Response to the NIST Request for Information on Developing a Framework to Improve Critical Infrastructure Cybersecurity

Carnegie Mellon University
Software Engineering Institute
CERT® Program

April 2013

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

DM-0000295

Table of Contents

The Software Engineering Institute (SEI) is a Federally Funded Research and Development Center administratively homed at Carnegie Mellon University. The CERT® Program of the SEI focuses on identifying and solving the nation's cybersecurity challenges.

CERT® Program at the Software Engineering Institute

The CERT® Program has over a decade of practical experience in the successful development of models and frameworks that help organizations measure, implement, and improve cybersecurity practices. Our goal is to enable organizations to transform uncertainties into manageable operational risks and then to efficiently manage those risks. We achieve this by using scientific rigor in our collection and analysis of data to drive the development and use of our products and services. As a well-established trusted resource, we have been actively engaged in efforts to improve the resilience practices of the nation's critical infrastructure owners and operators.

The SEI and the CERT Program address cybersecurity through an integrated, holistic approach that combines our knowledge and experience in software engineering process improvement, malware detection and analysis, digital forensics, secure coding practices, insider threat, and cyber workforce development. Our location allows us to work with the world-renowned faculty and students on Carnegie Mellon University's main campus and work closely with departments including Computer Science, Machine Learning, Statistics, Business, and many other disciplines.

Leveraging our work with public- and private-sector partners and the Critical Infrastructure Key Resources (CIKR) owners and operators, we have responded to the RFI questions based on our experiences and observations along with recommendations that may be useful in the planning for a Cybersecurity Framework.

It has been our experience and practice that any Framework should use a standard glossary of terms, such as the DHS Risk Lexicon or ISO 31000. We have included a few definitions in Appendix A for reference.

Current Risk Management Practices

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

Based on our experience and observations:

I. Establishing an integrated approach to managing cybersecurity-related risks
   a. Challenges with integrating organizational, sector, and regional activities
   b. Communication and collaboration among groups
   c. Allocating resources to cybersecurity, a non-revenue producing activity

II. Identification of critical assets and services
   a. Absence of a common taxonomy
   b. Inadequate methods for service/asset definition and evaluation

III. Risk metrics and measures
   a. Lack of common, accepted definition of cyber risk metrics
   b. Lack of scientific rigor in cyber risk metrics (e.g., no systematic validation)

c. No common framework to facilitate comparison and benchmarking
d. Cybersecurity metrics not integrated with other business measures
e. No measures of performance or effectiveness for risk practices

IV. Information sharing
a. Information vs. intelligence dilemma (which information is most relevant)
b. Regulatory and internal legal hurdles
c. Classification and dissemination of threat intelligence
d. Reluctance to reveal information that may create adverse publicity
e. ISAC shortcomings

V. Identification of dependencies
a. Understanding interdependencies among national critical infrastructures (i.e., an organization's position relative to and relationship with other CIKR organizations)
b. Inadequate methods for determining cyber dependencies of services and assets
c. Absence of tools and techniques designed to identify dependencies within sectors/subsectors

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

Based on our experience and observations:

I. Diversity of mission and objectives
a. Existing discipline and sector-specific standards designed to address specific operating requirements
b. Limited applicability of generic standards and measures
c. Ability to address both information technologies as well as specific operational technologies unique to each sector and sub-sector

II. Effective communication
a. Organizational and sector "stovepipes"
b. Establishing trusted relationships
c. Variations in terminology and taxonomies

III. Scale
a. Organizations vary widely in size and complexity
b. Resources required for framework implementation

IV. Sector reticence
a. Aversion to perceived oversight/regulation
b. Competing initiatives

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?

