards to make the standards more encompassing, and clearly marking the standards to be used for a particular type of asset."

Representative Questions:

- How can the Framework be effective in helping sectors with existing approaches, standards, and best practices?
- How should the Framework discuss factors/issues/guidance that could be considered by owners/operators in selecting which approach, standard, best practice set to leverage?

b. Common Points

Practices identified as having wide utility and adoption

Senior Management Engagement Senior management engagement in and accountability for cybersecurity.	
Associated key terms/phrases: • Senior Management • Buy-in • Education • Challenge	**Statistics:** Discussed in 163 out of 243 responses (67.0%).
RFI Response Examples: • "Risk portfolios for companies can often be broken down into four areas – Strategic, Operations, Legal/Compliance, and Financial/Reporting. Enterprise risk management within each pillar can be sponsored by an executive from a company's senior leadership team, who ensures that a regular and effective risk management rhythm is followed and accountability for enterprise risk exists." • "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." • "To the extent organizations have incorporated cybersecurity risk into the overarching enterprise risk, the organization has greater awareness of the impact of cyber threats to its operations. As a result, senior management is more involved and resources are more appropriately allocated to address the threats."	
Representative Questions • What exposure does your organization's senior management have into your cybersecurity practices? • What is the forum used internally to ensure that senior management is engaged in the organization's cybersecurity practices? • How does holding senior leadership accountable for implementing cybersecurity practices improve cybersecurity? • How can senior leadership avoid the "check-the-box" mentality when implementing cybersecurity practices?	

Baseline Security

Baseline security refers to the core cybersecurity practices that any organization should fulfill.

Associated key terms/phrases:

- Baseline Security
- Cyber Hygiene
- Common practice

Statistics:

Discussed in 51 out of 243 responses (20.9%).

RFI Response Examples:

- "Good cyber "hygiene"—or taking relatively simple behavioral precautions, such as keeping antivirus software up to date and backing up files—can reduce a significant percentage of cyber risks to information networks."
- "Cyber hygiene was specifically referred to by several of the presenters throughout the workshop and has been identified as the number one problem to tackle by leading experts in the field of information security. Former NSA Director Mike McConnell noted that 80-85% of recent breaches are due to poor cyber hygiene among users and three members of the framework team that kicked off the workshop alluded to this issue as well..,."
- "The [Name Removed] has determined that the compromise of critical digital assets (CDAs) associated with critical plant functions (e.g., safety, security, and emergency preparedness) is not acceptable. The [Name Removed] selected the NIST Special Publication (SP) 800-53, Revision 3, high security control baseline as the starting point for developing its suite of security controls (presented in RG 5.71, Appendices B and C). The [Name Removed] tailored the NIST SP 800-53, Revision 3, high security control baseline to account for the unique environment at nuclear power plants."
- "The SANS Critical Security Controls were developed with input from over 20 individual Federal agencies and contain recommendations for a baseline security program. The SANS Institute (SANS) Critical Security Controls are effective and provide a predictable level of protection. Building from this framework or incorporating these approaches into the planned NIST framework will enhance future efforts in the risk domain."
- "Broadly speaking ISO 27001, and NIST 800-53 (REV 4) are the baseline security control frameworks in uses at [Name Removed]. However, other specific regulatory needs are address in the context of the environment under the specific regulatory scrutiny, like PCI. [Name Removed] does not simply strive to comply, but rather to manage risk and make smart decisions on a situation-by-situation basis. NIST 800-30 is useful within [Name Removed] for Risk Assessments."
- "Common frameworks, like the ISO27000 series may provide a baseline for IT systems, but specific industry standards will still be required."

Representative Questions

- What are the core cybersecurity practices employed by your organization?
- How do these core cybersecurity practices vary based on size of the organization?
- How do these core cybersecurity practices change depending on the threat, or is it independent of the threat?
- How do you determine and define the baseline set of security practices that can be applicable across sectors?

Understanding the Threat Environment

Improved understanding, knowledge and information sharing of threats and the constantly evolving threat landscape and its impact on critical infrastructure.

Associated key terms/phrases:

- Information sharing
- Actionable
- ISACs (sector-specific)
- Supply chain
- Education
- Challenge
- Timely and actionable information
- Situational awareness

Statistics:

Discussed in 183 out of 243 responses (75.3%).

