Cybersecurity Executive Order 13636
Presidential Policy Directive Policy-21

MULTI-STATE / SAADRA

Joint Regional Workshop

April 29, 2013

Homeland
Security

Agenda

- Welcome/Introductions
- EO-PPD Overview – An Integrated Approach
  - Cybersecurity Executive Order and Critical Infrastructure
  - PPD-21
- SLTT Participation
- Integrated Task Force
- Discussion

Critical Infrastructure Cyber-Physical Security Policies

President Obama issued new policies for critical infrastructure and cybsersecurity on February 12, 2013

- **Executive Order 13636:** *Improving Critical Infrastructure Cybersecurity*
- **Presidential Policy Directive** (PPD 21): *Critical Infrastructure Security and Resilience* (replaces HSPD-7)

Integrating Cyber-Physical Security

- ***Executive Order 13636*** directs the Executive Branch to**:**
    - Develop a technology-neutral voluntary cybersecurity framework
  - Promote and incentivize the adoption of cybersecurity practices
  - Increase the volume, timeliness and quality of cyber threat information sharing
  - Incorporate strong privacy and civil liberties protections
  - Explore the use of existing regulation to promote cyber security

- ***PPD-21*** directs the Executive Branch to**:**
- Develop situational awareness capability that addresses both physical and cyber aspects
    - Understand the cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan
  - Develop comprehensive research and development plan

Major Deliverables

120 days

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

150 Days

- Identify cybersecurity critical infrastructure
- Evaluate public-private partnership models

240 Days

- Develop a situational awareness capability
- Update the National Infrastructure Protection Plan
- Publish voluntary Cybersecurity Framework

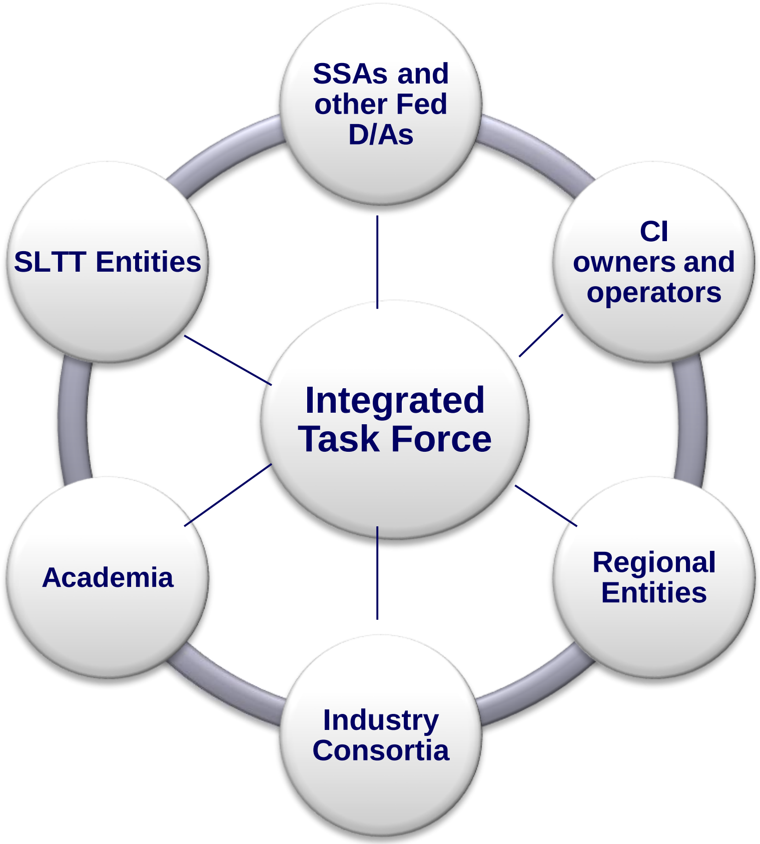
360 days

- Report on privacy and civil rights and civil liberties cybersecurity enhancement risks

Beyond 360

- Implement voluntary critical infrastructure cybersecurity program

Stakeholder Engagement Model



Guiding Principles

- Involve those responsible for critical infrastructure security and resilience.
- Reflect stakeholder views in program design and policy implementation.
- Use existing bodies and channels when possible, supplemented as needed to ensure a diversity of relevant viewpoints.

