Implementing Executive Order 13636 and Presidential Policy Directive 21

DHS Science and Technology

Cyber Security Division

2013 Principal Investigators' Meeting

Jeanette Manfra, Deputy Director,
EO-PPD Integrated Task Force

September 18, 2013

Homeland
Security

Taking Action

President Obama announced two policies in February, 2013:

Executive Order 13636:
Improving Critical Infrastructure Cybersecurity

Presidential Policy Directive – 21:
Critical Infrastructure Security and Resilience

- Together, they create an opportunity to effect a comprehensive national approach
- Implementation efforts will 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 cybersecurity critical infrastructure
- Evaluate public-private partnership models
- Expedite security clearances for private sector

240 Days – **October 10, 2013**

- Develop a situational awareness capability
- Update 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

INCREASING ADOPTION OF THE CYBERSECURITY FRAMEWORK

Increasing Framework Adoption

- National Performance Goals
  - Promote consideration of cybersecurity investment as a strategic decision
  - Developed in collaborated 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 option
  - Proposals would help to minimize the costs or maximize the benefits associated with Framework adoption

National Performance Goals

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

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, and 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

Incentives

Recommended Areas:

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

How to Engage

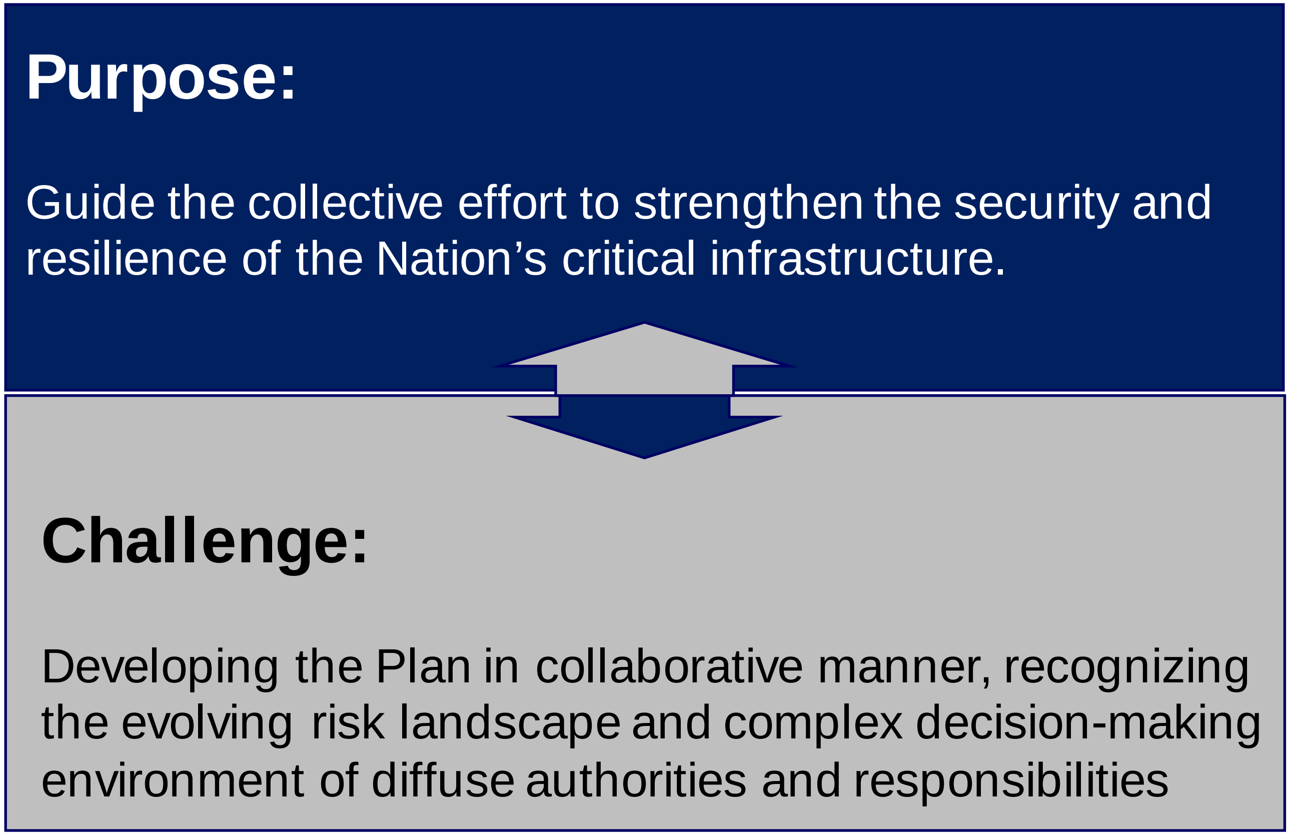
- National Infrastructure Protection Plan process
  - Review and comment on Draft Documents
    - www.dhs.gov/eo-ppd
    - Provide input through dialogue on IdeaScale -- http://eoppd.ideascale.com
    - Encourage partners to review and provide input
- PPD/EO Integrated Task Force Weekly Stakeholder Bulletin
  - Current status of activities
  - List of upcoming Open Forums, Webinars and other Engagement Opportunities
- *Contact EO-PPDTaskForce@hq.dhs.gov for more information*

UPDATING THE NATIONAL INFRASTRUCTURE PROTECTION PLAN

PPD-21 Requirements and Scope

- Directs the Secretary of Homeland Security to provide to the President…a successor to the National Infrastructure Protection Plan to address the implementation of this directive [PPD-21], the requirements of Title II of the Homeland Security Act of 2002 as amended, and alignment with the National Preparedness Goal and System required by PPD-8.
- Developed in coordination with the CI community of stakeholders.
- Must be completed within 240 days (10 Oct 2013).

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

Changes from 2009 NIPP to 2013 Plan

Structural

- Moved details of Roles and Responsibilities to Appendix
- Weaved information sharing throughout the plan, but did not include a separate section
- Retained the partnership structure approach
- Addressed cybersecurity and international issues throughout, but did not include separate sections

Content

- Evolved the Risk Management Framework and chevrons
- Demonstrated alignment to the National Preparedness System
- Continued focus on CIPAC as key decision-informing tool
- Included a new focus on actions to guide collective efforts for the near future

Milestone Schedule

- Sept 20: Comments due on Aug 30th draft
- Sept 25: Send revised redline draft and adjudication matrix to adjudication session participants
- Sept 26 & 27: Comment Adjudication sessions
- Oct 10: Deliver final draft

QUESTIONS

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland
Security