RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Cyber Legislation & Policy Developments 2014

SESSION ID: LAW-Fo2

Michael A. Aisenberg, Esq.

Chair, ABA Information Security Committee Policy Task Force
ABA Section on Science & Technology Law

Principal Cyber Analyst/Counsel, The MITRE Corporation
McLean, Virginia

AMERICAN BAR ASSOCIATION
Defending Liberty
Pursuing Justice

Objectives

- **Understand the procedural context into which new Cyber security legislation and policy initiatives are being introduced**
- **Describe the major existing statutes constituting the U.S. legal framework for Cyber security policy**
- **Catalog the major legislative Cyber security proposals introduced in this Congress**
  - **may have further action,**
  - **become law, or**
  - **influence other national policy initiatives**
    - **Executive Orders, Regulations and Departmental guidance, state law or informal policy.**

Background

- February 2013: Executive Order 13636 released from White House
- AND House Intelligence Committee-authored bill H.R. 624, “CISPA” passed Committee and went on to eventual House passage (April, 2013) with high expectations
- In this Congress, fewer than 30 bills in total have been sent to the President for signature.
- 12 Senate bills, resolution have been introduced with “Cyber” in caption or purpose
- 22 House bills, resolutions and amendments introduced with “Cyber” in caption or purpose, 11 passed House, 2 Public Laws
- “IT” appears in Title or purpose of 101 bills, 5 passed House, 5 passed Senate, only 2 “IT” Public Laws (both Appropriations)
- February 2014: First Public Release of the Cyber Security Framework pursuant to the 2013 Executive Order released February 13.

Context-Existing Federal "Cyber" Law-I

- The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984
  - prohibits various attacks on federal computer systems and on those used by banks and in interstate and foreign commerce.
- The Electronic Communications Privacy Act of 1986 (ECPA)
  - prohibits unauthorized electronic eavesdropping.
- The Computer Security Act of 1987
  - Gave NIST responsibility for developing security standards for USG computer systems,
    - except the national security systems that are used for defense and intelligence missions (CNSS)
    - gave responsibility to the Secretary of Commerce for promulgating electronic security standards.
- The Paperwork Reduction Act of 1995
  - Gave OMB responsibility for developing Federal agency cybersecurity policies.
- The Clinger-Cohen Act of 1996
  - agency heads responsible for ensuring the adequacy of agency information-security policies & procedures, established the CIO position in agencies
- The Homeland Security Act of 2002 (HSA)
  - gave the Department of Homeland Security (DHS) some cybersecurity responsibilities in addition to those implied by its general responsibilities for homeland security and critical infrastructure, through National Program and Policies Directorate and "Cybersecurity Division".

Context--Existing Federal “Cyber” Law-II

- The Cyber Security Research and Development Act
  - also enacted in 2002, established research responsibilities in cybersecurity for the National Science Foundation (NSF) and NIST.
- The E-Government Act of 2002
  - serves as the primary legislative vehicle to guide federal IT management and initiatives to make information and services available online, and includes various cybersecurity requirements.
- The Federal Information Security Management Act of 2002 (FISMA)
  - clarified and strengthened NIST and agency cybersecurity responsibilities, established a central federal incident center, and made OMB, rather than the Secretary of Commerce, responsible for promulgating federal cybersecurity standards.

Cyber Legislation in 113th Congress-I

- House bills with Floor or Committee Action

- HR 624: House version of Intelligence ISE: Cyber Information Sharing ("CISPA")**: Passed house 4/18/2013.**
  - CRS Summary/link to text: http://thomas.loc.gov/cgi-bin/bdquery/D?d113:1:./temp/~bdiAhN:@@@D&summ2=m&|/home/LegislativeData.php|
- H.R. 933 (Commerce/Justice/NASA Continuing Appropriation) passed House March 6, passed Senate March 11, ***Public Law 113-6.*** (China SCRM Provision).
  - Section 516 Prohibits Commerce, Justice, NASA and National Academies from using appropriated funds to acquire ICT electronics (hardware AND software) produced in China without conducting FBI-type vulnerability/threat assessment.
  - CRS Summary: http://thomas.loc.gov/cgi-bin/bdquery/D?d113:1:./temp/~bdEWGK:@@@D&summ2=m&|/home/LegislativeData.php|
- **HR 3696 National Cyber Security & Critical Infrastructure Act** of 2014 (McCaul-Tx.) Bipartisan comprehensive cyber security bill marked up and **passed House Homeland Security Cte 2/ 5/2014**.
- HR 1163: ("FISMA II) among other things requires continuous security monitoring for federal agency data
- HR 756: "Cybersecurity Enhancement Act"
- HR 967: "Advancing America's Network & Information Technology R&D Act"
  - CQ article on the three bills: http://www.cq.com/doc/news-4257169

