Critical Infrastructure Cybersecurity

Executive Order 13636

December 1, 2015

Erin B. Sheppard
Michael J. McGuinn
Dentons US LLP

Overview

- **Introduction of Executive Order (EO) 13636**
  - The White House released Executive Order 13636, Improving Critical Infrastructure Cybersecurity, on February 12, 2013.
  - **Underlying policy:** “It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.”

Overview

- **Introduction (Cont.)**
  - **Critical infrastructure definition:** “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”
  - **IT and ICS.** Members of each critical infrastructure depend on both Information Technology (IT) and Industrial Control Systems (ICS).

Overview

- **Introduction (Cont.)**
  - **Sixteen critical infrastructure sectors identified in Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience:**

    - Chemical
    - Commercial Facilities
    - Communications
    - Critical Manufacturing
    - Dams
    - Defense Industrial Base
    - Emergency Services
    - Energy
    - Financial Services
    - Food and Agriculture
    - Government Facilities
    - Healthcare and Public Health
    - Information Technology
    - Nuclear Reactors, Materials, and Waste
    - Transportation Systems
    - Water and Wastewater

Overview

Technology-Neutral Cybersecurity Framework

- Tasks Director of the National Institute of Standards and Technology (NIST) with leading this effort.
  - Voluntary, consensus standards
  - Industry best practices
  - Prioritized, flexible, repeatable
  - Performance-based
  - Cost-effective

Overview

Incentives for Adoption

- The Secretary of Homeland Security “shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities.”
- The EO recommends incentives to promote participation in the program.

NIST Framework

Framework Core— cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors.

Framework Implementation Tiers— mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk**.**

Framework Profile— tool to help an organization align its cybersecurity activities with its business requirements, risk tolerances, and resources.

NIST Framework

- **Framework Core**
  - Presentation of industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization.
  - Five concurrent and continuous functions: identify, protect, detect, respond, and recover.

NIST Framework Core

Identify

- Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Outcome categories include asset management, business environment, governance, risk assessment, and risk management strategy.

Protect

- Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Outcome categories include access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology.

Detect

- Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Outcome categories include anomalies and events, continuous security monitoring, and detection processes.

Respond

- Develop and implement the appropriate activities to take action regarding a detected cyber security event.
- Outcome categories include: response planning, communications, analysis, mitigation, and improvements.

Recover

- Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
- Outcome categories include: recovery planning, improvements, and communications.