Based on our experience and observations:

I. The presence, quality, and level of attention of such policies vary widely by organization.

a. Some organizations are policy averse; of those
    a. some have not considered or implemented any such policies
    b. others have issued board-level or senior-management-level directives that have the weight/function of policy but are not called policy
b. Organizations in highly regulated industries typically have policies, but the level of attention and rigor tends to vary.
c. Larger, investor-owned organizations tend to have a web of policy that directs them.
d. Larger organizations may have an enterprise risk committee at the board level. At some of these organizations, cybersecurity risk is on the radar of the risk committee; at others, it is not.
e. Larger organizations also tend to have auditing groups that occasionally test for policy compliance.

We recommend:

I. Employing a governance approach and process that utilizes policy, procedures, practices, standards, and guidelines as implementation artifacts and constructs
II. Policies, procedures, and/or organizational directives should be utilized because they
    a. represent an organizational commitment to ensure that appropriate security behaviors are established and measured
    b. provide business rules that help guide practices and behavior
    c. help ensure that cybersecurity program activities persist over time
    d. help ensure consistency in large organizations
    e. help avoid dependence on a single individual or small group
III. Such policies, procedures and/or directives should
    a. be compact enough that they can be easily changed over time to match current threat/risk conditions
    b. direct routine risk assessments and analyses (driven by schedule) and those triggered by events
    c. direct that a risk repository be established, maintained, monitored, and used as a basis for other monitoring activities in the organization to drive mitigation of risks
    d. direct improvements to policies, procedures, and directives based on lessons learned
IV. A senior-level role (or body) should monitor the status of major risks to the organization. This is a good practice and can help ensure that resources are provided and appropriately allocated to address risk.

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

Based on our experience and observations:

I. Industry survey data illustrates wide variability in where organizations place the various organizational components of such programs as cybersecurity, information security, IT and operational risk management, IT disaster recovery, and business continuity. (See two sample survey results below from Gartner; the first focused on information security programs and the second focused on other operational risk management programs.)

We recommend:

The location the organization's cybersecurity program/office does not have a single correct answer. In fact, it is not even a single question, but rather a series of complex and interrelated questions about both the organizational structure and the location of the cybersecurity functions. The location and the structure of the most appropriate security organization for a specific organization will depend on a wide range of factors such as

- the industry vertical within which it operates
- the size of the organization
- the threat landscape
- the organization's risk appetite (tolerance or threshold)
- the legal and regulatory frameworks within which it operates
- the maturity of the enterprise's information security and risk management programs and processes
- geographical issues
- cultural issues, management style, and organizational politics
- the enterprise's overall structure

