Framework for Improving Critical Infrastructure Cybersecurity Version

April 16, 2018

(National Institute of Standards and Technology)

1. Introduction

- **Purpose**: To manage cybersecurity risks by providing a flexible, performance-based framework.
- **Context**: Critical infrastructure like energy, transport, and communications is highly dependent on technology, increasing exposure to cyber risks.
- **Framework Evolution**: Initiated by Executive Order 13636 in 2013 and refined under the Cybersecurity Enhancement Act of 2014.

---

2. Framework Basics

- **Structure:**
  1. **Framework Core**: High-level cybersecurity activities grouped under **Identify, Protect, Detect, Respond, Recover**.
  2. **Implementation Tiers**: Reflect the maturity of an organization's cybersecurity risk management, from **Tier 1 (Partial)** to **Tier 4 (Adaptive)**.
  3. **Profiles**: Align Framework practices with business goals, identifying gaps to develop action plans.

---

3. Framework Components

- **Functions**:
    - **Identify**: Asset management, risk assessment, and governance.
    - **Protect**: Safeguards like access control, training, and data security.
    - **Detect**: Monitoring anomalies and ensuring timely detection.
    - **Respond**: Incident analysis and mitigation.
    - **Recover**: Resilience plans and post-incident recovery.
- **Implementation Tiers**:
    - Tier 1: Ad-hoc and reactive risk management.
    - Tier 2: Risk-informed decisions with limited consistency.
    - Tier 3: Repeatable and integrated organization-wide policies.
    - Tier 4: Adaptive and evolving with advanced capabilities.
- **Profiles**:
    - Tools to compare current and desired cybersecurity states.
    - Example: **Current Profile** shows existing controls, and **Target Profile** sets future goals.

---

4. Self-Assessing Cybersecurity Risk

- **Key Practices**:
    - Use metrics to evaluate cybersecurity maturity.
    - Self-assessment identifies gaps between current and target profiles.
    - Results guide prioritization of investments and improvements.

---

5. Cyber Supply Chain Risk Management (SCRM)

- **Importance**: Addresses vulnerabilities in outsourced services or supply chain products.
- **Practices**:
  - Set clear cybersecurity requirements for vendors.
  - Use contracts to enforce these requirements.
  - Continuously monitor and validate supplier compliance.

---

6. Privacy and Civil Liberties

- **Objective**: Protect privacy while implementing cybersecurity measures.
- **Methods**:
  - Limit data collection and usage to cybersecurity purposes.
  - Incorporate privacy policies into workforce training.
  - Regularly review and address privacy implications of cybersecurity actions.

---

7. Applications of the Framework

- **Organizational Use**:
  - Helps establish or refine cybersecurity programs.
  - Facilitates communication between internal teams and external stakeholders.
- **Buying Decisions**:
  - Guides informed procurement by comparing supplier products against Target Profiles.
- **Global Relevance**: Adaptable for international use to foster standardized practices.

By Ritesh Jha