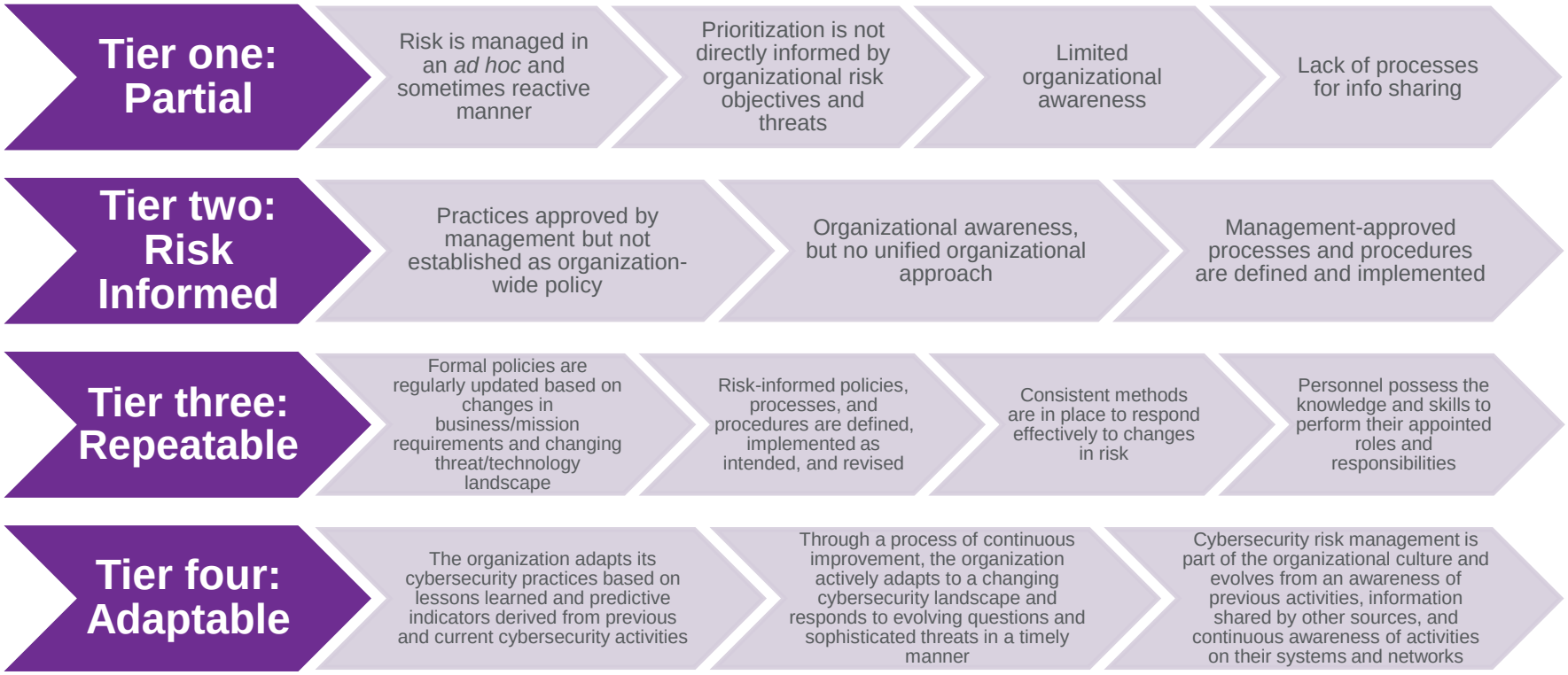
NIST Framework

- **Framework Core**
  - In Appendix A of the Framework, each of these functions corresponds to categories and subcategories of recommended behaviors or practices. In connection with each category and subcategory, the Framework suggests informative references corresponding to COBIT 5, CCS CSC, ISA, ISO/IEC, and NIST standards.
  - Mappings between Framework Core subcategories and specified sections in the informative references, however, represent general correspondence that a given reference provides the desired outcome.

NIST Framework

- **Framework Profile**
  - Represents outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices used to identify opportunities for improving cybersecurity posture by comparing a "current" profile (the "as is" state) with a "target" profile (the "to be" state).
- **Framework Implementation Tiers**
  - Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the Framework's defined characteristics (e.g., risk and threat awareness, repeatable, and adaptive).
  - Progression to higher tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective. Successful implementation of the Framework is based upon achievement of the outcomes described in the organization's target profile and not upon tier determination.

NIST Framework Implementation Tiers



NIST Framework Implementation Tiers

- **Tier 1: Partial**
  - Risk is managed in an *ad hoc* and sometimes reactive manner.
  - Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
  - Limited awareness of cybersecurity risk at the organizational level.
  - Lack of processes that enable cybersecurity information to be shared within the organization.
- **Tier 2: Risk Informed**
  - Risk management practices are approved by management but may not be established as organization-wide policy.
  - Awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established.
  - Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties.

NIST Framework Implementation Tiers

- **Tier 3: Repeatable**
  - Risk management policies are formally approved as policy and are regularly updated based on changes in business/mission requirements and a changing threat and technology landscape.
  - Risk-informed policies, processes, and procedures are defined, implemented as intended, and revised.
  - Consistent methods are in place to respond effectively to changes in risk.
  - Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.

NIST Framework Implementation Tiers

- **Tier 4: Adaptable**
  - The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.
  - Through a process of continuous improvement, the organization actively adapts to a changing cybersecurity landscape and responds to evolving questions and sophisticated threats in a timely manner.
  - Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.

NIST Framework

- **The Framework is a tool to help establish or review a cybersecurity program, focusing on the following seven steps:**
  - **(1) Prioritize.** Ascertain organizational objectives and make strategic decisions regarding cybersecurity implementation.
  - **(2) Identify** related systems and assets, regulatory requirements, and overall risk approach.
  - **(3) Develop a current profile.** Indicate which outcomes from the Framework Core are currently being achieved.
  - **(4) Conduct a risk assessment.** Discern the likelihood of a cybersecurity event and impact the event could have on the organization. Seek to incorporate emerging risks and threat/vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

NIST Framework

- **The Framework is also a tool to help establish or review a cybersecurity program, focusing on the following seven steps (Cont.):**
  - **(5) Create a target profile.** Focus on the Framework categories to describe the organization's desired cybersecurity outcomes.
  - **(6) Determine, analyze, and prioritize gaps.** Compare the current profile and target profile to determine gaps. Create a prioritized action plan to address gaps and allocate resources accordingly.
  - **(7) Implement action plan.** Determine which actions to take in regards to the gaps.