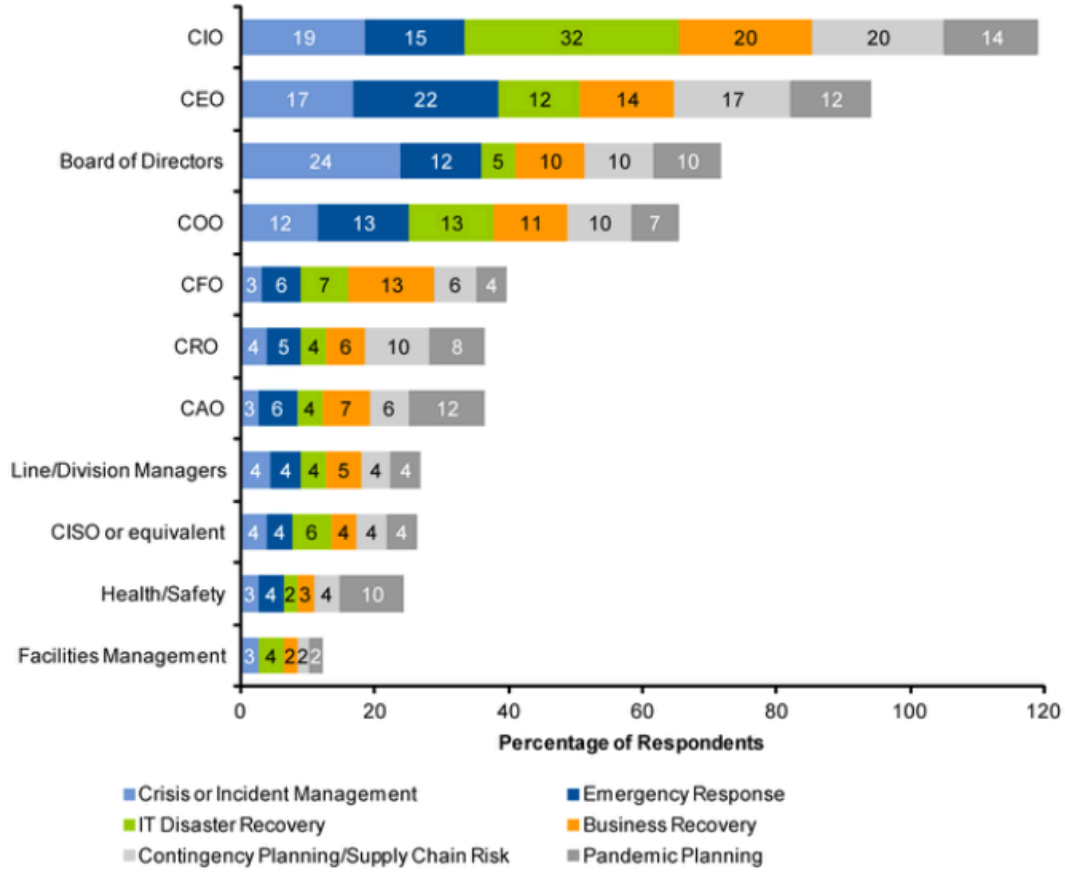
In addition to organizationally unique factors such as those listed above, there are also some fundamental and strategic cybersecurity principles that should drive the structure and the placement of an organization's cybersecurity program. Such principles include the

- integration of cybersecurity considerations into organizational planning and decision making
- need for centralized coordination of information security in federated environments
- emergent nature of operational and strategic security functions
- need to drive information security activities and behaviors closer to the business and closer to other corporate risk management functions
- need to emphasize that information security encompasses much more than IT
- inherent nature of information security—that is, a set of disciplines, controls, and behaviors that should cross all horizontal and vertical functions

Figure 1. Reporting Line of the Most Senior-Level Person Dedicated Exclusively to Information Security

Source: Gartner (December 2012)

Figure 2. Who Has Primary Responsibility for Each of the Following Activities?



Acronym Key: CISO — chief information security officer

Source: Gartner (July 2012)

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

Based on our experience and observations:

I. Cybersecurity risk assessments are most typically conducted at the individual organizational unit, system, or application level.
II. Cybersecurity risk assessments are not typically coordinated/managed at the enterprise level.
III. Cybersecurity risk assessments and vulnerability assessments are often conflated.
IV. The cybersecurity risk assessment requirements for many organizations are driven by compliance requirements and tend to focus on risk of noncompliance and not cybersecurity risks.
V. Cybersecurity risk assessment activities are often initiated in response to compliance requests or current events and not situational awareness of the current risk environment.
VI. Most risk assessments are qualitative, but there is increasingly a push for quantitative approaches.
VII. Quality and consistency of results is not high in the quantitative approaches we have observed.
VIII. We have observed few cybersecurity risk assessments that actually inform a business case for investing in cybersecurity as a result of the assessment.
IX. Risk assessments we have observed are typically internally focused and do not specifically account for critical infrastructure risks and other external dependencies.
X. The quality of the cybersecurity risk assessment results are highly correlated to the quality and experience of the individuals performing the assessments.
XI. There is a growing level of attention to proactive threat management and situational awareness.