Cyber Legislation in 113th Congress-II

- Major Senate Cyber bills
- S. 1353: "Cybersecurity Act of 2013" Rockefeller/Thune truncated version of S. 21 "3 Committee" consensus bill
  - Reported from Senate Commerce Committee 24 July 2013.
- 3 Bills addressing "Data Breach"
  - S.1193 : Data Security and Breach Notification Act of 2013
    Sponsor: Sen Toomey, Pat [PA] (introduced 6/20/2013) Cosponsors (7)
    Committees: Senate Commerce, Science, and Transportation
    Latest Major Action: 6/20/2013 Referred to Senate committee. Status: Read twice and referred to the Committee on Commerce, Science, and Transportation.
  - S.1897 : Personal Data Privacy and Security Act of 2014
    Sponsor: Sen Leahy, Patrick J. [VT] (introduced 1/8/2014) Cosponsors (5)
    Committees: Senate Judiciary
    Latest Major Action: 1/8/2014 Referred to Senate committee. Status: Read twice and referred to the Committee on the Judiciary.
  - S.1976 : Data Security and Breach Notification Act of 2014—revises S. 1193
    Sponsor: Sen Rockefeller, John D., IV [WV] (introduced 1/30/2014) Cosponsors (3)
    Committees: Senate Commerce, Science, and Transportation
    Latest Major Action: 1/30/2014 Referred to Senate committee. Status: Read twice and referred to the Committee on Commerce, Science, and Transportation.
- Plus one intended to plug hole in Health care Exchanges
  - S.1902 : Health Exchange Security and Transparency Act of 2014
    Sponsor: Sen Barrasso, John [WY] (introduced 1/9/2014) Cosponsors (25)
    Committees: Senate Health, Education, Labor, and Pensions
    Latest Major Action: 1/9/2014 Referred to Senate committee. Status: Read twice and referred to the Committee on Health, Education, Labor, and Pensions.

Key Issues Addressed by Active "Comprehensive" Cyber Bills

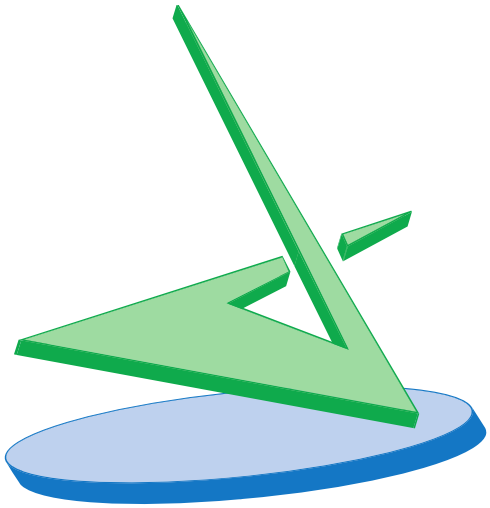
- HR 3696 **Key Provisions**
  - Would codify in law the National Cybersecurity and Communications Integration Center, a DHS agency that promotes real-time cyberthreat information sharing across critical infrastructure sectors.
  - establish an equal partnership between industry and DHS, and ensures that DHS properly recognizes industry-led organizations (ISACs, Sector Councils) to expedite critical infrastructure protection and incident response.
  - prohibit DHS from obtaining new cybersecurity regulatory authority
  - Codify and strengthen the National Infrastructure Protection Plan, a public-private partnership framework that has been supported by the private sector since 2003;
  - Codify the Cyber Incident Response Teams to provide timely technical assistance, crisis management and actionable recommendations on cyberthreats to critical infrastructure owners and operators on a voluntary basis;
  - Ensure that the National Cybersecurity Incident Response Plan is updated regularly and coordinated with federal, state, local and private-sector stakeholders;
  - Codify DHS operational information security activities to ensure the resiliency of all federal civilian information systems and networks; and
  - Amend the SAFETY Act to so private organizations can submit voluntarily their cybersecurity procedures to the government to gain additional liability protections in the event of a qualifying cyber-incident.

Key Issues Addressed by Active "Comprehensive" Cyber Bills

- **S. 1353 Key Provisions**
- **Cyber Standards:** Permits NIST to facilitate and support the development of a voluntary, industry-led set of standards and procedures to reduce cyber risks to critical infrastructure. (c.f.-EO Framework). Prohibits the Director from prescribing a specific solution or requiring that products or services be designed or manufactured in a particular manner. Prohibits information provided to NIST for purposes of developing cyber risk standards from being used by federal, state, tribal, or local agencies to regulate the activity of any entity.
- **R&D:** Directs OSTP to develop, and update triennially, a federal cybersecurity research and development plan to meet cybersecurity objectives, including how to guarantee individual privacy, verify third-party software and hardware, address insider threats, determine the origin of messages transmitted over the Internet, and protect information stored using cloud computing or transmitted through wireless services. Directs NSF to support cybersecurity research and to review cybersecurity test beds. Requires OSTP to coordinate with other ongoing federal research initiatives. Amends the Cyber Security Research and Development Act to permit NSF research and development grants for 5 areas. Directs specified agencies under the High-Performance Computing Act of 1991 to support research leading to a scientific foundation for the field of cybersecurity.
- **Workforce & Education:** Directs the Department of Commerce, NSF, and the Department of Homeland Security (DHS) to support competitions and challenges to recruit individuals to perform information infrastructure security duties or to stimulate cybersecurity innovations. Directs NSF to continue the Federal Cyber Scholarship-for-Service program. Requires NSF and DHS to enter arrangements with the National Academy of Sciences to conduct a comprehensive study of government, academic, and private-sector education, accreditation, training, and certification programs for the development of professionals in information infrastructure and cybersecurity.
- **Public Awareness**: Directs NIST to continue coordinating a national cybersecurity awareness and preparedness campaign to increase public awareness and understanding of cybersecurity risks, support education programs, and evaluate workforce needs. Requires NIST to develop a strategic plan to guide federal activities in support of such campaign.

