National Defense Industrial Association

Manufacturing Division Meeting

Cyber and Supply Chain Policy Issues

Eisenhower School for National Security and Resource Strategy
National Defense University
Fort McNair, Washington, DC

February 21, 2013

Jamie Barnett
Rear Admiral, USN (Retired)
Attorney at Law
Partner, Venable LLP
Co-Chair, Telecom

VENABLE® LLP

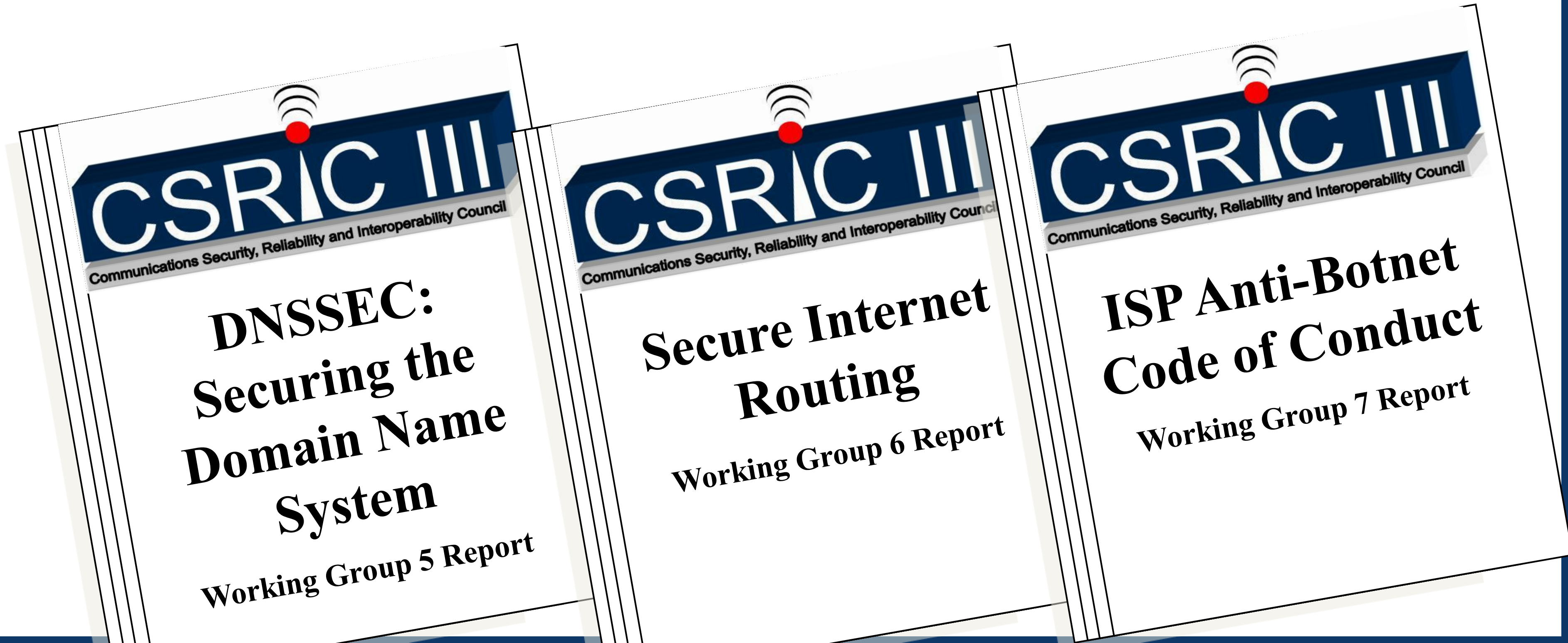
Federal Communications Commission

Communications Security, Reliability & Interoperability Council (CSRIC III)

Glen Post, CEO of CenturyLink, Chair of CSRIC III

Cybersecurity Reports

Fighting Botnets, Securing the Domain Name System, & Securing Internet Routing



CSRIC III

Communications Security, Reliability and Interoperability Council

DNSSEC: Securing the Domain Name System

Working Group 5 Report

CSRIC III

Communications Security, Reliability and Interoperability Counci

Secure Internet Routing

Working Group 6 Report

CSRIC III

Communications Security, Reliability and Interoperability Council

ISP Anti-Botnet Code of Conduct

Working Group 7 Report

FCC Communications Security, Reliability & Interoperability Council

The FCC recruited top leaders in cybersecurity to serve on CSRIC III and its working groups, for example:

Mike O'Rierdan
Chairman, MAAWG

Rodney Joffe
CTO - Neustar

Dr. Steve Crocker
CEO Shikuro &
Chair of ICANN

Danny McPherson
CSO - Verisign

Ed Amoroso
CISO – AT&T

Prof. Jen Rexford
Princeton University

Alan Paller
Research Director
SANS Institute

Rod Rasmussen
CTO – Internet Identity

Barry Greene
President – Internet
Systems Consortium

Executive Order 13636: Cyber

Information Sharing: streamline the government's sharing of crucial information (volume, quality, speed) - 120 days

Privacy: Agencies must use Fair Information Practice Principles, DHS assesses and consults with the Privacy and Civil Liberties Oversight Board (PCOB)

Michael Daniel
White House Cyber Coordinator

Standards: NIST shall lead development of voluntary Cybersecurity Framework of standards, methods, procedures for critical infrastructure owners and operators

Three Pillars of EO 13636

Cybersecurity Framework & Process

- Not performance standards per se: methods, best practices
- Consultative and participatory: NIST convenes, stakeholders decide
- Sector Coordinating Councils play big role
- 240 days to draft framework
- 1 year to publish final Cyber Framework
- 120 days DHS/DoC/Treasury recommend incentives to adopt framework
- 120 days DoD/GSA recommend incorporating security standards into acquisition/contracts
- 150 days DHS identifies critical infrastructure at "greatest risk" (where cyber incident could have catastrophic regional or national effects)

Dr. Pat Gallagher
Under Secretary of Commerce
Director of NIST

Cyber Framework Implications

- Presidential Policy Directive 21 replaces HSPD-7
- Government relies on the private sector for the input
- Voluntary, self-governed process and consensus-based
- Government will then set “performance goals”
- Companies will participate to certify that they are compliant
- So, voluntary, but incentives and comparisons may apply
- Lesson: participate in the process, monitor what is happening
- Consult your lawyer (you knew I would say it)

If you don’t have a seat at the table, you may be on the menu

Supply Chain Threats

- As significant as cybersecurity
- All critical infrastructures, but esp. communications & energy
- Cannot be transactional or foreign versus domestic approach
- Recommended: Tiered system of supply chain risk management
- Incentives and best practices for industry
- Legal authorities for effective approach may not exist

Addressing the Supply Chain Threat Symposium, September 26, 2012
Potomac Institute for Policy Studies

- Dennis Bartko, Director's Special Assistant for Cyber, National Security Agency;
- Melissa Hathaway, former Senior Director for Cyberspace, National Security Council;
- Brett Lambert, Deputy Assistant Secretary of Defense for Manufacturing and the Industrial Base.
- Jamie Barnett, Moderator

http://www.potomacinstitute.org/index.php?option=com_content&view=article&id=1282:special-event-addressing-the-supply-chain-threat-&catid=65:past-events&Itemid=94

Cyber Policy Needs

- Legislation: Incentives, limitation of liability for information-sharing
- New organs of government
- Reconciliation of existing authorities and targeted expansion of new authorities (recognizing that the first line of cyber defense is in the commercial sector)
- National Critical Infrastructure Cyber Exercise Capability
- National Cyber Doctrine

Doctrine: (n.) a body of principles that is advocated and taught

Questions

Backup slides follow

Jamie Barnett
jbarnett@venable.com
(202) 344-4695

Cybersecurity Act of 2012/S. 3414

- **Establish the National Cybersecurity Council:** an interagency chaired by DHS to conduct risk assessments
- **Create a Public-Private Partnership to Combat Cyber Threats:** industry-led groups will develop voluntary outcome-based cybersecurity practices
- **Incentivize the Adoption of Voluntary Cybersecurity Practices**
- **Improve Information Sharing While Protecting Privacy and Civil Liberties**
- **Improve the Security of the Federal Government's Networks:**
  - ✓ federal government must develop a comprehensive acquisition risk management strategy
  - ✓ Move from culture of compliance to culture of security
  - ✓ Continuous monitoring of systems
  - ✓ Red team exercises and operational testing
- **Strengthen the Cybersecurity Workforce**
- **Coordinate Cybersecurity Research and Development**

52 voted for, 46 against taking up S.3414