“Developing a Framework to Improve Critical Infrastructure Cybersecurity”

Current Risk Management Practices

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

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

Leadership concerns:

- Budget
- Shortage of IT talent
- Preparedness
- Leadership value of enterprise security agenda
- Training/Education

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

Consensus among government, industry sectors and stakeholders in determining industry wide solutions/ roadmaps for cross sector cooperation and the promotion of continuous improvement in security posture..

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?

Generally:

Enterprise Security Office within organizational structure
Creation and communication of a Security Charter to leadership and IT staff.
Enterprise Security Strategic Plan
Enterprise Security gap analysis
Enterprise security training (onboarding and annual refresher training)
Security policies align with controls (NIST SP 800-53 rev.3).
Procedures enforce policies.
Engaging leadership in security (Enterprise Security Steering Committee)

Cybersecurity

System Security Plan
Internal/ External audits
Incident Response Team/Plan

Risk Management
Penetration Testing/ Vulnerability Application Scanning
Application code review

Leadership Communication
Approval of policies prior to publication
Requirement of Enterprise security training (onboarding and annual refresher training)

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

Information Technology (IT) – Enterprise Security Office

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

Internal Audit Department

Cybersecurity risk:

Audits (SSAE16, FISCAM, Financial Statement, FFEIC and 3rd party lending clients)
Annual review of System Security Plan
Annual review of Configuration Management Plan, BCP and DR Plans
Policy review and rewrite
Procedure Update
Privacy Impact and Threshold Analysis
Incident Response team and process
Continuous Monitoring
GRC enterprise tool

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

Enterprise Security Strategic Plan shared with executive team (includes gap analysis).

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?Show citation box
NIST SP 800-30
NIST Risk Management Framework RMF
ISACA
Risk Registry (IT/security)
GRC tool for Incident Response, Audits and Continuous Monitoring
Gartner Inc.

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?

Federal requirements:

Authority to Operate (ATO) as a federal sub-contractor is recertified every 3 years.
Annual System Security Review
Annual Configuration Management Plan review
Annual Business Continuity and Disaster Recovery Plan review
Annual assessment of NIST 800-53 controls
Annual Data Sensitivity Worksheet
Annual Privacy Threshold Analysis
Annual Privacy Impact Analysis
Annual Incident Response Plan review

Incident reporting to Federal government based on Incident level. Level 1: incident at most critical level that may harm impact public long term perception of the organization, either in part or whole requires notification/reporting to federal government within 2 hours.

Commercial: Incident notification provided to client based on contractual or state of residence requirement.

Commercial: Yearly review of cyber security by all lenders and clients.

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

Employees
Data Center/ Facilities
Remote Access
Internet
IVR _ Integrated Voice Response
Telecommunications
Financial services
Access to credit bureaus, federal systems (NSLDS etc.)
Supply Management Chain
Print to Mail
U. S. Postal Service

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

Service level agreements
Availability of systems
Disaster Recovery (hot site)

Electronic Vaulting (VTL)

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?

NIST 800-53 compliant
Federal Contractor Authority to Operate
Plan of Action Milestones
Third party vendor security surveys/questionnaires
Incident Response Reports
BCP/DR overview of test results

Experience: Redundancy of reports and survey responses for clients is an issue due to the format of the exercise. Security surveys, reports and artifacts should be consistently aligned with a standard control practice and artifacts should be requested instead of adhoc responses to adoc security surveys/questionnaires. A standard format for security surveys and reports is recommended.

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

Best Practices
Benchmarking
Education
Disaster Recovery Planning

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?

“Developing a Framework to Improve Critical Infrastructure Cybersecurity”

NIST Standards (800 series)
Sarbanes- Oxley (SOX)
ISO 27002 - International Organization for Standardization
PCI- Payment Card Industry Standards
ISACA Best Practices materials

2. Which of these approaches apply across sectors?

All

3. Which organizations use these approaches?Show citation box

Federal contractors
Financial Institutions
Private and public sectors

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

Budget/Financial
Complexity
Maturity level: particularly in cloud services

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

Timeliness of updates and release to publish
Link relationships of all publications similar to a roadmap of all pieces of the controls and standards
6. How do these approaches take into account sector-specific needs?

Protection of PII
Protection of credit card information
FIPS 199

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

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

Helping to understand challenges and business cost of implementation as it relates to system classification (FIPS 199) or security controls adopted.

9. What other outreach efforts would be helpful?

Networking opportunities

Case studies of real world modeling of implementation
Collaborative committee/workgroup structure to assist in standardization, problem solving, guidance
Website where information is accessible and shared

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

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

- Separation of business from operational systems; **No**
- Use of encryption and key management; **Moderately**
- Identification and authorization of users accessing systems; **Yes**
- Asset identification and management; **Moderate to widely used**
- Monitoring and incident detection tools and capabilities; **Moderately**
- Incident handling policies and procedures; **Minimum to Moderately**
- Mission/system resiliency practices; **Not routinely applied**
- Security engineering practices; **Not routinely applied**
- Privacy and civil liberties protection; **Moderately**

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

See above, varies by component

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

N/A however existing international standards may be more mature than US standards.

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

In order:
1. Identification and authorization of users accessing systems
2. Monitoring and incident detection tools and capabilities;
3. Mission/system resiliency practices;
4. Incident handling policies and procedures
5. Privacy protection
6. Security engineering practices;
7. Asset Identification and Management

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

Separation of business from operational systems;
Asset Identification and Management
civil liberties protection
Mission/system resiliency practices

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

1. Separation of business from operational systems;
2. Monitoring and incident detection tools and capabilities

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

Standards/Best Practices
Regulatory/Mandatory
Contractual

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

Yes

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

Yes, but in general more reactive culture, risks when surfaced are addressed.

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

When monitoring inside security controls, have access to all PII data.
Perception of Big Brother watching/monitoring

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

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

Mandated/regulated
Required formal Incident Management Program

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

Minimum acceptable Identify Methodology

“Developing a Framework to Improve Critical Infrastructure Cybersecurity”