We recommend that organizations

I. establish and implement a strategy for identifying, analyzing, and mitigating cybersecurity risks
II. ensure that cybersecurity risk assessments align with compliance requirements but are focused on cybersecurity risks
III. connect cybersecurity risk assessment and management activities to enterprise risk management processes
IV. take a more integrated approach to risk management that considers interdependencies with external suppliers and organizations
V. expand efforts related to intelligence gathering and analysis, proactive threat management, and establishing a risk-based situational awareness capability.
VI. ensure that cybersecurity risk assessment outputs support the business case for cybersecurity (i.e., cybersecurity risk tied to business risk)
VII. define and document the assessment process to ensure consistency of results
VIII. monitor and measure the performance of their cybersecurity risk assessments to ensure desired performance is achieved
IX. require a scientific approach to conducting quantitative risk assessments and the analysis and interpretation of their results

X. include critical infrastructure considerations in cybersecurity risk assessment and management activities

6. To what extent is cybersecurity risk incorporated into organization's overarching enterprise risk management?

In our experience, the extent of this integration varies widely:

I. For some large organizations with an enterprise risk committee (or function, possibly at the board level), cybersecurity risk is closely monitored if it has been identified as a substantial risk to the enterprise mission.
II. Organizational capabilities for managing cybersecurity risk are typically less mature than financial, reputational, or litigation-related aspects of enterprise risk management.
III. The integration of cybersecurity into enterprise risk management programs has been hampered by weaknesses in cybersecurity measurement and reporting capabilities.
IV. For other organizations, cybersecurity risk is compartmentalized and relegated to the IT organization.

We recommend that any organization that relies on any computer-based technologies as part of its operation should include and integrate cybersecurity risk into its overarching enterprise risk management processes. We also advocate a broad definition of cybersecurity risk to reflect operational risks: the inadvertent or deliberate actions of people, system and technology failures, process failures, and natural disasters and other interruptions. An operational risk management approach transcends a typical focus on technical security issues to those that broadly affect mission assurance.

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

We have been directly involved in the development and implementation of several bodies of work in the risk management space, as identified below. Our recommendation, based on these bodies of work, is that organizations should prioritize the management of risks based on the role of key assets (information, technology, facilities, people) in supporting the delivery of critical services.

- ES-C2M2
  http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20%28ES-C2M2%29%20-%20May%202012.pdf

- DHS Cyber Resilience Review (CRR)
  http://www.dhs.gov/xlibrary/assets/pso-safeguarding-and-securing-cyberspace.pdf

  http://www.ahrmm.org/ahrmm/news_and_issues/issues_and_initiatives/files/ahrmm_cyber_resilience_review_032712.pdf

- CERT Resilience Management Model (CERT-RMM)
  http://www.sei.cmu.edu/library/abstracts/reports/10tr012.cfm

- OCTAVE
  http://www.cert.org/octave/

- ASAP-SG Security Profiles
  http://www.smartgridipedia.org/index.php/ASAP-SG

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?

I. Federal regulations requiring cybersecurity reporting
   a. Federal civilian agencies
      i. FISMA
         1. § 3543. Authority and functions of the Director
         2. § 3544. Federal agency responsibilities
         3. OMB M-10-15
   b. FTC
   c. Department of Defense
      i. CJCSM 6510.01B Cyber Incident Handling Program
   d. OMB

II. Sector-specific Regulations requiring cybersecurity reporting
   a. Financial Services
      i. FFIEC Handbooks
      ii. GLBA
      iii. Basel III
      iv. Financial Crimes Enforcement Network
         1. FinCEN FIN-2011-A016 "Account Takeover Activity"
      v. Securities and Exchange Commission
         1. CF Disclosure Guidance: Topic No. 2 Cybersecurity
      vi. Energy
         1. NERC CIP
            a. CIP-008-4
         2. Nuclear Regulatory Commission
            a. Regulatory Guide 5.71 "Cybersecurity Programs for Nuclear Facilities"
      vii. Health
         1. HIPPA
         2. HITECH
      viii. State-specific regulations requiring cybersecurity reporting
         1. State breach disclosure laws
            a. 46 states, Guam, Washington, D.C., Puerto Rico, and the Virgin Islands have legislation requiring breach notification. Source: http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

