

# Implementing the Administration's Critical Infrastructure and Cybersecurity Policy

Cybersecurity Executive Order and Critical Infrastructure  
Security & Resilience Presidential Policy Directive  
Integrated Task Force

*Discussion with the National Infrastructure Advisory Council*

April 8, 2013



Homeland  
Security

# The Need to Enhance Security and 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 indispensable 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 issued two new policies:
  - 1) Executive Order 13636: Improving Critical Infrastructure Cybersecurity
  - 2) Presidential Policy Directive – 21: Critical Infrastructure Security and Resilience
- 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



# Integrated 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
- ***Presidential Policy Directive-21: Critical Infrastructure Security and Resilience*** replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:
  - 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



# Major Deliverables

Within... ...do the following:

- 120 days
  - Publish instructions to produce and disseminate unclassified threat information
  - Report on incentives for cybersecurity
  - 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

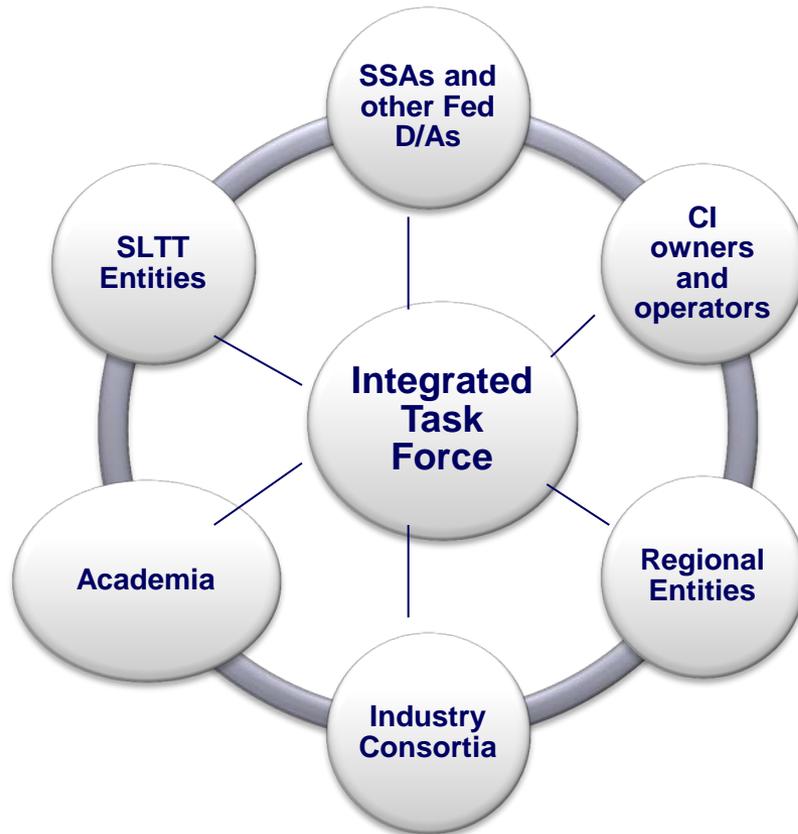
***Other deliverables are required from both documents***



**Homeland  
Security**

Unclassified

# 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.



**Homeland  
Security**

Unclassified

# Purpose of the Critical Infrastructure Partnership

- The purpose of the public-private partnership model is to manage risks to critical infrastructure for the aim of achieving critical infrastructure security and resilience.

This is achieved via:

Shared risk mitigation

Policy coordination

Information sharing

Public-private financing models

Research and development

Risk transfer

Capability building



**Homeland  
Security**

Unclassified

# Questions for Discussion – Existing Public-Private Partnership

- Do we have the right purpose?
- How do we get expanded and continued commitment at the corporate level, in the full range of security and resilience issues?
- Through that commitment, how do we ensure right person/people are participating?
  - Where do gaps currently exist?
- How can we engage the Executive Level in goal setting, and to drive toward a specific set of high-level shared goals and priorities?
- What are incentives for participating in the partnership, and what must the value proposition look like from an industry perspective?



# Incentive for Promoting Voluntary Adoption: Examples

- The 8 sources reviewed proposed the following broad categories of remunerative and coercive incentives (1-7):
  1. Expedited Security Clearance Process: a procedure to expedite the provision of security clearances to appropriate personnel employed by CI owners/operators under the framework.
  2. Grants: direct federal funding for investment in cybersecurity products and services for framework owners and operators; alternatively, tie existing grants to adoption of cybersecurity framework.
  3. Include Cybersecurity in Rate Base: rate-based recovery of cybersecurity investments in the rate base for services provided by framework owners and operators.
  4. Information Sharing: a procedure for ensuring that framework owners and operators are informed of relevant real-time cyber threat information.
  5. Insurance: promoting cybersecurity insurance through related incentives and/or federal reinsurance programs to help underwrite the development of cybersecurity insurance programs.
  6. Liability Considerations: reduced liability in exchange for improved cybersecurity or increased liability for the consequences of poor security.
  7. New Regulation/Legislation: for example, a Cyber SAFETY Act.



# Incentive Category Examples

- The 8 sources reviewed proposed the following broad categories of remunerative and coercive incentives (8-14):
  8. Prioritized Technical Assistance: ensure framework owners/operators receive prioritized cybersecurity technical assistance (e.g. ICS-CERT).
  9. Procurement Considerations: preferential consideration in the procurement process for framework owners and operators and/or requiring framework adoption by federal goods/services providers.
  10. Public Recognition: create an award for companies that adopt the framework and/or best practices.
  11. Security Disclosure: requiring public notification of disclosures to encourage owners and operators to take care to avoid breaches.
  12. Streamline Information Security Regulations: create unified compliance model for similar requirements and eliminate overlaps among existing laws (e.g. Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley).
  13. Subsidies: direct purchase of cybersecurity products and services for framework owners/operators.
  14. Tax Incentives: tax credits and/or deductions for framework owners and operators.



# Questions for Discussion – Incentives for Participation

- Are there suggestions for additional incentive categories beyond the list of 14 incentives proposed that the ITF should consider in its analysis. Is anything missing?
- Can participants enumerate incentive sub-types not already clearly included in the 14 broad incentive categories (i.e., do specific subtypes come to mind)?
- Are specific types/subtypes more likely to increase the adoption of the voluntary framework? Why/why not? Are there examples in other arenas that stand out?
- Is there particularly relevant research and/or experience on the effectiveness of the incentive categories from non-cyber contexts in the literature the ITF should consider?





# Homeland Security