Implementing Executive Order 13636 and Presidential Policy Directive 21

2013 – 2014

Winter Energy Conference

November 1, 2013

Bob Kolasky
Director, EO-PPD Integrated Task Force

Homeland Security

Announcement of the EO and PPD

President Obama announced new policies on cybersecurity and critical infrastructure security and resilience in February, 2013:

Executive Order 13636:
Improving Critical Infrastructure Cybersecurity

Presidential Policy Directive - 21:
Critical Infrastructure Security and Resilience

- Together, create an opportunity to effect a comprehensive national approach to cyber and physical security and resilience
- Implementation efforts designed to drive action toward ***system*** **and** ***network*** security and resiliency

EO-PPD Deliverables

120 days – **June 12, 2013**

- Publish instructions: unclassified threat information
- Report on cybersecurity incentives
- Publish procedures: expand the Enhanced Cybersecurity Services

150 Days - **July 12, 2013**

- Identify cyber-dependent critical infrastructure
- Evaluate public-private partnership models
- Expedite security clearances for private sector

240 Days – November 8, **2013**

- Develop a situational awareness capability
- Publish a successor to the National Infrastructure Protection Plan
- Publish draft voluntary Cybersecurity Framework

365 days – **February 12, 2014**

- Report on privacy and civil rights and civil liberties cybersecurity enhancement risks
- Stand up voluntary program based on finalized Cybersecurity Framework

Beyond 365 - **TBD**

- Critical Infrastructure Security and Resilience R&D Plan

Homeland Security

NIPP 2013: *PARTNERING FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE* DEVELOPMENT

NIPP Update Purpose and Challenge

Purpose:

Guide the collective effort to strengthen the security and resilience of the Nation's critical infrastructure.

Challenge:

Developing the Plan in collaborative manner, recognizing the evolving risk landscape and complex decision-making environment of diffuse authorities and responsibilities

Guiding Principles

Through partnerships, infrastructure is made more secure and resilient

Build on the successful work to date and leverage existing knowledge and structures wherever possible

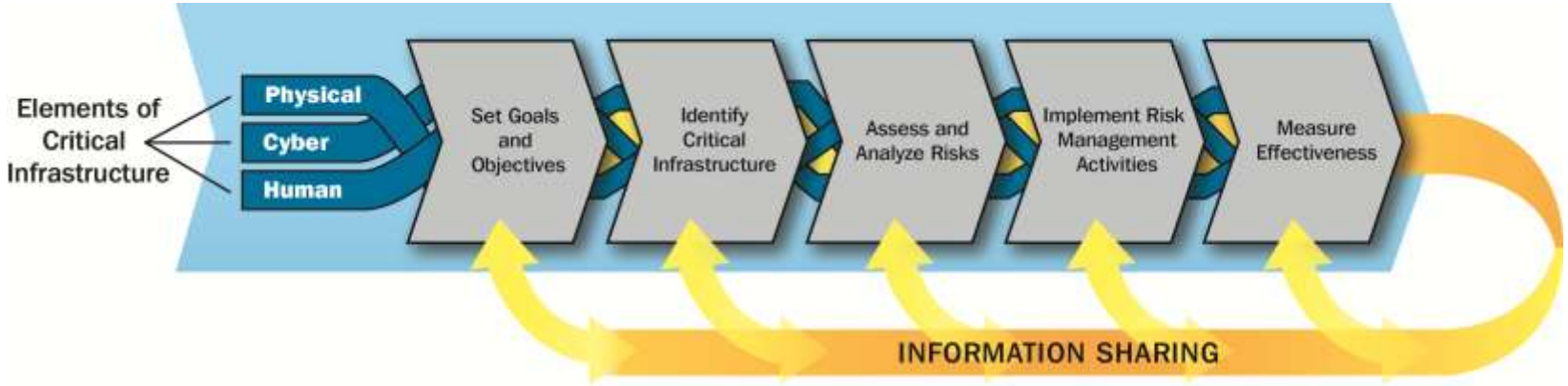
Describe the conditions that necessitate an updated approach to critical infrastructure security and resilience

Lay out the broad principles and policies that underpin this approach in the public and private sectors

Describe the national program that will implement these principles and policies to achieve shared outcomes

Evolution from 2009 NIPP

- Recognize the change in the strategic environment
  - Risk landscape
  - Infrastructure operations
  - Policy changes
- More strategic and flexible document
- Focus on actions and implementation
- Retains a focus on risk management as the foundation of national CI security and resilience; makes enhancements to framework



Goals of National Effort

Articulated Goals:

- Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities;
- Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;
- Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation, as well as effective responses to both save lives and ensure the rapid recovery of essential services;
- Efficiently share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and
- Promote learning and adaptation during and after exercises and incidents.

