Initial Analysis of Cybersecurity Framework RFI Responses

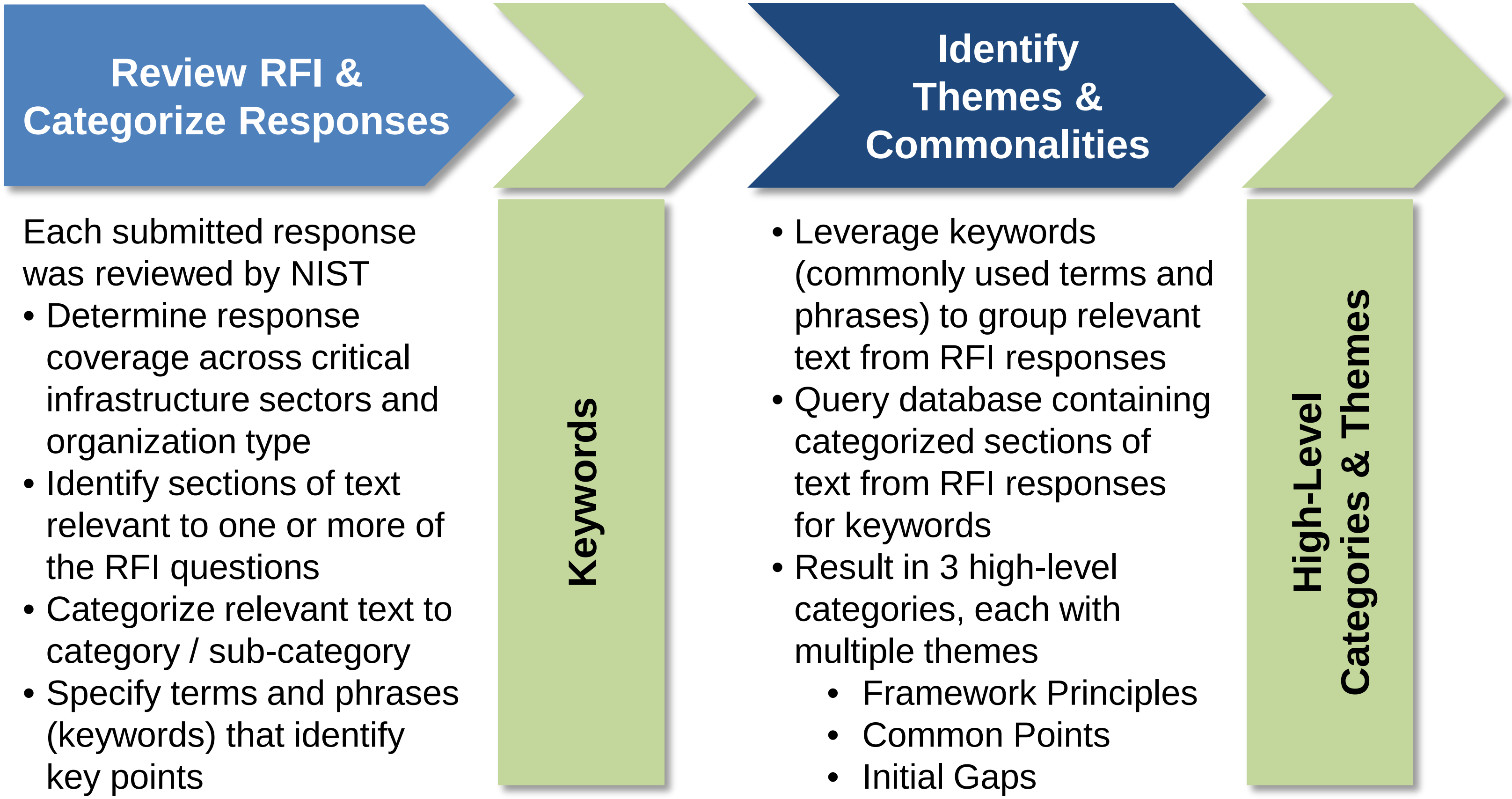
Courtesy HDR Architecture, Inc./Steve Hall © Hedrich Blessing

Agenda

- Methodology
- Framework Principles
- Common Points
- Initial Gaps
- Conformity Assessment Approaches From Other Applications

Methodology

Analysis of Framework RFI Responses Process



Review RFI & Categorize Responses

Each submitted response was reviewed by NIST

- Determine response coverage across critical infrastructure sectors and organization type
- Identify sections of text relevant to one or more of the RFI questions
- Categorize relevant text to category / sub-category
- Specify terms and phrases (keywords) that identify key points

Keywords

Identify Themes & Commonalities

- Leverage keywords (commonly used terms and phrases) to group relevant text from RFI responses
- Query database containing categorized sections of text from RFI responses for keywords
- Result in 3 high-level categories, each with multiple themes
  - Framework Principles
  - Common Points
  - Initial Gaps

High-Level Categories & Themes

Cybersecurity Framework Categories and Themes

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

Framework Principles

Framework Principles

Flexibility (35.8%)

- Apply across multiple, diverse sectors, stakeholders, and infrastructure
- Sectors, stakeholders, infrastructure differ (needs, size, resources, life cycles, etc) so solutions need to be flexible.
- Risk is dynamic with an evolving threat landscape – adaptability is key.
- Performance-based (neither prescriptive nor static).