RFI Response Examples:

- "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."
- "In addition, standards and guidelines take a long time to develop and obtain industry acceptance for implementation. Thus, they may not be able to keep up with the continually changing threat landscape and may become ineffective for incident management."
- "We further believe that the federal government can play an important role in educating industry participants, retail and business customers and counterparties regarding their role in enhancing cybersecurity and protecting against cyber threats."
- "Shared situational awareness and timely information sharing is critical and must include focus on optimizing mission effectiveness and increased operational efficiencies to support a viable outcome for all parties."
- "…ensure that information sharing includes privacy and civil liberties safeguards. While personal privacy must be adequately guarded, improved information sharing should aim to enhance situational awareness to detect, prevent, mitigate, and respond to emerging and rapidly changing threats. Importantly, enhancing the situational awareness of critical infrastructure owners and operators would actually increase the security of personal information that is maintained on company networks and systems. Improved information sharing would benefit individuals' privacy protections, not detract from them."
- "The federal government's threat intelligence is often classified, which slows down its sharing with and use by private sectors. Also, the federal government may not have the technical expertise specific to critical infrastructure to determine which threat information is most needed by the sector. Within a critical infrastructure, antitrust laws may inhibit information sharing among companies."

- "One important role that various sector agencies and similar councils can play is the development of a comprehensive communication and information sharing strategy. Such a strategy could help foster support and knowledge of cybersecurity threats that may not have an immediate impact on one potential sector but allow for the other sectors to gain valuable intelligence that may allow them to modify their recommended security postures. Information sharing is most successful, valuable and effective when it includes liability and confidentiality protections for providers and receivers. Sector specific agencies and their stakeholders represent a valuable communication channel for NIST in the promotion of any developed framework."

Representative Questions:

- Does your organization currently have processes for obtaining threat information?
- What are some of your organization's impediments to sharing threat information outside of your organization?
- How could the Framework address these impediments?
- What resources exist today to enable greater sharing of threat information?
- What types of resources are needed to more effectively share threat information?

Cyber Risk in the Context of Business Risk

Cohesive risk management process that addresses cyber risk in conjunction with other types of risk at the organizational level and mission/business level.

Associated key terms/phrases:

- Assessment methods
- Business risk
- Resources
- Economics
- Regulations
- Operational impact
- Prioritization

Statistics:

Discussed in 167 out of 243 responses (68.7%).

RFI Response Examples:

- "Organizations typically consider this particular risk – cyber risk – alongside other risks, such as natural disasters, supply chain risks, human resources risks, espionage, etc. Identified risks are then evaluated holistically, with the organization determining how the risk (if realized) could affect its operations, finances, and reputation. … Depending on the nature of the risk, its prioritization placement, its probability of realization, and its potential impact, businesses then pick among the traditional strategies of avoid, reduce through mitigation, transfer, or accept, depending on their own business plans, the strategy's cost-justifiability, the company's risk tolerance levels, and/or resource availability."
- "A systematic process should be followed to evaluate risk. Such a process leads to a business decision regarding the available choices concerning risk. These include: Accepting the risk; Mitigating, reducing, or eliminating the risk; or Transferring the risk (e.g., insurance). [Name Removed] recommends a thorough review of the available options to mitigate the risk be conducted before deciding to accept the risk. Although accepting the risk can sometimes be a valid choice, in some instances business decisions are made to accept a risk that could otherwise be economically mitigated if the risk assessment team had current knowledge of the methods and techniques to secure the system. "
- "Business process risks are assessed based upon a number of factors and weighted based upon the potential cost of various risks. Computing risks are also reviewed as part of an integrated risk management process that considers risks of loss of information integrity, information disclosure, information or processing loss, risks of failing to meet contractual or regulatory requirements, impact on others, and financial consequences. Cybersecurity risks fall under this general computing risks area and are assessed using its framework."

Representative Questions:

- What is the scope of business risk?
- How do organizations consider the interconnected nature of systems when making business and cyber risk decisions?
- How can the framework help owners/operators make good cyber security decisions in the broader context of business risk?
- Does the framework need to address the relationship with business risk, or can it represent cyber risk management as a standalone function?

