U.S. Cybersecurity Policy: History, Lessons Learned & The Future

September 15, 2014

Cheri F. McGuire

Vice President, Global Government Affairs & Cybersecurity Policy

Cybersecurity – A National and Economic Security Imperative for the U.S. and India

Barack Obama
President of the United States of America

"America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet."

Narendra Modi
Prime Minister of India

"While cyber space is a source of great opportunity, cyber security has become a major concern."
(BRICS Summit, July 2014)

Cyber Threats Continue to Escalate in Scale and Impact

Ransomware

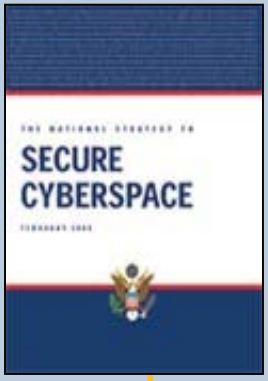
Data Breaches

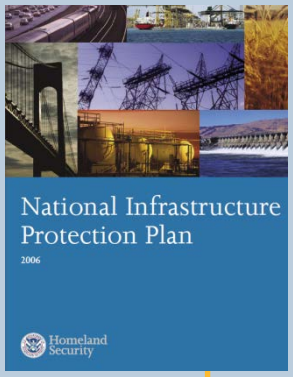
Cyberespionage
Privacy
Malicious Insider

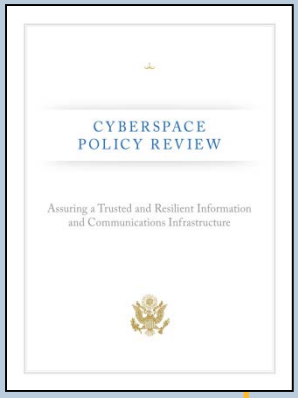
Mobile & Social

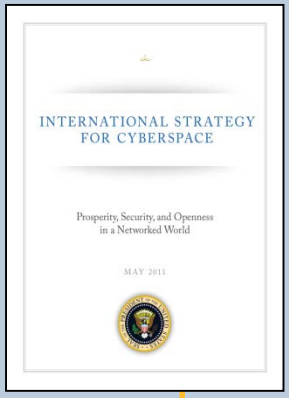
Internet of Things

History of U.S. Cyber Policy – A Decade+ of Action









Executive Order 13636:

Improving Critical Infrastructure Cybersecurity

2002..2003..2004..2005..2006..2007..2008..2009..2010..2011..2012..2013..2014…

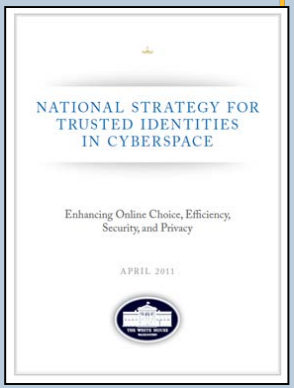
E-Gov Act of 2002

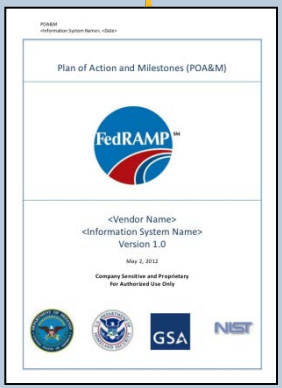
(FISMA)

HSPD-7

Critical Infrastructure Identification, Prioritization, and Protection

Comprehensive National Cybersecurity Initiative





Framework for Improving Critical Infrastructure Cybersecurity Version 1.0

NIST

Case Studies – U.S. Information Technology Sector & PPP

- NIST Collaboration
  - Cyber Security Framework, Special Publications, NVD, SCAP, Standards, etc.
- Exercises & National Cyber Incident Response Planning
- Information Sharing for Threats & Vulnerabilities
- Education & Awareness
- IT Sector-Specific Plan - Cyber, Physical, Human Risks
- Sector-wide Risk Assessment
  - Critical Function Risk Assessments
- Industry Botnet Group
- Trusted Identity Management
- International Cooperation

Lessons Learned – PPP Fundamentals for Success

- Recognizes cybersecurity is a “shared responsibility” across society
- Embraces core aspect of inclusiveness in the terms "public-private" and "partnership“
- Provides the structure, processes, and environment for trusted collaboration and repeatable consultation
- Aligns industry and government priorities, goals and objectives
- Flexible and adaptable to address the changing risk landscape
- Recognizes “one-size does not fit all” sectors and cybersecurity innovation as a priority
- Provides value for government and industry members
- Employs a mechanism for assessment of lessons learned and continuous improvement

The Future of U.S. Policy – Weighing National and Global Security and Privacy Issues

- National
  - Cyber Security Framework: Voluntary/Regulatory, Metrics
  - Congressional Action
  - Government Surveillance Reform
  - Privacy
- International
  - ICANN & Internet Governance
  - ITU & Cyber
  - Internet Balkanization
  - Trust in Foreign/U.S. ICT
  - Cyber Norms of Behavior

Summary

- The threat landscape is more complex and challenging than ever
- The U.S. has a robust history of policymaking on cyber matters
- Case studies of cyber public-private partnerships demonstrate where progress has been made – and areas for improvement
- Lessons learned – positive and negative – form the basis for core aspects of successful PPPs
- Future U.S. cyber policy is highly complex – both at the national and international levels
- The U.S. and India share national security and economic imperatives for securing cyberspace – cooperation is key

Thank you

Cheri F. McGuire

Cheri_McGuire@symantec.com

Copyright © 2014 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.