NATIONAL DEFENSE INDUSTRIAL ASSOCIATION
Homeland Security Symposium

Securing Cyber Space & America's Cyber Assets: Threats, Strategies & Opportunities

September 10, 2009, Crystal Gateway Marriott, Arlington, Virginia

Securing Cyber Space & America's Cyber Assets: Threats, Strategies & Opportunities

- **IT SCC- IT Sector Baseline Sector Risk Assessment**
- **Comprehensive National Cybersecurity Initiative- Project 12**
- **National Security Telecommunications Advisory Committee: Cybersecurity Collaboration Task Force**
- **President's 60-Day Cybersecurity Policy Review**
- **National Cyber Incident Response Plan / Framework**
- **Cyber Storm III**

The IT Sector Baseline Risk Assessment (ITSRA)

- The IT Sector Baseline Risk Assessment (ITSRA) is the result of unprecedented partnership among government and industry entities who engaged in a collaborative and iterative process to assess risk to critical IT Sector functions
- Conducted in support of the National Infrastructure Protection Plan (NIPP)
  - Sharing expertise allows for the accurate execution and refinement of the risk assessment methodology
  - Sharing information enhances the prevention, protection, response, and recovery from events that impact the Sector
- The IT Sector established a working group—the Risk Assessment Committee (formerly the Critical Functions and Information Sharing Working Group)—to coordinate and lead the IT Sector's risk assessment efforts
  - Co-chaired by representatives of the Department of Homeland Security's National Cyber Security Division and IT Sector Coordinating Council
  - Participation was conducted under the auspices of the Critical Infrastructure Protection Advisory Council (CIPAC) framework

ITSRA Scope: Analyze risks to critical IT Sector functions

- **Focuses on Critical IT Sector Functions that are essential for national security, economic security, public health and safety, government services and the operation of other critical infrastructures**
- **DOES NOT focus on attacks against individual networks, systems, or information theft**
- **All-hazards risk assessment that provides an evaluation of IT Sector threats, vulnerabilities, and consequences and informs the development of strategies to mitigate sector-wide risks**
- **An initial baseline that provides the foundation for future enhancements**
- **The critical IT Sector functions are:**
  - **Produce and provide IT products and services**
  - **Provide incident management capabilities**
  - **Provide domain name resolution services**
  - **Provide identity management and associated trust support services;**
  - **Provide Internet-based content, information, and communications services**
  - **Provide Internet routing, access, and connection services**

ITSRA: A major accomplishment of the NIPP Partnership Model

- **Validated the IT Sector's functions-based risk assessment approach**
- **Affirmed the resilience and redundancy of the infrastructure**
- **Identified significant interdependencies within functions**
- **As an example: Incident management depends on the availability of the Internet Content function**
- **Although several risks were identified throughout the critical functions, it is unlikely that any of these risks would lead to the complete failure of that function**

National Cyber Security Initiative will have a dozen parts

- Trusted Internet Connection
- Intrusion detection
- Intrusion prevention
- Research and development
- Situational awareness, specifically through the National Cyber Security Center, which will coordinate information from all agencies to help secure cyber networks and systems and foster collaboration
- Cyber counter intelligence
- Classified network security
- Cyber education and training
- Implementation of information security technologies
- Deterrence strategies
- Global supply chain security
- Public/private collaboration

The President's National Security Telecommunications Advisory Committee (NSTAC)

Cybersecurity Collaboration Report

Strengthening Government and Private Sector Collaboration Through a Cyber Incident Detection, Prevention, Mitigation, and Response Capability

May 2009

The White House Releases the 60-Day Cyber Security Review

CYBERSPACE

POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure

Cyber Security Review: Near-term action plan

1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.

2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.

3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics.

4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.

5. Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.

6. Initiate a national public awareness and education campaign to promote cybersecurity.

7. Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.

8. Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement

9. In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.

10. Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

Creating effective information sharing and incident response

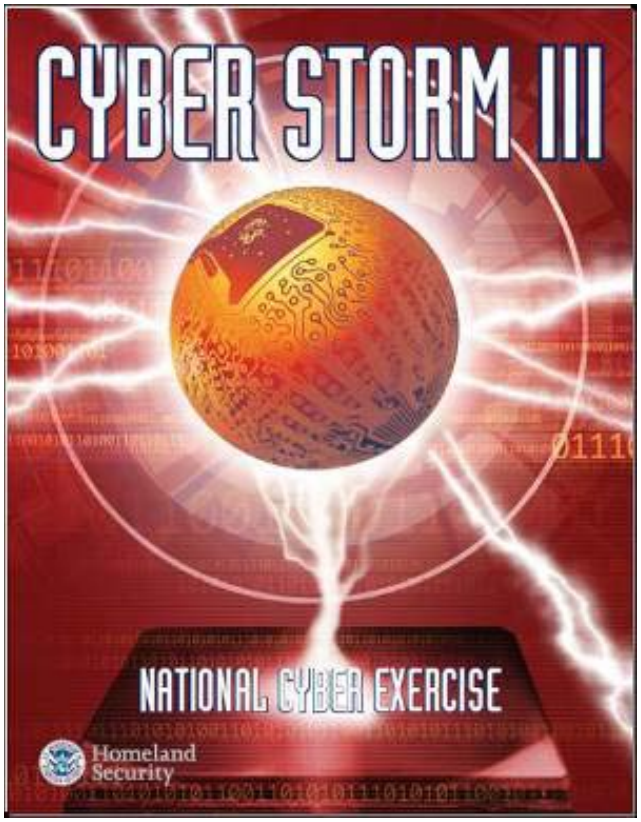
8. Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement

- Build a Framework for Incident Response
- Enhance Information Sharing To Improve Incident Response Capabilities

DHS' Cyber Storm III to test Obama's national cyber response plan

National Cyber Storm III Exercise

September, 2010



Securing Cyber Space & America's Cyber Assets: Threats, Strategies & Opportunities

Robert B. Dix, Jr.

Vice President

Government Affairs & Critical Infrastructure Protection

Juniper Networks

571-203-2687

rdix@juniper.net