- How can the framework be compatible (easier to use) with business risk strategies?

Separation of Business Systems and Operational Systems

Business systems and operational systems have traditionally been very different. However, they can now be core connected, share the same platforms, and have integrated functionality. The practice of separating these systems was the single most referenced best practice, often referred to as critical.

Associated key terms/phrases:

- Core practice
- Integration
- Risk
- ICS
- ISA/IEC 62443

Statistics:

Discussed in 146 out of 243 responses (60.0%).

RFI Response Examples:

- "We would add that policy controls are very important, for example a prohibition on mixing sensitive operations with routine e-mail and web use on the same system."
- "Today's ICS are being increasingly connected to company business systems that rely on common operating platforms and are accessible through the Internet. Even though these changes improve operability, they also create vulnerabilities because improvements in the security features of control systems are not concurrent."
- "Historically this has been a standard design principle. With rising adoption of COTS technologies and rising need for multi-system integration as well as integration with the enterprise architecture the separation of systems used for the operation of critical infrastructures from those used for regular business operations has been weakened in practice. However, the recognition of cyber security risks implied by this weakened separation has recently led to a return of this principle. Guidelines and standards such as the ISA/IEC 62443 […] emphasize this as well."
- "Companies may employ a "zoning model" to differentiate and segregate business and operational systems according to system content and risk. Footnote: The separation of business and operational systems may not be appropriate in all circumstances, particularly for smaller providers, or in instances where such segmentation adversely affects network functionality, operational controls, or system usability."

Representative Questions:

- Separating business and operational systems appears to be a recommended practice. Are there any barriers associated with the implementation of this practice? If so, what are they? Can they be overcome?
- The ability to use more COTS-like products and internet connectedness for operational systems may introduce new vulnerabilities to operational systems. What are the best practices for addressing these vulnerabilities?
- If an owner/operator decided to co-locate business and operational processes on the same system for valid reasons (to the owner), what recommendations or best practices aid in recognizing and managing the risk?

Models / Levels of Maturity

The term "maturity" relates to the degree of formality and optimization of processes, from ad hoc practices, to formally defined steps, to managed result metrics, to active optimization of the processes.

Associated key terms/phrases:

- Maturity Model
- Level of Maturity
- Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

Statistics:

Discussed in 48 out of 243 responses (19.7%).

RFI Response Examples:

- "For the electricity sector, the Department of Energy's, Electric Subsector Cybersecurity Capability Maturity Model (ES-C2M2) offers a good starting point for the Framework, along with the DOE's companion Risk Management Process guideline."
- "In developing its Cybersecurity Framework, NIST should recognize the many affirmative steps already taken by the sector and should incorporate the industry's approaches into the guidelines and standards that NIST develops. NIST also may need to account for differences in sectors when developing its framework. A 'one-size-fits-all' approach would likely be ineffective, as sectors will approach the Cybersecurity Framework from different positions (in terms of maturity and regulatory requirements) and face different threats. Best practices should be used to define the objective – not the specific processes and procedures to achieve the objective. This approach can provide the latitude for defining a strong Framework without constraining an organization to use its creativity and innovation."
- "Due to the different levels of maturity across and within sectors, there likely will need to be sector-specific analysis of the current state of security controls and timeline for adherence to new standards. Each sector should identify specific control areas and relativity to sector assets but the overall framework should be consistent with the standard framework. We should avoid industry-specific variants of the entire framework, which adds complexity and hinders cross-sector collaboration."
- "Different sectors and providers are at different levels of maturity in developing processes and procedures to respond to the cybersecurity challenges. Sharing the lessons learned within the information technology industry can shorten the learning and response timeframe. Use of a Capability Maturity Model (CMM) in implementing the Framework will allow individual sectors to develop tailored responses to their unique challenges while providing an overarching structure to share common problems and solutions. A CMM-integrated Framework will also provide mechanisms to measure progress made over time towards increasing security. The Capability Maturity Model Integration (CMMI) program is a well-recognized standard that could be used within the Framework. The National Initiative on Cybersecurity Education (NICE) CMM with its three main areas of focus: integrated governance; process and analytics; and, enabling technology, also provides a flexible organizational structure adaptable to the requirements of the Framework."

