Presidential Order 13636

Cheryl Santor, CGEIT, CISM, CISA, CISSP
Metropolitan Water District of So. CA

Presidential Order 13636

- February 12, 1013 – President Obama issues an Order to government departments to produce legislation and guidelines to protect critical infrastructure
- National Institute of Standards and Technology was mandated to produce a Cybersecurity Framework
- Congress was ordered to provide supporting legislation for some areas; Information Sharing, Education in Cybersecurity, etc.
- One year later Cybersecurity Framework issued

Order Directives – Section 1

Policy – improve the nation's cyber security due to repeated intrusions

- National and economic security of US
- Enhance security and resilience of critical infrastructure
- Encourage efficiency, innovation and prosperity while promoting safety, security, business confidentiality, privacy and civil liberties
- HOW? **Partner with owner/operators** to improve cybersecurity - information sharing and risk based standards

Order Directives Section 2

Critical Infrastructure –

- Key assets and systems (physical or virtual) vital to the US
- Incapacity or destruction of such systems and assets would debilitate security, national economic security, national public health or safety
- Any combination of those

Order Directives Section 3

Policy Coordination

- Presidential Policy Directive of Feb. 13, 2009
  - Guidance, dispute resolution and periodic in-progress reviews
  - Interagency process established in Policy Directive managed by the Organization of the National Security Council or successor

Order Directives Section 4

Cybersecurity Information Sharing

- Increase volume, timeliness, and quality of **cyber threat information shared** with private sector
- Better **protect and defend** against cyber threats
- 120 days from order, Atty General, Secty of DHS, and Director of National Intelligence issue instructions for section 12c of this order insure timely unclassified reports of cyber threats that identify specific targeted entity.
- Info sharing – classified cyber threat and tech information from Govt to eligible critical infrastrucutre companies or commercial service providers

Order Directives Section 5

Privacy and Civil Liberties Protections

- Incorporated into activities based on Fair Information Practice Principles and other policies/frameworks
- Chief Privacy Officer for Civil Rights/Liberties of DHS to assess functions and programs undertaken
- Report on how to minimize or mitigate risks due one year after this order
- Assessments shall include evaluation of activities against the Fair Information Practice Principles

Order Directives Section 6

Consultative Process

- Establish process to **coordinate improvements to the cybersecurity of critical infrastructure**
- Engage and consider advise from the Critical Infrastructure Partnership Advisory Council, Sector Coordinating Councils; critical infrastructure owner and operators; Sector-Specific Agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts

Order Directives Section 7

Baseline Framework to Reduce Cyber Risk to Critical Infrastructure

- Secretary of Commerce directed National Institute of Standards and Technology to **develop framework** to reduce cyber risks to critical infrastructure
- **Standards, methodologies, procedures, and processes that align policy, business and technological approaches to address cyber risks**
- Voluntary consensus standards and industry best practices to the fullest extent possible

Section 7 (continued)

- (b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

Order Directives Section 8

Voluntary Critical Infrastructure Cybersecurity Program

- Voluntary program to support adoption of Framework by owners/operators of critical infrastructure and other interested entities
- Coordinate with Sector Coordinating Councils to review Framework, if necessary develop implementation guidance or supplemental materials
- Agencies to report annually to President extent of participation
- Incentives designed to promote participation
- Recommendations to President
- Would legislation be required?
- Feasibility, security benefits, relative merits of security standards in acquisition planning and contract administration

Order Directives Section 9

Identification of Critical Infrastructure at Greatest Risk

- 150 days, risk based approach to identify critical infrastructure where cybersecurity incident could result in catastrophic regional/national effects on public health/safety, economic security, or national security.
- Use section 6 of this order and use expertise of Sector Specific Agencies.
- Consistent, objective criteria to identify and notify owners/operators of sectors provided basis of determination
- Review annually and provide list to President
- Owners/operators may submit relevant information for reconsideration

Order Directives Section 10

Adoption of Framework

- Regulatory agencies of critical infrastructure shall engage in review of Framework
- Determine current regulatory requirements are sufficient and projected risks
- 90 days of order submit report to President whether agency has authority to establish requirements
- Insufficient authority, propose prioritized, risk-based, efficient and coordinated actions
- 2 years agencies report on ineffective, conflicting, excessively burdensome cybersecurity requirements
- Tech assistance to develop cybersecurity workforce and programs, consultative process to mitigate cyber risks

Order Directives Section 11

Definitions

- Agencies
- Critical Infrastructure Partnership Advisory Council
- Fair Information Practice Principles
- Independent regulatory agency
- Sector Coordinating Council
- Sector-Specific Agency

Order Directives Section 12

General Provisions

- Order implemented consistent with applicable law and appropriations
- Nothing construed to give agency authority for regulating security of critical infrastructure
- Nothing construed to alter or limit any authority or responsibility of an agency under existing law
- Actions taken consistent with requirements and authorities to protect intelligence and law enforcement sources and methods

What Section of Presidential Order Meaningful to Us?

- Section 7 – the development of the NIST Cybersecurity Framework
- One year to complete
- Draft presented for comments before final version published
- Living document, undergo revisions as needed

Cybersecurity Framework

- DHS NIST conducted workshops across the country at universities to provide critical infrastructure opportunities to meet and discuss
- Draft Framework issued in October 2013 for critical infrastructure to review and make comments
- February 12, 2014 NIST Cybersecurity Framework issued
- NIST provided a Roadmap document to accompany the framework

Improving Critical Infrastructure Cybersecurity

- Policy – partnership with the owners and operators of critical infrastructure to improve sharing and develop and implement risk-based standards.
- Critical Infrastructure – systems and assets, physical or virtual, vital to the US that if destroyed or incapacitated would have debilitating impact on security, national economic security, national health or safety.

NIST Cybersecurity Framework

NIST released the first version of the Framework for Improving Critical Infrastructure on February 12, 2014.

The framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

DHS Critical Infrastructure Program

The Department of Homeland Security's CriticalInfrastructure Cyber Community C³ Voluntary Program helps align critical infrastructure owners and operators with existing resources that will assist their efforts to adopt the Cybersecurity Framework and manage their cyber risks.

Learn more about the C³ Voluntary Program by visiting: www.dhs.gov/ccubedvp.