NIST Framework: Key Attributes

- **Adaptable**
- **Technology Neutral**
- **Simplifies Compliance Regimes**

NIST Framework

- **Who's Using the Framework?**
  - Private sector
    - Large Businesses:
      - Gap filling
      - Risk management
      - Common terminology and setting expectations
    - Small to medium businesses and subcontractors:
      - Standing up an enterprise cyber risk management approach
      - Explanation of system
  - Government
    - FDA in connection with cybersecurity of medical devices
    - SEC Office of Compliance Inspections and Examinations in connection with examinations of registered entities regarding cybersecurity matters
    - FTC in connection with Framework's risk assessment and mitigation approach
    - NHTSA in connection with vehicle cybersecurity

NIST Framework

- **Adoption – Intel Corporation**
  - Intel implemented the NIST Framework in Intel IT, which provides IT-related services to many Intel business units.
    - Company customized the Framework by adding more specificity to tier definitions and replacing most of the subcategories, among other modifications.
    - Framework customization and implementation required approximately 175 FTE hours – a relatively low cost due to the Framework's alignment with existing industry practices and Intel's own established risk management culture and practices.
  - Pilot implementation resulted in a set of reusable tools and best practices for utilizing the Framework to assess infrastructure risk.

NIST Framework

- **Adoption – Intel Corporation (Cont.)**
  - Take-home points from Intel:
    - Start where you are comfortable or where the risk is – scale
    - Continuous iteration with decision makers throughout the process
    - Use group collaboration mixed with individual scoring
    - Customize the Framework to your business

NIST Framework

- **Adoption – University of Pittsburgh**
  - University faces a number of cybersecurity challenges:
    - Dispersed environment: 35,000 students and 13,000 faculty/staff spread across five campuses
    - Academic freedom: “runs completely contrary to the black and white security”
    - Tremendous diversity in cybersecurity needs
  - The University’s attraction to the Framework originated with its adaptability and flexibility
    - Other frameworks were “too one size fits all,” and required “extreme hybridization” to fit with the university’s information security environment
  - Benefits of implementation:
    - Value of comparing current profiles and target profiles
    - Risk-based prioritization
    - Communication

NIST Framework

- **Adoption – University of Pittsburgh (Cont.)**
  - Take-home points from the University of Pittsburgh's adoption:
    - Use the Framework to streamline existing practices and document them
    - Focus on including necessary actors to make sure the Framework exercise identifies all relevant risks and applies at the lowest applicable levels
    - Continue to improve current and target profiles

NIST Framework

- **Adoption – Sixth Cybersecurity Framework Workshop, University of South Florida, October 29-30, 2014**
  - Benefits of the Framework:
    - Improved awareness and communication across organizations, including executive leadership
    - Demonstrated alignment with standards, guidelines, best practices, and regulatory requirements
    - Development of a common language for describing and sharing information and needs about cybersecurity and risk
    - Cost reasonable given reliance on existing best practices
  - Criticism of the Framework:
    - Many attendees did not widely tailor Framework profiles
    - Lack of practical examples or reference models through sample profiles either at a broad or sector level
    - Difficult to understand the expectations of external entities, such as regulators

NIST Framework

- **July 1, 2015 NIST Update**
  - NIST has met with officials from more than 20 nations, encouraging them to consider the Framework's approach in order to get increased global alignment
  - NIST is seeking out small-medium business interactions to better understand needs, challenges, and adoption
  - Additionally, NIST has begun a campaign to clarify and highlight how the FISMA suite of guidelines and standards (e.g., FIPS-199, SP 800-53 rev 4) can be used in concert with the Framework
    - Effort will bring together federal organizations and other users of FISMA guidance at meetings and other events
    - Intended to result in a NIST publication

NIST Framework

- **Critical Infrastructure Cyber Community Voluntary Program**
  - DHS established the Critical Infrastructure Cyber Community (C^3) Program in conjunction with the Cybersecurity Framework to increase awareness/use of the framework and support industry
    - Program voluntary
    - Focus will be initially on developing guidance for implementation
  - Program includes cybersecurity system reviews
    - No-cost, voluntary, non-technical assessments
    - Based on Framework, provides recommendations for improvement
    - Can be self-assessment or conducted with DHS assistance
  - Other DHS resources include list of recommended practices, access to updated cyber-threat information, training programs