Impact on Global Operations (64.6%)

- Global economy - global ramifications.
- Need bilateral and multilateral engagement to ensure the U.S. approach is understood.
- Commitment to global standardization process.

Framework Principles

Risk Management Approaches (81.1%)

- Should encourage risk-based approaches rather than compliance-based approaches.
- Should not be rooted in audits and audit guidelines, but good security, which leads to good compliance.
  - Compliance-based approaches discourage innovative risk management.
- Need balance between risk-appropriate security controls and contractual or regulatory requirements.

Leverage Existing Approaches, Standards, and Best Practices (33.3%)

- Should not create the need for dual standards (Framework vs current regulatory requirement).
- Leverage existing approaches and public-private partnerships.
- Provide clarity on existing choices and suitability.

Common Points

Common Points

- Senior Management Engagement (Discussed in 67%)
  - Risk Portfolios; Messaging and Management Awareness; Integrate and Incorporate Cyber Risk; Commitment of Resources
- Understanding the Threat Environment (Discussed in 75.3%)
  - Information Sharing; Timely and Actionable; Sector ISACs; Knowledge Base
- Business Risk/Risk Assessment (Discussed in 68.7%)
  - Related to Management Engagement; Relationship to Other Risks; Assessment Methods; Use of Risk Assessments
- Separation of Business and Operational Systems (Discussed in 60%)
  - Related to Baseline Security and Core Practices; Technical Mechanisms to Implement

Common Points

- Models / Levels of Maturity (Discussed in 19.7%)
  - Mechanisms to Measure; Compare; Show Progression

- Incident Response (Discussed in 27.9%)
  - Testing; Leveraging Other Lessons/Drills; Operate Under Compromise/Resiliency

- Cybersecurity Workforce (Discussed in 61.7%)
  - Training; Outreach; Awareness; Education; Role-based; Use of Tools and Technologies; Other Area Analogies, e.g., safety

Common Points

- Continue to Seek Common Points in All Tracks
  - At All Levels of Specificity
  - Drive to the Framework

- Stay Within The Executive Order Parameters

- Create a Resource Body to Draw in the Future

Initial Gaps

Initial Gaps

“*The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations.*”

- Ex, lack of standards in a particular area

For the purposes of the initial analysis, an initial gap is an area where the RFI responses were not sufficient to meet the goal of the Executive Order.

- Metrics
- Privacy and Civil Liberties
- Tools
- Dependencies
- Industry Best Practices
- Resiliency
- Critical Infrastructure Cybersecurity Nomenclature

Initial Gaps

Metrics (59.2%)

- Performance-related data used to monitor and measure the accomplishment of goals and objectives by quantifying the implementation, efficiency, and effectiveness of security measures.
  - Metrics based on mission/business objectives
  - Meaningful to provide actionable data for decision making.

Privacy and Civil Liberties (52.2%)

- 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.
  - Privacy safeguards are vital to cybersecurity
  - Based on Fair Information Practice Principles (FIPPs)

Initial Gaps

Use of Tools (55.9%)

- Tools (products, processes, personnel) allow the organization to attain a higher level of situational awareness with respect to cyber risk.
  - Facilitate implementation of security practices
  - Provide implementation guidance

Dependencies (57.2%)

- 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.
  - Identify sector/organization dependencies
  - Products and technologies that are secure by design

Initial Gaps

Industry Best Practices (65.4%)

- 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.
  - Framework to enable measurement and management of cyber risk

Resiliency (46.5%)

- 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 include self-healing networks, fail-over, hot swaps, etc.
  - Mission and system resiliency
  - Increase resiliency of nation’s critical infrastructure

Initial Gaps

Critical Infrastructure Cybersecurity Nomenclature (27.1%)

- 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.
  - Common taxonomy of cybersecurity terminology and definitions to provide a foundation to enable interoperability and scalability across industries.

Conformity Assessment approaches from other applications

Industry Led Programs Addressing Public Needs

U.S. Industry has a rich history of developing conformity assessment programs to meet our society's needs.

Conformity Assessment - Information and Confidence

- Conformity assessment systems provide critical business-business and business-consumer information

- The rigor of conformity assessment systems can provide confidence and inform risk management

    - Supporting activities include:
        - testing
        - inspection
        - supplier’s declaration
        - certification
        - accreditation

- Authorities and regulators may rely on effective conformity assessment to support their missions