Changes and Evolution

- Elevates security and resilience as the primary aim of CI planning efforts
- Draws alignment between critical infrastructure risk management efforts and the National Preparedness System (across five mission areas)
- Focuses on national priorities jointly determined by public and private sectors, while limiting discussion of Federal programs
- Integrates cyber and physical security and resilience efforts into an enterprise approach to risk management
- Continues progress to support execution of the *National Plan* at both the national and community levels

Changes and Evolution, cont.

- Affirms the reality that critical infrastructure security and resilience efforts require international collaboration;
- Incorporates practical lessons learned from national program and feedback from partners
- Is mindful of the perspectives and capabilities of different partners – including Federal roles outlined in PPD 21 -- and how this affects collective efforts
- Includes a detailed Call to Action, with steps that the Federal Government will undertake – working with CI partners – to make progress toward security and resilience

THE CYBERSECURITY FRAMEWORK

Cybersecurity Framework Requirements

- Incorporate voluntary consensus standards and industry best practice
- Have the following characteristics:
  - Cross sector
  - Flexible
  - Repeatable
  - Performance-based
  - Cost effective
- Be cognizant of need for business confidentiality and individual privacy and civil liberties
- Be developed with awareness of the threat and vulnerability landscape to the Nation's cyber systems

Cybersecurity Framework Overview

- Developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk
- Supports the improvement of cybersecurity for the Nation's Critical Infrastructure using industry-known standards and best practices
- Provides a common language and mechanism for organizations to:
  1. Describe current cybersecurity posture;
  2. Describe their target state for cybersecurity;
  3. Identify and prioritize opportunities for improvement within the context of risk management;
  4. Assess progress toward the target state;
  5. Foster communications among internal and external stakeholders.
- Composed of three parts: the **Framework Core**, the **Framework Implementation Tiers**, and **Framework Profiles**

Framework Implementation Overview

An adopting organization would use the elements of the **Framework Core** as part of its risk management approach leveraging two additional Framework concepts:

Framework Implementation Tiers

- Demonstrate the implementation of the Framework functions and categories, and indicate how cybersecurity risk is managed.
- These Tiers range from Partial (Tier 0) to Adaptive (Tier 3), with each Tier building on the previous Tier.

Framework Profiles

- Conveys how an organization manages cybersecurity risk in each of the Framework functions and categories by identifying the subcategories that are implemented or planned for implementation.
- Profiles also can be used to identify the appropriate goals for an organization or for a critical infrastructure sector and to assess progress against meeting those goals.

Homeland Security

Promoting Framework Implementation

- National Performance Goals
  - Promote consideration of cybersecurity investment as a strategic decision
  - Developed in collaboration with critical infrastructure partners
- Establish a Voluntary Program
  - Leverage existing cybersecurity initiatives
  - Provide a touch point for organizations interested in Framework adoption
- Incentives
  - EO-PPD conducted study and analysis
  - Administration is consideration options
  - Proposals would help to minimize the costs of, or maximize the benefits associated with, Framework adoption

Performance Goals

National Goals

1. Critical systems and functions are identified and prioritized and cyber risk is understood as part of a risk management plan.
2. Risk-informed actions are taken to protect critical systems and functions.
3. Adverse cyber activities are detected and situational awareness of threats is maintained.
4. Resources are coordinated and applied to triage and respond to cyber events and incidents in order to minimize impacts to critical systems and functions.
5. Following a cyber incident, impacted critical systems and functions are reconstituted based on prior planning and informed by situational awareness.
6. Security and resilience are continually improved based on lessons learned consistent with risk management planning.

Cybersecurity Incentives

Eight Recommended Areas for Further Analysis:

1. Cybersecurity Insurance
2. Grants
3. Process Preference
4. Liability Limitation
5. Streamline Regulations
6. Public Recognition
7. Rate Recovery for Price Regulated Industries
8. Cybersecurity Research

"While these reports do not yet represent a final Administration policy, they do offer an initial examination of how the critical infrastructure community could be incentivized to adopt the Cybersecurity Framework as envisioned in the Executive Order. We will be making more information on these efforts available as the Framework and Program are completed."

Michael Daniel,
Special Assistant to the President and Cybersecurity Coordinator
White House Blog
August 6, 2013

Homeland Security

Voluntary Program

DHS will establish a *"Voluntary Program"* to:

- Provide critical infrastructure owners and operators with a centralized resource to access guidance on Framework adoption;
- Identify DHS and government-wide assistance around other cybersecurity risk management activities;
- Share best practices with sector and cross-sector partners.

Specifically the program will:

- Serve as a link and customer relationship manager between stakeholders and government programs to implement the Cybersecurity Framework, and provide cybersecurity resources;
- Identify and advocate for mechanisms that promote Cybersecurity Framework adoption;
- Promote understanding of the impact of the Framework via risk management.

DISCUSSION

Homeland Security