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

I. People
II. Information and Data
III. Information Technology
    A. Local- and wide-area networks
    B. Business management systems
    C. Voice networks
IV. Operations Technology
    A. Local- and wide-area networks
    B. Production management systems
    C. Cyber-physical systems
V. Facilities
    A. Data centers
    B. Production facilities
    C. Command and control centers

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk? (See Appendix A for some definitions)

Based on our experience and observations:

I. Organizations generally do not formally establish and manage specific performance goals for the availability of essential services that may be disrupted by realized cybersecurity risks. Data is often gathered on cybersecurity events, but there remains a reluctance to report that information due to a desire to limit reputational and regulatory impacts. There does appear to be ad hoc performance measures that affect individuals or groups within organizations from a career or compensation perspective. We have observed this in our interactions with organizations using the methods described in our response to Question 7.

II. Service performance goals are often specified and measured in general (not for cybersecurity risk in particular) for such characteristics as
    a. service disruptions and their impact (on end user, customer, and financial outcome)
    b. service availability (including the availability of the IT infrastructure components supporting the service)
    c. service cycle/transaction time
    d. service capacity
    e. service security (if important to end users and customers)
    f. service maintenance

Our recommendation:

I. Organizations should establish and maintain (develop, document, assign owner, observe use, maintain, improve) performance goals that reflect the organization's tolerance for risk, expressed as defined risk thresholds.
II. Specify performance goals for a geographic area, an organizational entity or facility, type of service, type of asset, type of system or network, or type of application.
III. Express a performance goal as either qualitative (e.g., high, medium, low, or score for customer satisfaction) or quantitative (based on levels of loss, fines, number of customers lost, etc.).
IV. Use these performance goals as the basis for criticality assessments—continuously identifying, prioritizing, analyzing, assigning dispositions to, and mitigating risks to essential services.
V. Some examples of performance goals and measures are as follows:
    a. Service outage/downtime (percentage); some expression of impact to customer
    b. Asset (servers, databases, workstations, mobile devices) outage/downtime (percentage)
    c. Public infrastructure outage/downtime (such as power, water, telecomm/ISP)
    d. Transactions affected/lost (total, per unit time) (number and percentage)
    e. Users affected
    f. Dollars lost/dollar cost (total, per unit time) (number and percentage)
    g. Fines/legal penalties (currency)
    h. Some expression of percentage of compliance/noncompliance by asset/service type
    i. For malware infections (or some other category of incident), enact mitigating controls (take assets offline) whenever more than 200 users are affected
    j. Zero involvement of law enforcement
    k. Zero involvement of regulatory agencies
    l. Zero press/social media headlines
    m. Zero breach notifications to affected customers (for breaches that require notification); alternatively zero breaches that are significant enough to require notification
    n. Change in number of high-priority risks that exceed performance goals
    o. Percentage of essential services with (or without) an implementation risk mitigation strategy/plan
    p. Percentage of *realized* risks that exceed established performance goals (may be helpful to specifically categorize by source of realized risk that is of greatest interest such as incidents, control gaps, noncompliance, vulnerabilities, disruptions in continuity, etc.)

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?

Based on our experience and observations:

I. Regulated industries typically report to multiple regulatory bodies at the Federal, State, and in some instances international levels. This overlapping accountability and reporting is a challenge to manage and is getting more complex, in particular in the international cybersecurity arena. Though the reporting is well intentioned, its extent and complexity has created a massive challenge as well as organizational frustration and confusion. This can be a particular issue for smaller organizations that lack resources to track and manage compliance reporting.

II. Incident reporting requirements from some regulations have led organizations to carefully define what they consider an "incident," so that it is very unlikely that they will have any incidents to report.
    a. Many organizations hesitate to share incident information due to
        i. concerns about additional regulation
        ii. concerns about negative publicity
        iii. concerns about legal action
    b. Safeguards need to be in place to insulate organizations who must report from these unwanted consequences.
    c. Collected information must be used to drive improvements, not to punish.