Representative Questions:

- What are characteristics of a meaningful, effective, and scalable maturity model?

- What are examples of maturity models in use today?
- How could a maturity model be incorporated into this Framework?

Incident Response

The capability to continue or resume operations in the event of disruption of normal operation. Incident response entails the preparation, testing, and maintenance of specific policies and procedures to enable the organization to recover operational status after the occurrence of a disruption.

Associated key terms/phrases:

- Incident response
- Tests

Statistics:

Discussed in 68 out of 243 responses (27.9%).

RFI Response Examples:

- "As NIST considers what is needed to support the "response" portion of the risk management framework, [name removed] would strongly encourage NIST to consider the Incident Command System (ICS) as a foundation for any recommendations. ICS has an established history of success in the United States, and it is a well-recognized approach for incident response. Some of the strengths of ICS include:
  - Allowing for the integration of facilities, equipment, personnel, procedures and communications operating within a common organizational structure.
  - Enabling a coordinated response among various jurisdictions and functional agencies, both public and private.
  - Establishing common processes for planning and managing resources.

  Clearly, incident response is a priority for all companies in the IT sector, given the ways in which attackers attempt to use vulnerabilities in software or compromise features in a product or service to commit some harm. There are a number of steps that can be considered when looking at incident response, in particular for CIs."
- "The sector coordinating councils, the Electricity Sub-sector Coordination Council (ESCC) and the Government Coordinating Council (GCC), should focus on bringing together electricity and government executives to focus on key cybersecurity challenges such as sector-wide incident response to a large-scale cyber event. Working groups such as the Energy Sector Control Systems Working Group (ESCSWG) can be used to implement the coordinating council priorities."
- "Among other things, the standard [NERC standard CIP-008-3] requires entities subject to the standard to develop, maintain, and implement a cybersecurity incident response plan, which includes processes and procedures for classifying events as reportable cybersecurity incidents, reporting such incidents to the ES- ISAC, and retaining documents relevant to any such reportable incidents."
- "[Name removed]'s normal incident response processes comprehend rapid changes in the cybersecurity risks and threat landscape. Within the IT incident response process there is a triage process which allows for a risk management-based escalation in response to changes in threat severity. In cases where escalation is necessary, escalations rise to the appropriate level of management and may trigger corporate emergency operations, as appropriate. Similar processes are mirrored in our Product Security Incident Response Team, which also has an escalation path to senior business unit and corporate management. [Name removed] has dedicated Threat Management and Threat Intelligence teams chartered to monitor and respond to changes in the threat landscape. Regular threat briefings occur with security and management stakeholders to increase awareness of the emerging threat landscape and to adjust our internal controls to address such changes. [Name removed] has an internal cross- organizational team that maintains our Threat

Agent Library and monitors for actor-based threats, and is a resource for internal risk management and security personnel. [Name removed] tests and exercises its enterprise and product security escalation and response processes and makes continuous improvement adjustments as a result.
Representative Questions: • What best practices enable organizations to respond to cyber incidents effectively? • What areas of incident response require additional attention given that this is a relatively mature area of cybersecurity? • What role should the Information Sharing and Analysis Centers (ISACs) play?

Cybersecurity Workforce

A skilled cybersecurity workforce is important to meet the needs of critical infrastructure cybersecurity.

Associated key terms/phrases:	**Statistics:**
• Training/education • Outreach • NICE	Discussed in 150 out of 243 responses (61.7%).

RFI Response Examples:

- "… that a government-led campaign (similar to the one for general cybersecurity practitioners)is needed, including new educational degrees or concentrations/certificates, incentives for entering careers in the field of utility cybersecurity, and changes to college curricula to increase general awareness among technology professionals. [Name removed] applauds the US government efforts in establishing National Centers of Academic Excellence in Information Assurance Education (CAE/IAE) as well as the National Initiative for Cybersecurity Education (NICE). These efforts are currently creating the underpinnings of a cybersecurity workforce for the future. Like the current shortage of general cybersecurity experts, there is a shortage of qualified cybersecurity experts that have expertise in utility networks. Utilities are experiencing both a shortage of senior talent that can advocate cybersecurity priorities to company executives, and a shortage of qualified cybersecurity talent that can implement the necessary practices within the operational environment. There are simply not enough qualified cybersecurity professionals who have experience in the utilities sector."
- "…ensure that information sharing includes privacy and civil liberties safeguards. While personal privacy must be adequately guarded, improved information sharing should aim to enhance situational awareness to detect, prevent, mitigate, and respond to emerging and rapidly changing threats. Importantly, enhancing the situational awareness of critical infrastructure owners and operators would actually increase the security of personal information that is maintained on company networks and systems. Improved information sharing would benefit individuals' privacy protections, not detract from them."
- "There are many examples of the difference the right skills and staffing can make in the current environment - and this difference will persist for a while, even if automation and game changing research result in simpler ways to secure complex systems. There are four elements of any strategy to deal with this challenge, all of which can be accelerated by governmental action:
    - Promoting and funding the development of more rigorous curricula in schools (there is significant activity underway here, but there is a consensus that more is needed);
    - Supporting the development and adoption of technically rigorous professional certifications;
    - Using a combination of hiring, acquisition, and training resources to raise the level of technical competence of those who build, operate, and defend systems; and

- Assuring, as with other disciplines, like engineering or medicine, there is a career path to reward and retain those with high-level technical skills, both in the civilian workforce and in the uniformed services."

Representative Questions:

- What types of resources exist and are employed today?
- How effective are these resources?
- What types of resources are needed to improve the cybersecurity workforce needed?
- How are cybersecurity responsibilities defined and assigned within the organization?
- How are cybersecurity responsibilities incorporated into job descriptions or performance evaluation criteria?
- How are cybersecurity knowledge, skill, and ability gaps managed for the organization?

c. Initial Gaps

Areas where RFI responses were not sufficient to meet the goal of the Executive Order.

<table>
<tr><th colspan="2">Metrics
Performance-related data used to monitor and measure the accomplishment of goals and objectives by quantifying the implementation, efficiency, and effectiveness of security measures.</th></tr>
<tr><td>Associated key terms/phrases:
Performance goals
Metrics
Measures</td><td>Statistics:
Discussed in 144 out of 243 responses (59.2%).</td></tr>
<tr><td colspan="2">RFI Response Examples:
“A key issue that can limit of any CyberSecurity Framework is how to assure interoperability and scalability between existing and proposed instantiations of the proposed CyberSecurity framework by members of industry and government. To address this limitation, a hierarchical framework approach is recommended, whereby (1) The top layer would contain definitions of common terms, identification and definition of metrics to be applied in assessing risk and the performance of standards and best practices applied to systems, and core cyber defense standards and principles (best practices) that are generally applicable to all critical infrastructure domains.”
“Metrics should be applied to assess effectiveness of application security programs. Among the direct application security-specific metrics available are vulnerability scores and patch coverage. These metrics can indicate the quality of application coding. Indirect data handling metrics, such as the percentage of data encrypted, can indicate that responsible decisions are being made from an application architecture perspective.”
“Cybersecurity metrics/measures must be based on business or mission goals and objectives. Without being tied to the mission context of the organization it is challenging to make these metrics meaningful to provide actionable data for executive decision making”</td></tr>
<tr><td colspan="2">Representative Questions:
What are specific examples of metrics that are currently used?
How are they measured?
What are suggestions for metrics that can apply across a broad range of critical infrastructure (size and scope)?
How to develop metrics that can apply across multiple sectors?
How can the Framework explain the relationship between risk management and maturity models?</td></tr>
</table>

Privacy and Civil Liberties

The ability of individuals to avoid harmful consequences to themselves arising from the use or exposure of information about themselves; civil rights and freedoms that provide an individual specific rights.

Associated key terms/phrases:

- Legislation/regulation
- PII
- FIPPS
- OECD
- Privacy Act of 1974
- Freedom of Information Act

Statistics:

Discussed in 127 out of 243 responses (52.2%).

