Implementing the Administration's Critical Infrastructure and Cybersecurity Policy


March 13, 2013

Homeland Security
Enhancing Security & Resilience

- America's national security and economic prosperity are dependent upon the operation of critical infrastructure that are increasingly at risk to the effects of cyber attacks
- The vast majority of U.S. critical infrastructure is owned and operated by private companies
- A strong partnership between government and industry is indispensible to reducing the risk to these vital systems
- We are building critical infrastructure resiliency by establishing and leveraging these partnerships
Taking Action

- In February 2013, the President announced two new policies
  1) Executive Order 13636: Improving Critical Infrastructure Cybersecurity

- Together, they create an opportunity to work together to effect a comprehensive national approach to security and risk management

- Implementation efforts will drive action toward system and network security and resiliency
Integrating Cyber-Physical Security

- Executive Order 13636: Improving Critical Infrastructure Cybersecurity 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 into every initiative to secure our critical infrastructure
  - Explore the use of existing regulation to promote cyber security

  - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
  - 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
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.
Major Deliverables

Within… …do the following:

120 days
- Publish instructions to produce and disseminate unclassified threat information
- Report on incentives for cybersecurity
- Establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors

150 days
- Identify critical infrastructure for which a cybersecurity incident will result in catastrophic regional or national effects
- Evaluate and enhance public-private partnership models
Major Deliverables (continued)

Within…  …do the following:

240 days  ▪  Develop a situational awareness capability for critical infrastructure  
         ▪  Update the National Infrastructure Protection Plan  
         ▪  Publish voluntary Cybersecurity Framework standards 

365 days  ▪  Report on privacy and civil rights and civil liberties risks associated with cybersecurity enhancements 

Beyond 365 Days  ▪  Implement a voluntary critical infrastructure cybersecurity program 

Other deliverables are required from both documents
Integrated Task Force (ITF)

- Establishes and manages working groups to accomplish the major deliverables and action items
- Integrates efforts for delivering EO and PPD requirements
- Develops and manages the governance process
- Engages relevant partners and stakeholders to develop products
  - Request for Information, Federal Register Notices, social media, meetings, presentations, workshops, interviews, etc
- Regularly reports on progress made throughout the EO and PPD implementation to partners and stakeholders
Working Groups

1) Stakeholder Engagement
2) Planning and Evaluation
3) Situational Awareness and Information Exchange
4) Cyber-Dependent Infrastructure Identification
5) Incentives
6) Research and Development
7) Framework Collaboration
8) Assessments: Privacy and Civil Rights & Civil Liberties
Principles of Engagement

- Partnership and inclusivity
- Leverage existing and ongoing work, frameworks, and venues
  - ... and identify opportunities to expand
- Strive towards broad support for EO and PPD products
- Communicate clearly
- Be transparent in product development
- Embed privacy and civil rights & civil liberties protections
- Innovate engagement opportunities
Contact Us and Participation

- Federal homeland security partners administer the working groups
- The working groups seek regular and substantive engagement from across the community
- The ITF has engagements with Federal, State, local, Tribal, Territorial, international, private sector and academic partners
  - We welcome and encourage additional engagements
- Inquires can be sent to EO-PPDTaskForce@hq.dhs.gov