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

I. National standards
    a. What role do national standards play in critical infrastructure cybersecurity conformity assessment?
        i. Serve as a basis for the assessment
        ii. Should drive organizations toward a deeper understanding of what practices reinforce organizational objectives, and where additional investment (time, people, money) is necessary
    b. What role should national standards play in critical infrastructure cybersecurity conformity assessment?
        i. Serve as a basis for the assessment
        ii. Support the national strategy
        iii. Serve as a roadmap for reducing gaps

II. National standards organizations
    a. What role do national standards organizations play in critical infrastructure cybersecurity conformity assessment?
        i. Develop unambiguous quantitative measures aligned to the objectives of agreed-upon standards

ii. Facilitate the use of measures that can be consistently and easily applied during assessments
iii. Set clear expectations about how reporting of assessment results should be conducted, including details about how collected data support conclusions

b. What role should national standards organizations play in critical infrastructure cybersecurity conformity assessment?
i. Create and establish incentives that promote effective assessments

III. International standards
a. What role do international standards play in critical infrastructure cybersecurity conformity assessment?
i. Serve as a basis for the assessment
ii. Serve as a checklist of practices that organizations might conduct a gap assessment against

b. What role should international standards play in critical infrastructure cybersecurity conformity assessment?
i. Inform the development of the assessment

IV. International standards organizations
a. What role should international standards organizations play in critical infrastructure cybersecurity conformity assessment?
i. Encourage adoption of national standards where they are absent
ii. Encourage quality assurance in national cybersecurity assessment development, similar to that found in ISO JTC 1/SC 27 IT Security Techniques

Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. ***What additional approaches already exist?***

The SEI's CERT Program has been directly involved in the development and implementation of several bodies of work:

- CERT-RMM
- ES-C2M2
- OCTAVE
- CERT Common Sense Guide to Mitigating Insider Threats
- CSIRT best practices and Incident Management Capability Metrics
  http://www.cert.org/csirts/
- Computer forensics guidance
  http://www.cert.org/forensics/
- CERT Secure Coding Standards for C, C++, Java, and Perl
  http://www.cert.org/secure-coding/scstandards.html
- ISO/IEC Standards
  - *Programming Languages—C, 3rd ed* (ISO/IEC 9899:2011) In particular, the following annexes, which were added to address cybersecurity concerns: C11 Annex K, "Bounds-checking interfaces," C11 Annex L, "Analyzability"
    http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=57853
  - *Information Technology—Programming Languages, Their Environments and System Software Interfaces—C Secure Coding Rules* (ISO/IEC TS 17961 Draft)
  - *Information technology -- Programming Languages -- Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use* (ISO/IEC TR 24772:2013)
    http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61457

- ASAP-SG Security Profiles http://www.smartgridipedia.org/index.php/ASAP-SG
- Department of Homeland Security Build Security In website https://buildsecurityin.us-cert.gov/bsi/home.html

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

   - Nearly all of these approaches can apply across sectors. Of the above, only ASAP-SG is clearly specific to a particular sector.

3. ***Which organizations use these approaches?***

   - Financial services, electric utilities, health care organizations, and government agencies, among others, are types of organizations using these approaches.

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

   - In our experience, the correlation between specific performance outcomes and conformance is weak. There can be great variability in performance among those organizations that have achieved a particular level of capability.

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

   - Provide standards that are outcome-based (i.e., what's being measured is the end state rather than the development or implementation of a practice.)
   - Provide implementation guidance, case studies, automated tools, and other assistance to simplify adoption.
   - Include actual performance data into the assessment and certification process.
   - To the extent that a framework includes levels or other summary scores, these should be based on specific performance targets.
   - In general, an assessment that is taken at a point in time is less useful than an approach that is instantiated as a periodic or continuous process.
   - These approaches need to move from discrete measurement to continuous measurement. We do not have a good exemplar in this space.