RFI Response Examples:

- "Privacy safeguards are vital to cybersecurity. Robust privacy protections promote cybersecurity in a number of ways. Proper privacy protections, including adequate data protection and avoidance of unnecessary transfers of personal information, limit exposure to a cyberattack or other type of breach and minimize the risk to individuals when such attacks occur. Protecting individual privacy keeps cybersecurity efforts focused on robust efforts to secure cyberspace, prevent attacks, and minimize damage and disruption when attacks do occur"
- "Organizations must classify and protect confidential and restricted data as per national and state law, and the utility industry has a commitment to protect customer privacy. While access controls are included in most frameworks, not many of the current industry requirements speak to privacy concerns. States already have existing privacy and breach laws that provide coverage for personally identifiable information. Further, the DOE and NIST consultative processes should be encouraged to continue."
- "Importantly, enhancing the situational awareness of critical infrastructure owners and operators would actually increase the security of personal information that is maintained on company networks and systems. Improved information sharing would benefit individuals' privacy protections, not detract from them."
- "Any legislative or regulatory approach taken by the government should encourage adoption of practices in compliance with Fair Information Practice Principles (FIPPS), including adequate notice to impacted individuals and consideration of "proportionality" in developing a cybersecurity framework. Proportionality is the balancing of the intended activity with the potential impact on an individual's privacy rights and related civil liberties. For example, policymakers are currently considering various approaches to enabling more effective sharing of cyber threat information between government and industry, in a manner that balances the essential need to share as much cyber threat information as quickly as possible with as many stakeholders as possible, while also optimizing for the privacy and civil liberties of citizens and the needs of businesses for strong liability protections to incentivize such sharing. In this and all contexts, including under the Framework, the question should always be asked whether there is a less intrusive manner to implement a specific regulatory cybersecurity solution that will minimize the impact on an individual's rights."

Representative Questions :

- In addition to data security issues, what kinds of privacy and civil liberties issues arise out of cybersecurity practices?
- How do we quantify privacy and civil liberties risks arising out of cybersecurity practices?
- What should the Framework include with respect to privacy and civil liberties protections?
- How does your organization ensure that privacy and civil liberties are maintained?
- What is the organizational overlap between cybersecurity and privacy?

Use of Tools Tools allow the organization to attain a higher level of situational awareness with respect to cyber risk. For example, tools could enable greater visualization, compliance checking, continuous monitoring, or asset management. Tools are not necessarily products; they can be processes or personnel resources that enable security.	
Associated key terms/phrases: • Automated tools • Measure risk • Monitoring tools	**Statistics:** Discussed in 136 out of 243 responses (55.9%).
RFI Response Examples: • **"**Tools to facilitate the implementation of a new cybersecurity framework such as checklist summaries, use cases, and a map of the Framework to other sector specific and cross‐sector cybersecurity guidance will also help to encourage adoption." • "Provide implementation guidance, case studies, automated tools, and other assistance to simplify adoption" • "Monitoring tools that are used in business environments may not be appropriate in a process control environment."	
Representative Questions: • Is the need for automated tools generally for audit/reporting, managing cyber risk assessment process document control, cyber risk assessment workflow, etc.? • What attributes could the tools have that would lend themselves to help small and mid-size owner/operators? • What capabilities are enhanced by automation and the use of tools? • What are the associated process and people controls that should accompany the use of tools?	

Dependencies

Providing products, services, and functionality has become increasingly dependent on a variety of entities. Organization's critical functions rely on other organizations in order to perform.

Associated key terms/phrases:

- Supply Chain
- Sector Dependency
- Critical Assets
- IT dependency
- Software quality

Statistics:

Discussed in139 out of 243 responses (57.2%).

RFI Response Examples:

- "Corporations have a wide range of assets and processes that may be considered critical under some definitions. Many of these are dependent on externally provided services such as power, water, telecommunications (such as data transfer via satellites or local microwave from an offshore rig to a service provider), financial services, and transportation."
- "Suppliers do not provide "Secure by Design" products. This is particularly true in process control environments where vendors have not certified their systems for various cybersecurity tools that would greatly improve our security posture."
- "While we agree that owners and operators of critical infrastructure play a critical role in protecting their systems, processes and information, the IT and telecommunication sectors play an equally critical role to ensure that software and hardware products and telecommunication services are provided to the end user community that have the most up to date and advanced cyber security protection available. […] Therefore, the IT industry has a higher stewardship responsibility to work with all critical infrastructures to ensure their products are secure for their intended use."