SLTT Engagement

- Kick-off conference call April 11, 2013
  - General update and methodology for future engagement
  - Information sharing

Work group participation

  - Especially Planning and Evaluation and Cyber-Dependent Infrastructure Identification Work Groups
  - Work Groups seek regular and substantive engagement from across the community

SLTT work collaboration group concept

  - Discuss options for overarching SLTT-specific input, guidance, and periodic engagement

Integrated Task Force (ITF)

- Integrates efforts for delivering EO and PPD requirements
  - Coordinates Federal Departments and Agencies
  - Conducts consultative process with government and private sector partners
- Establishes working groups
- Develops the governance process
- Regularly reports on progress

Work Groups

Working Group	Description	Deliverables
Stakeholder Engagement	Responsible for coordinating outreach to stakeholders (including critical infrastructure owner-operator communities and State, local, tribal and territorial governments) throughout the implementation process.	• Consultative process for engaging stakeholders
Cyber-Dependent Infrastructure Identification	Responsible for identifying critical infrastructure where a cybersecurity incident could result in catastrophic regional or national effects on public health or safety, economic security, or national security, as well as how best to enhance the ongoing prioritization process for all critical infrastructure.	• Identification of CI at Greatest Risk • Process of notifying CI owners of status on the list
Planning and Evaluation	Responsible for leading the effort to evaluate the existing public-private critical infrastructure partnership model and its functionality for physical and cyber security, and update the National Infrastructure Protection Plan, in coordination with the Sector Specific Agencies and other critical infrastructure partners, as appropriate.	• Evaluation of the Public-Private Partnership Model • Update the NIPP
Situational Awareness and Information Exchange	Responsible for identifying and mapping existing critical infrastructure security and resilience functional relationships across the Federal Government, identifying baseline data and systems requirements for the Federal Government, and developing a situational awareness capability for critical infrastructure. Responsible for identifying mechanisms to improve effective information sharing.	• Description of CISR Functional Relationships • Baseline System and Data for information exchange • Situational awareness capability for critical infrastructure
Incentives	Responsible for leading the study of incentives for participating in the voluntary critical infrastructure cybersecurity program and contributing to efforts to develop recommendations on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration.	• Cybersecurity voluntary program incentive reports
Framework Collaboration (with NIST)	Responsible for working with the National Institute of Standards and Technology to develop, evaluate, and disseminate the cybersecurity framework and encourage adoption by owners and operators, to include adoption of cybersecurity performance goals.	• Cybersecurity Framework • Report on applicability of Cybersecurity Framework to regulations • Performance Goals
Assessments: Privacy and Civil Rights and Civil Liberties	Responsible for coordinating with Privacy and Civil Rights and Civil Liberties representatives from across the interagency to support the accomplishment of individual Department and Agency requirements within the EO and PPD	• Engage in ongoing consultation on assessment implementation as needed by Departments and Agencies
Research and Development	Responsible for leading all research and development-related tasks in Executive Order 13636 and Presidential Policy Directive 21.	• CISR R&D Plan

Example:
Possible Topics for SLTT Input

Existing Public-Private Partnership

Purpose of the Critical Infrastructure Partnership

The purpose of the existing sector partnership model is to manage risks to critical infrastructure through active public-private collaboration and information sharing.

Discussion Questions:

- Do we have the right purpose?
- How can we expand our partnership at the state level across the full range of security and resilience issues?
- How does the partnership change/or operate differently when addressing steady state operations verses incident response?
- Where do gaps currently exist in the partnership?

Example: Possible Topics for SLTT Input

Situational Awareness and Information Exchange

- Identify and maps existing security and resilience relationships across the Federal government
- Identifies baseline data and systems requirements
- Develops a situational awareness capability in conjunction with national infrastructure centers.

Discussion

- What are the key SLTT information sharing channels and frameworks that need to be captured and represented in the analysis?
- What is the best way to engage with the SAIE WG from the SLTT level? How can SLTT provide input?
- Are any new processes or procedures going to be developed by the SLTT WG?
- When will SLTT have access to the “roadmap” document?

Example:
Possible Topics for SLTT Input

Cyber Dependent Infrastructure Identification

- Identifies critical infrastructure where a cybersecurity incident could result in catastrophic effects
- Evaluates how to best enhance ongoing prioritization process.

Current Activities

- Work with Critical Infrastructure Community to develop criteria options, via sector and cross-sector models
- Development of tasks related to notifying owner/operators

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland
Security