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

   - All of these approaches establish core requirements and methodologies that can be applied to different sectors. Requirements that vary by sector are unspecified or are allowed to be tailored during implementation to meet the needs of those specific sectors.

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

- Our experience is that voluntary programs that encourage community engagement and participation in program development yield better rates of adoption.
- Voluntary programs need to identify and implement proper incentives to encourage adoption and participation.

- Standards need to be specific to the operational goals and objectives of the sector.
    a. One approach is to have sector-specific interpretation and guidance, which may encourage sector adoption. One example can be found in ISO/IEC 90003:2004, which provides guidance for organizations in the application of ISO 9001:2000 to the acquisition, supply, development, operation, and maintenance of computer software and related support services.
    b. Alternatively, different industries have standards issued through their industry associations.
        i. The Society of Automotive Engineers publishes many standards for the automotive and aerospace industries.
        ii. During the rewrite of ISO 9000 for the year 2000 release, the Aerospace Standard (AS) group worked closely with the ISO organization. As the year 2000 revision of ISO 9000 incorporated major organizational and philosophical changes, AS9000 underwent a rewrite as well. It was released as AS9100 to the international aerospace industry at the same time as the new version of ISO 9000.
        iii. Deliverable Aerospace Software Supplement for AS9100a

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

- Provide leadership and facilitate communication within and among sector organizations
- Contribute to the development of standards and/or frameworks
    a. Ensure the standards and frameworks are appropriate for their constituents
    b. Identify sector-specific requirements and performance targets
- Encourage adoption of standards and frameworks
    a. Identify best practice in adoption
    b. Conduct outreach
    c. Reinforce the importance of the standards and frameworks
- Educate constituents about the standards and frameworks
- Use the standards and/or frameworks
- Conduct compliance evaluations
- Conduct analysis and reporting
    a. Publish sector-specific benchmark data and services
    b. Provide performance information
    c. Develop education and awareness based on analysis
- Enable information protection and anonymity
    a. Ensure that CIKR have a safe harbor in communicating about cybersecurity information by, for example, broadening the DHS/PCII information protection; this will
        i. Reduce organizational barriers to assessing compliance
        ii. Reduce suspicion of retribution for non-compliance
        iii. Contribute to building trust relationships

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

- Reduce costs and effort for CIKR in adoption
    a. Develop supporting materials for CIKR use

i. Tools
ii. Techniques and best practices
iii. Specific implementation guidance
iv. Training
v. Case studies
vi. Templates
vii. Measures and metrics

b. Provide facilitated assessments for the framework that include subject matter expertise

- Conduct traditional outreach activities
    a. Conferences
    b. Workshops
    c. Symposiums
- Consider nontraditional outreach activities
    a. Social media
- Publicize endorsement from influential leadership
    a. Sector leadership
    b. Executive Branch leadership
- Develop and publicize the value proposition of adopting the framework
    a. Use collected data from compliance assessments to refine the value proposition
- Explore sector-specific incentive programs to encourage adoption

Specific Industry Practices

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

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

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

I. Our experience is that these (and other practices) are used to varying degrees throughout the sectors.
    a. Adoption of given practices is influenced by many factors:
        i. The mission of an organization
        ii. The technology deployed in the organization

iii. Available resources
iv. Laws and regulations, and compliance obligations

II. Our recommendation is that use of these practices (and others) is most effective when they are aligned under a comprehensive risk management program that is aligned to the mission of the organization.

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

Efforts to implement and refine the above practices should be in concert with similar international efforts. The interconnectedness of organizations globally requires coordination and integration of practices to help simplify and encourage broad-based adoption.

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

The most critical activity for the secure operation of critical infrastructure is to establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the cybersecurity risks to critical infrastructure.

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

No. The extent and rigor of the use of the practices will vary.

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

Challenges will vary by organization and sector. The core challenge remains the interconnectedness of the cybersecurity risk ecosystem. Addressing that challenge requires integration, communication, and incentives to promote investment in cybersecurity risk management.