NIST Framework

- **Sector-Specific Guidance**
  - Department of Energy (DOE)
    - Cybersecurity Framework Implementation Guide (January 2015)
      - Provides guidance to energy sector and electricity and oil and natural gas subsectors
      - Maps to the DOE Cybersecurity Capability Maturity Model (C2M2)
  - Federal Communications Commission
    - Working Group's Final Report on Cybersecurity Risk Management and Best Practices (March 2015)
      - Provides implementation guidance to help communication providers use and adapt the Framework
      - Covers broadcast, cable, wireless, satellite, and wireline segments
      - Recommends a number of voluntary mechanisms to promote cybersecurity
  - Guidance for other sectors has been issued by trade groups and commercial entities
    - Department of Defense has not issued framework guidance

NIST Framework and Existing Regulations

- **Sufficiency of Current Cybersecurity Regulations**
  - According to Section 10 of EO 13636, federal agencies "with responsibility for regulating the security of critical infrastructure shall engage in a consultative process" to "determine if current cybersecurity regulatory requirements are sufficient given current and projected risks."
  - "Section 10" reports have been submitted related to various sectors:
    - United States Coast Guard and Maritime Critical Infrastructure Cybersecurity Standards
      - Focused on utilizing voluntary standards
    - DHS Chemical Facility Anti-Terrorism Standards
      - "No significant gaps" between existing high-risk chemical facility cybersecurity policy and the NIST Framework and cybersecurity is currently addressed "in a sufficient manner"
    - Transportation Security Administration's (TSA) Approach to Voluntary Industry Adoption of the NIST Cybersecurity Framework
      - TSA has chosen to "pursue collaborative and voluntary approaches with industry"

Cyber Information Sharing Programs

- **Enhanced Cybersecurity Services (ECS) Program**
  - Voluntary information sharing program
  - Provides for sharing by DHS of cyber-threat indicators
  - Broad Applicability:
    - All 16 critical infrastructure sectors
    - Also permits approved Commercial Service Providers (CSPs) to extend their ECS customer base to all U.S.-based public and private entities
  - DHS shares sensitive and classified government-vetted cyber-threat information with qualified Commercial Service Providers (CSPs) and Operational Implementers (OIs) (i.e., qualified participating owners and operators of critical infrastructure)
    - Both CSPs and OIs subject to mandatory security requirements, validation, and accreditation
    - The CSPs in turn can use the cyber-threat information to protect their customers
    - OIs use the cyber-threat information to protect their internal networks

Cyber Information Sharing Programs

- **DHS's National Cybersecurity and Communications Integration Center (NCCIC)**
  - NCCIC's functions include serving as an interface for the "real-time" "sharing of information related to cybersecurity risks, incidents, analysis, and warnings between Federal and non-Federal entities
    - NCCIC shares information among public and private sectors to provide greater understanding of cybersecurity and communications situation awareness of vulnerabilities, intrusions, incidents, mitigation, and recovery actions
    - Center also provides a number of additional services, including technical assistance, risk management support, and incident response capabilities
  - February 13, 2015 EO mandated that the NCCIC coordinate with Information Sharing and Analysis Organizations (ISAOs)
    - Formal or informal entity or collaboration created or employed by public or private sector organizations that gather, analyze, and disseminate cyber-threat information
    - Intended to supplement existing sector-specific Information Sharing and Analysis Centers

Cyber Information Sharing Programs

- **Cybersecurity Information Sharing Act (S. 754) passed Senate in October 2015**
  - Creates liability protections for entities that monitor their information systems and share cyber-threat information with, or receive information from, the federal government through the mechanisms established in the bill
  - Privacy advocates argue that these liability protections permit government collection of citizens' data without sufficient privacy safeguards
    - CISA requires that certain personal information be removed from the information that is shared with the government
  - House passed own versions of the bill, subject to resolution in conference

Cyber Information Sharing Programs

- **2016 National Defense Authorization Act (NDAA) (Nov. 25, 2015)**
  - Provides for liability protection for cleared defense contractors and operationally critical contractors who make required reports to DOD
    - These provisions were part of 2013 and 2015 NDAAs
    - Required reports were implemented by the August 2015 DFARS update to the UCTI clause
  - "No cause of action shall lie or be maintained in any court"
    - Exception exists for willful misconduct:
      - (i) intentionally to achieve a wrongful purpose;
      - (ii) knowingly without legal or factual justification; and
      - (iii) in disregard of a known or obvious risk that is so great as to make it highly probable that the harm will outweigh the benefit.
  - Contractor impact?

Questions?

Erin B. Sheppard

(202) 496-7533

erin.sheppard@dentons.com

Michael J. McGuinn

(303) 634-4333

mike.mcguinn@dentons.com