Cybersecurity:
The U.S. Legislative Agenda
Part II

Melissa E. Hathaway

Senior Advisor, Belfer Center for Science and International Affairs

Harvard University

November 2010

HARVARD Kennedy School

BELFER CENTER for Science and International Affairs

US Legislative Agenda

- Over 50 pieces of legislation relating to Cybersecurity have been introduced in the 111th Congress addressing, among other things:
  - Organizational Responsibilities
  - Compliance and Accountability
  - Data Accountability, Personal Data Privacy, Data Breach Handling and Identity Theft
  - Cybersecurity Education, Research and Development and Grants
  - Critical Electric Infrastructure Protection and Vulnerability Analysis
  - International Cooperation and Addressing Cybercrime
  - Procurement, Acquisition and Supply Chain Integrity

Senate Leadership Letter

- Senator Reid's letter to POTUS expresses a desire to collaborate on comprehensive cyber legislation. It was countersigned by: Sen. Leahy, Sen. Levin, Sen Kerry, Sen Rockefeller, Sen. Lieberman, and Sen. Feinstein. This suggests that the following list of bills are in play for a comprehensive piece of legislation:

  - Cybersecurity Act of 2009 (S. 773). Introduced by Senator Rockefeller and Senator Snowe
  - National Asset Act of 2010 (S. 3480). Introduced by Senator Lieberman, Senator Collins, and Senator Carper.
  - Personal Data Privacy and Security Act of 2009. (S. 1490 and S. 139). Introduced by Senator Leahy.
  - National Cyber Infrastructure Protection Act of 2010 (S. 3538). Introduced by Senator Bond and Senator Hatch.
  - International Cyberspace and Cybersecurity Coordination Act of 2010 (S. 3193). Introduced by Senator Kerry.
  - National Defense Authorization Act of 2011 (S. 3454). Introduced by Senator Levin.
  - Data Security and Breach Notification Act (S. 3742). Introduced by Senator Rockefeller and Senator Pryor.
  - Combating Online Infringement and Counterfeits Act (S. 3804). Introduced by Senator Leahy and Senator Alexander.

GAO Pressure Increases

- GAO reports highlight that not enough is being done:
  - March 2010 report on Progress Made and Challenges to Date with Coordinating (and executing) CNCI.
  - June 2010 report on Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development
  - June 2010 report on Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats
  - October 2010 report on Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed
  - GAO is currently conducting a review of the USG's approach to international cybersecurity. The inquiry includes questioning of whether a Cybersecurity Ambassador is needed.

Other Key Events

- Senate Select Committee on Intelligence (SSCI) established a Task Force on Cybersecurity (12-9-09). It was chaired by Senator Whitehouse (D-RI) with two sub-chairs: Sen Snowe (R-ME) and Sen Mikulski (D-MD). It convened in January 2010 and completed its work in July 2010. It delivered a classified report to the committee on 1 July and noted publicly "America's vulnerability to massive cyber crime, global cyber espionage, and cyber attacks has emerged as one of the most urgent national security problems facing our country today and our nation is at risk. Cyber hackers' offensive capabilities are outpacing our network defenses. Protecting our national security and our very way of life is a bipartisan issue that needs an immediate bipartisan solution. Congress must act now." This report further underscores the bipartisan consensus within the Congress to confront this urgent threat and enact comprehensive cybersecurity legislation

- 2 September 2010: National Institute of Standards and Technology released a three volume report: Guidelines for Smart Grid Cyber Security. In 2007, Congress assigned NIST with responsibility to develop a framework for secure, interoperable smart grid technology, and the new NIST report was produced by a 450-member working group, going through several public drafts along the way.

Key Events: Law

- **Intelligence Authorization Act (H.R. 2071) Becomes Public Law 111-259 on 7 October 2010**: It strengthens and enhances America's intelligence capabilities, and improves congressional oversight of our intelligence agencies. It provides our intelligence community with the tools and resources to train more officers, expand language skills, strengthen cybersecurity efforts, and more effectively prevent the spread of weapons of mass destruction.

