Cybersecurity Policy Roadmap

16th Annual New York State Cyber Security Conference
June 5, 2013

Presented by:
Robert Mayer
USTelecom, Vice-President Industry & State Affairs
Chairman, Communications Sector Coordinating Council (CSCC) Cybersecurity Committee
<table>
<thead>
<tr>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Policy Ecosystem</td>
</tr>
<tr>
<td>The 2010 Cyber Policy Review</td>
</tr>
<tr>
<td>Public-Private Partnership Framework, Venues and Accomplishments</td>
</tr>
<tr>
<td>2013 Cybersecurity Executive Order</td>
</tr>
<tr>
<td>2013 Presidential Policy Directive 21</td>
</tr>
<tr>
<td>National Institute of Standards and Technology (NIST) Role in Cyber Framework</td>
</tr>
<tr>
<td>Key Congressional Initiatives</td>
</tr>
<tr>
<td>Discussion/Q&amp;A</td>
</tr>
</tbody>
</table>
The landscape evolves in response to the growing threat environment and associated political, economic, and social interests.
“Public-private partnerships have fostered information sharing and served as a foundation for U.S. critical infrastructure protection and cybersecurity policy for over a decade. During that time, the Federal government and the private sector have engaged in a number of forums on cybersecurity and information and communications infrastructure issues.”

The White House Cyberspace Policy Review
March, 2010
Public-Private Partnership Entities

The Public-Private Partnership Operates on Multiple Levels

STRATEGY
National Cybersecurity Framework
National Institute of Standards and Technology (NIST)

PLANNING
16 Sector Coordinating Councils
Critical Infrastructure Partnership Advisory Council (CIPAC) (PCIS)

OPERATIONS
National Infrastructure Protection Plan
Executive Order Rewrite (NIPP)
Cyberspace Policy Review
White House 60-Day Cyber Policy Review
Cyber Unified Coordination Group (UCG)
National Cyber Incident Response Plan
USCERT
US Computer Emergency Readiness Team
InfraGuard
Led by FBI Public/Private Partnership

NCICC
National Cybersecurity and Communications Integrations Center
### Recent Partnership Examples

#### The Industry Botnet Group
- The Industry Botnet Group
- National Strategy for Trusted Identities in Cyberspace (NSTIC)

#### Cyberspace Policy Review
- The Comprehensive National Cyber Security Initiative Project 12

#### The White House
- The National Cyber Incident Response Plan
- The 2012 National Sector Risk Assessment
- The Blueprint for a Secure Cyber Future
- The Sector-Specific Plan/Sector Annual Report

#### Department of Homeland Security
- National Cybersecurity Integration Command Center (NCICC)
- National Coordinating Center (Comms –ISAC)
- National Cybersecurity Awareness Month
- Cyber Storm Exercises
- National Response Framework (NRF)
- National Infrastructure Protection Plan (NIPP)
# Recent Partnership Examples

**Department of Homeland Security (Continued)**

<table>
<thead>
<tr>
<th>The Joint Coordinating Center Pilot</th>
</tr>
</thead>
<tbody>
<tr>
<td>The DIB Pilot</td>
</tr>
<tr>
<td>The National Security Information Exchange</td>
</tr>
</tbody>
</table>

| The Cross-Sector Cyber Security Working Group (CSCWG) |

| The Telecom Energy Alliance |

| The National Security Telecommunications Advisory Committee (NSTAC) |
### Recent Partnership Examples

#### Department of Commerce
- The Internet Task Force
- The Industry Botnet Group
- National Cyber Security Center for Excellence
- Cyber Security Innovations and the Internet Economy
- Smart Grid Cyber Security Working Group
- The National Vulnerability Database
- Information Security and Privacy Advisory Board

#### Department of Justice
- Internet Crime Complaint Center (IC3)
- InfraGuard
- Business Alliance Initiative
- Computer and Telecommunications Coordinator (CTC) Program
- Domestic Security Alliance Council
Recent Partnership Examples

Federal Communications Commission (FCC)

Communications Security, Reliability, and Interoperability Council I

Communications Security, Reliability, and Interoperability Council II

Network Reliability and Interoperability Council (NRIC)

Communications Security, Reliability, and Interoperability Council III

Network Security
Network Best Practices

DNSSEC Implementation

Secure BGP

U.S Anti Botnet Code of Conduct

CSRIC IV in Planning Stage
It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

White House
Executive Order 13636
February 12, 2013
The Executive Order’s impact has already been significant. Its affect on the public-private partnership will be a function of how the Order is implemented.

- New information sharing programs to provide both classified and unclassified threat and attack information to U.S. companies
- The development of a Cybersecurity Framework
- Establishment of a voluntary program to promote the adoption of the Framework
- The review of existing cybersecurity regulation
- Strong privacy and civil liberties protections based on the Fair Information Practice Principles

- Identify the functional relationships across the government related to critical infrastructure
- Work to improve the effectiveness of the existing public-private partnership with owners and operators and state, local, tribal and territorial partners in both the physical and cyber space
- Develop an efficient situational awareness capability that addresses both the physical and cyber implications of an incident
- Ensure further integration and awareness throughout the government and enables responsible info sharing of with stakeholders
- Produce a comprehensive research and development plan for critical infrastructure to guide the government’s effort to enhance and encourage market-based innovation
NIST Cybersecurity Framework

NIST has 240 days to develop a voluntary cybersecurity framework.

- Identify security standards and guidelines applicable across sectors of critical infrastructure, while identifying areas that should be addressed through future collaboration with particular sectors and standards-developing organizations
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach
- Help owners and operators of critical infrastructure identify, assess, and manage cyber risk
- Provide guidance that is technology neutral and enables critical infrastructure sectors to benefit from a competitive market for products and services
- Include guidance for measuring the performance of implementing the Cybersecurity Framework
- Include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties
Key Congressional Initiatives

Congress continues to search for ways to build support for cybersecurity legislation

- Cybersecurity Act of 2012 – S.2105 – Sponsored by former Senators Joe Lieberman (I-Conn) and Susan Collins (R-Maine). Senate failed in August 2012 to move bill past cloture.

- Cyber Intelligence Sharing and Protection Act – H.R.624 (CISPA) – Sponsored by House Intel Committee Chairman Mike Rogers and Ranking Member Dutch Ruppersberger and reintroduced and passed in the 113th Congress as H.R. 624. Bill now moves to the Senate. Sen. Jay Rockefeller, Senate Commerce Committee Chairperson, said the Senate would not approve CISPA but would instead draft an alternative bill.

Support of the Public-Private Partnership (Cont)

Discussion/Q&A

THANK YOU