Representative Questions:

- What is generally considered a 'critical asset'? Are they only locally defined?
- Can critical assets be defined at the national level? At the sector level? Has any sector defined them; and if so what are they?
- What are effective ways to address dependencies in the framework?
- Are there significant considerations for the difference between identified sector dependencies and local dependencies that need to be addressed?
- Should the framework include the concept of sector level dependencies such that sector-level discussions are encouraged? Or are these dependencies really only addressed at the owner/operator level?
- How can the framework help owners/operators make informed decisions about the quality/security of the IT products/services procured?

Industry Best Practices

Industry best practices are the activities that are performed by multiple organizations that allow that organization to achieve repeatable, reliable, and scalable service. These practices range from low level implementation details to high level risk management techniques.

Associated key terms/phrases:

- Best Practice
- Good Practice
- Practice

Statistics:

Discussed in 159 out of 243 responses (65.4%).

RFI Response Examples:

- "A best practice of how to define and measure a risk by breaking into 3 pieces:
  - Personnel – How many individuals can influence this risk – positive or negative
  - Probability –What is the probability of this risk being exploited
  - Collateral Damage –What further exposure or damage can this risk introduce."
- "They define best practices such as penetration testing, executive ownership, as well as tools such as anti virus, firewalls, intrusion prevention, web application firewalls, and even vulnerability scans. However, none of these standards are designed to measure and manage cybersecurity risk."
- "The Risk Management Framework (RMF) described in SP 800-39 provides a baseline for the development of appropriate risk mitigation actions. The RMF includes a well-defined set of information security standards and guidelines that, when implemented, can be used to demonstrate compliance with industry "best practices" for security."

Representative Questions:

- At least one commenter suggested that "best practices" may not be good or best, just frequently repeated. How are best practices defined? What constitutes a best practice?
- Should we reference the best practices already instantiated in accepted industry/international Standards?

Resiliency

Resiliency is the ability to sustain an attack and continue to deliver critical services to customers with minimal or no downtime. In the context of cybersecurity, resiliency can address: self-healing networks, fail-over, hot swaps, etc.

Associated key terms/phrases:

- Resiliency
- Resilience
- Resilient

Statistics:

Discussed in 113 out of 243 responses (46.5%).

RFI Response Examples:

- "… the use of non-mandatory best practices has resulted in immeasurable increases in communications network resiliency and security."
- "Each of our members is committed to working with their respective suppliers … to enhance the protection and resiliency of the nation's critical infrastructure from cyber attack."
- "One area that requires extra attention by the Framework is mission and system resiliency. If system backup and recovery procedures are not properly designed there is an increased risk of PII being exposed or compromised because proper controls are not in place and enforced."
- "For example, under the joint partnership of FSSCC and FBIIC, our sector has developed leading practices to mitigate risks associated with the resiliency of the telecommunications infrastructure including critical undersea cables, , and other important risks or threats facing the security and resilience of the sector. Likewise, the FS-ISAC routinely shares risk mitigation tactics and information to address vulnerabilities and evolving cyber-attacks."

Representative Questions:

- What does it mean to be resilient in terms of the EO/CSFW?
- Who decides what is considered sufficient resiliency?
- How do organizations weigh the cost of resiliency against the value?
- How do organizations determine the appropriate level of protection, detection, and recovery capabilities?
- What are some potential ways that the framework provides the flexibility needed for organizations to make the decisions most appropriate for their environment?

Critical Infrastructure Cybersecurity Nomenclature

As the Framework is developed, it is important that terms and concepts are fully defined such that they are clear and consistent. The cyber risk space has a wealth of terms and concepts, with many terms mapping to many concepts.

Associated key terms/phrases:

- Nomenclature
- Terms
- Mapping
- Unambiguous
- Standards

Statistics:

Discussed in 66 out of 243 responses (27.1%).