Thank You !

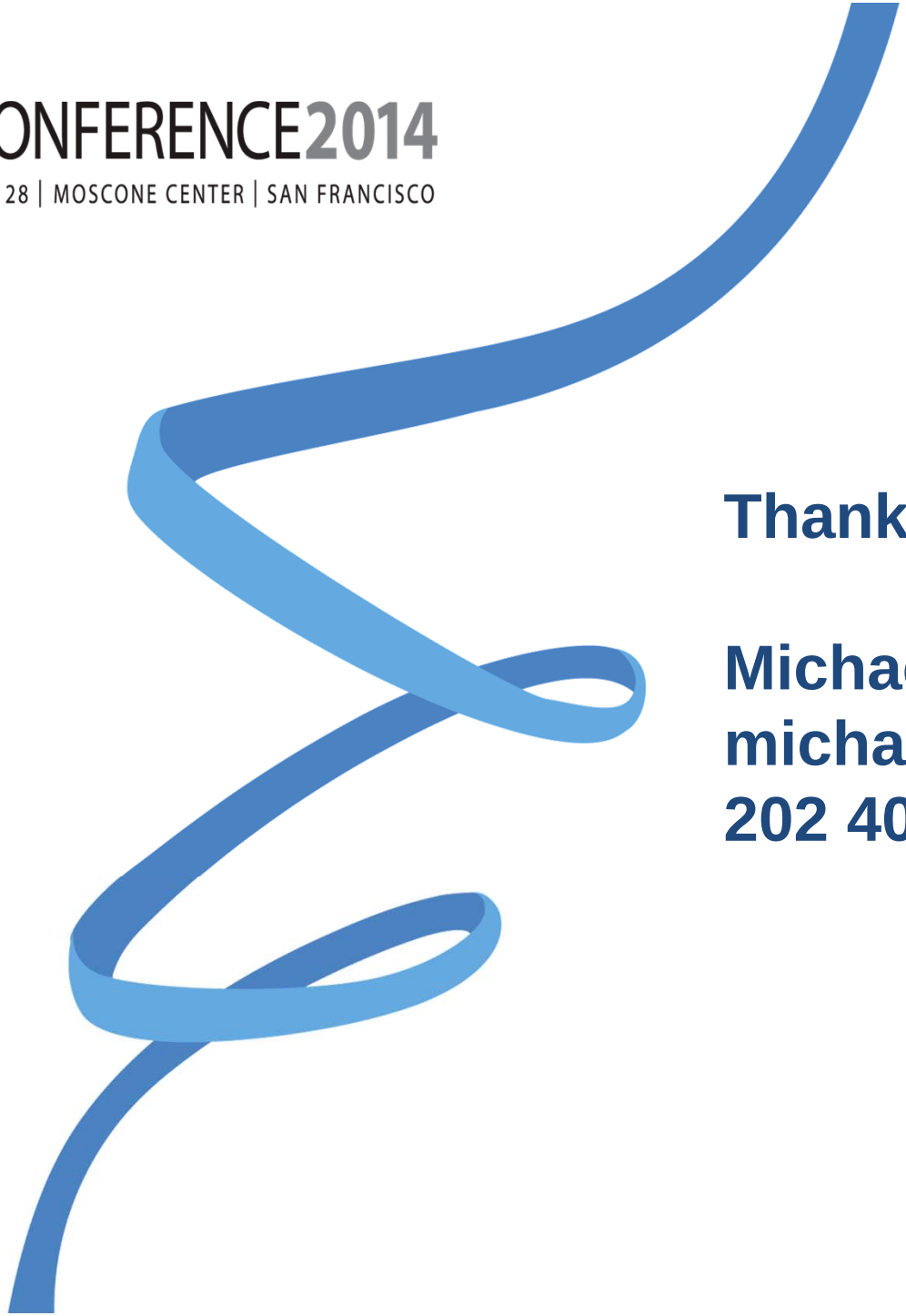
- Questions ?



ABA SECTION OF
SCIENCE & TECHNOLOGY LAW

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Thank You !

Michael Aisenberg
michael@cybsec.us
202 409-1509