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

I. Our experience is that use of these practices varies due to many factors:
   a. Size and complexity
   b. The threat/vulnerability/risk landscape faced by an organization
   c. Compliance environment
      i. Commercial/business obligations
         1. Example: service level agreements
      ii. Some industry standards specify practices in these categories
         1. Example: the Payment Card Industry's PCI Standard
         2. Example: NERC CIP Standards
      iii. Some catalogs of practice recommend these practices
         1. Example: NIST Special Publication 800-53
   d. An organization's culture

i. Organizations may voluntarily adopt frameworks or catalogs of practice.
ii. An organizations' use of these practices (and others) changes as a result of incidents.

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

I. Our experience is that some organizations have methods of allocating resources to invest in, create, and maintain IT standards, and some do not. Use of a methodology for allocating resources is influenced by the
   a. size and complexity of the organization
   b. compliance environment
   c. organization's mission and culture

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

Our observations show that escalation processes vary across organizations; the variance is often influenced by the factors listed in the response to Question 7 on allocation of resources.

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

No answer to contribute.

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

No answer to contribute.

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

No answer to contribute.

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

I. Situational awareness
   a. Collect, analyze, alarm, present, and use cybersecurity information to form a common operating picture, commensurate with the risk to critical infrastructure and organizational objectives.
II. Information sharing/threat management/cyber intelligence management
   a. The multi-directional communication of cybersecurity information between organizations
      i. International
      ii. Government to/from industry

iii. Inter-sector
iv. Cross-sector

III. Cyber risk management
   a. The identification, assessment, and prioritization of cyber risk

IV. Vulnerability management
   a. The identification, assessment, and prioritization of vulnerabilities
      i. Vulnerabilities in process
      ii. Vulnerabilities in technology
         1. Software vulnerabilities
         2. Hardware vulnerabilities

V. Mission assurance
   a. Secure lifecycle engineering of information technology (IT) and operational technology (OT) systems and devices
      i. Secure design
      ii. Secure procurements, development, integration, and deployment
      iii. Secure operation and maintenance
      iv. Secure disposal

VI. Supply chain risk management
   a. Identifying, analyzing, and prioritizing cyber risks related to the supply chain of high-value services

VII. Performance measurement
   a. Collecting, analyzing, and reporting information about cybersecurity performance
      i. Nation-level measures
      ii. Sector-level measures
      iii. Organization-level measures

VIII. Cybersecurity program
   a. Governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure

For more information or clarification on our answers, please contact:

Summer C. Fowler
Technical Manager
412-297-6366
sfowler@cert.org

Austin Montgomery
SEI Program Development
703-908-1110
amontgom@sei.cmu.edu

Appendix A

Definitions (from DHS Risk Lexicon 2010 unless otherwise noted)

- Criticality assessment (DHS): product or process of systematically identifying, evaluating, and prioritizing based on the importance of an impact to mission(s), function(s), or continuity of operations

- Essential services (CERT-RMM®):

    - Service: a set of activities that the organization carries out in the performance of a duty or in the production of a product

    - High-value service: services on which the success of the organization's mission depends

- Risk: potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences

- Risk disposition (CERT-RMM, DHS): a statement of the organization's intention for addressing an operational risk. Typical actions include accept, avoid, transfer, or control it to an acceptable level considering associated costs and benefits of any actions taken.

- Risk management: process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken

- Risk mitigation (CERT-RMM): the act of reducing risk to an acceptable level; DHS risk mitigation: application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences

- Risk threshold: an organizationally developed type of risk parameter that is used by management to determine when a risk is in control or when it has exceeded acceptable organizational limits. Examples include availability/downtime; transactions affected/lost (total, per unit time); dollars lost (total, per unit time)

- Risk tolerance: degree to which an entity, asset, system, network, or geographic area is willing to accept risk