RFI Response Examples:

- "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.)."
- "Each sector, though, has different key assets that will be prioritized and protected differently. Reaching a decision within the Framework on taxonomy and severity of risks will be a challenge."
- "A key issue that can limit of any CyberSecurity Framework is how to assure interoperability and scalability between existing and proposed instantiations of the proposed CyberSecurity framework by members of industry and government. To address this limitation, a hierarchical framework approach is recommended, whereby (1) The top layer would contain definitions of common terms, identification and definition of metrics to be applied in assessing risk and the performance of standards and best practices applied to systems, […]"

Representative Questions:

- How far should the Framework go to help ensure successful mapping of concepts to existing approaches, standards, BPs, etc.?
- Is it acceptable that NIST rely on its own set of terms and definitions in the Framework?

Appendix A – RFI Input Categorization

Category	Sub-Category	Relevant RFI Questions
1 | Current Practice	1| Risk Management Governance	• 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? • Where do organizations locate their cybersecurity risk management program/office? • How do organizations define and assess risk generally and cybersecurity risk specifically? • To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management? • What additional approaches already exist? • Which of these approaches apply across sectors? • Which organizations use these approaches? • How do these approaches take into account sector-specific needs? • Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards? • Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?
	2| Risk Management Implementation	• What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels? • What additional approaches already exist? • Which of these approaches apply across sectors? • Which organizations use these approaches? • How do these approaches take into account sector-specific needs? • Are these practices widely used throughout critical infrastructure and industry? • How do these practices relate to existing international standards and practices? • Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure? • How are standards or guidelines utilized by organizations in the implementation of these practices?
	3 | Challenges / Gaps	• What, if any, are the limitations of using such approaches? • Are some of these practices not applicable for business or mission needs within particular sectors? • Which of these practices pose the most significant implementation challenge?
	4 | Dependencies	• What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?
2 | Regulation / Legal	1 | Requirements	• 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? • 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?
	2 | Challenges / Gaps	

Category	Sub-Category	Relevant RFI Questions
3 | Future Practice	1| Risk Management Governance	
	2| Risk Management Implementation	
	3 | Challenges / Gaps	• What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure? • What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure? • What, if any, modifications could make these approaches more useful?
	4 | Roles	• What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?
4 | Privacy / Civil Liberties		• What risks to privacy and civil liberties do commenters perceive in the application of these practices? • How should any risks to privacy and civil liberties be managed?
5 | Conformity	1 | SDO Role	• What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?
	2 | Assessment Information	
6 | Metrics	1 | Current	• What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?
	2 | Suggested	
7 | Other Topics		• What other outreach efforts would be helpful? [KEYWORD: outreach] • What are the international implications of this framework on your global business or in policymaking in other countries? [KEYWORD: global] • In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?
8 | Framework Development		• When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

Appendix B – RFI Questions and Initial Category/Sub-Category Mapping

RFI Question	Category	Sub-Category
Current Risk Management Policies		
1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?	3	3
2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?	3	3
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?	1	1
4. Where do organizations locate their cybersecurity risk management program/office?	1	1
5. How do organizations define and assess risk generally and cybersecurity risk specifically?	1	1
6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?	1	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?	1	2
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?	2	1
9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?	1	4
10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?	6	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?	2	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?	5	1
Use of Frameworks, Standards, Guidelines, and Best Practices		
1. What additional approaches already exist?	1	1
	1	2
2. Which of these approaches apply across sectors?	1	1
	1	2
3. Which organizations use these approaches?	1	1
	1	2
4. What, if any, are the limitations of using such approaches?	1	3
5. What, if any, modifications could make these approaches more useful?	3	3
6. How do these approaches take into account sector-specific needs?	1	1
	1	2
7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?	8	
8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?	3	4
9. What other outreach efforts would be helpful?	7	
Specific Industry Practices		

Areas of interest: 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.		
1. Are these practices widely used throughout critical infrastructure and industry?	1	2
2. How do these practices relate to existing international standards and practices?	1	2
3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?	1	2
4. Are some of these practices not applicable for business or mission needs within particular sectors?	1	3
5. Which of these practices pose the most significant implementation challenge?	1	3
6. How are standards or guidelines utilized by organizations in the implementation of these practices?	1	2
7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?	1	1
8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?	1	1
9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?	4	
10. What are the international implications of this framework on your global business or in policymaking in other countries?	7	
11. How should any risks to privacy and civil liberties be managed?	4	
12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?	8	