  - Requires a report from the DNI to the intelligence and foreign relations committees assessing the threat to national security presented by efforts of foreign countries to acquire sensitive equipment and technology and the degree to which U.S. export controls are adequate to defeat such efforts

  - Requires reports to Congress from the DNI and the National Counterintelligence Executive regarding global supply chain vulnerabilities

  - Directs the President to notify Congress of each cybersecurity program that includes specified documentation, including the program's legal justification and any approved concept for program operation. Requires the head of any federal department or agency for which a notification is submitted to report on such program to Congress and the President. Directs the DHS Inspector General and the IC Inspector General to submit a joint report to Congress and the President on the sharing of cyber threat information. Terminates the requirements and authorities of this section at the end of 2012.

  - Establishes the Cybersecurity Task Force to: (1) conduct a study of existing tools and provisions of law used by the IC and law enforcement agencies to protect the cybersecurity of the United States; and (2) report to Congress initially and annually thereafter for two years on improvements of such capabilities. Terminates the Task Force 60 days after its last report.

Legislation to Watch

- **National Defense Authorization Act of 2011 (H.R. 5136 and S. 3454)**. These two bills introduce key initiatives for cybersecurity, including: Requiring a report to the Congress on the cyber warfare policy of DOD, including legal, strategy, and doctrinal issues; Authorizing funds for cybersecurity demonstration projects using commercial technology; Requiring DoD to develop a tailored acquisition process for cyberspace; Requiring DoD to develop a strategy to address software vulnerabilities and supply chain risk mitigation strategies; Requiring implementation continuous monitoring of computer networks (FISMA Reform); Requirng annual damage assessments and annual net assessments (reports) comparing US and other country cyber capabilities; Limiting use of funds for National Cyber Range; and Requiring establishment of a National Cyber Coordinator within EOP.

- **The Grid Reliability and Infrastructure Defense Act (H.R. 5026)**. The bill would amend the Federal Power Act and direct the Federal Energy Regulatory Commission to protect the electric transmission and distribution grid from vulnerabilities. In addition to providing authority to address immediate threats, the GRID Act would also give FERC authority to mandate measures to protect against system "vulnerabilities" if it finds that the North American Electricity Reliability Corp. ("NERC) standards are insufficient. If passed, the legislation will provide a security framework for the Smart Grid.

New Bills Since May 2010 Analysis

- H.R. 5136 National Defense Authorization Act Amendment (Section 1701). Introduced on 21 May 2010.

- S. 3454 National Defense Authorization Act for FY 2011. Introduced by Sen. Levin (D-MI) on 4 June 2010 in Senate Armed Services Committee.

- S. 3480 Protecting Cyberspace as a National Asset Act of 2010. Introduced by Sen. Lieberman (I-CT) and Sen. Collins (R-ME) on 6 June 2010 in the Senate Committee on Homeland Security and Government Affairs.

- H.R. 5548 Protecting Cybersapce as a National Asset Act of 2010. Introduced by Rep. Harmon (D-CA) on 16 June 2010 in the House Committee on Oversight and Government Reform.

- S. 3538 National Cyber Infrastructure Protection Act of 2010. Introduced by Sen. Bond (R-MO) on 24 June 2010 in the Senate Select Committee on Intelligence.

- S. 3611 (formerly S. 1494) Intelligence Authorization Act for FY 2010. Introduced by Sen. Feinstein (D-CA) on 19 July 2010 in the Senate Select Committee for Intelligence. It passed the Senate on 5 August 2010.

New Bills Since May 2010 Analysis

- H.R. 5966 Cybersecurity Enhancement Act of 2010. Introduced by Rep. Murphy (D-PA) on 29 July 2010 in the House Permanent Select Committee on Intelligence.

- S. 3579 Data Security Act of 2010. Introduced by Sen. Carper (D-DE) and Sen Bennett (R-UT) on 21 July 2010 in the Senate Committee on Banking, Housing, and Urban Affairs.

- S. 3579 Data Security Act of 2010. Introduced by Sen. Carper (D-DE) and Sen Bennett (R-UT) on 21 July 2010 in the Senate Committee on Banking, Housing, and Urban Affairs.

- S. 3742 Data Security and Breach Notification Act. Introduced by Sen. Rockefeller (D-WV) and Sen. Pryor (D-AR) on 5 August 2010 in the Senate Commerce Committee.

- S. 3804 Combating Online Infringement and Counterfeits Act. Introduced by Sen. Leahy (D-VT) and Sen. Alexander (R-TN) on 20 September 2010 and has been referred to the Committee on the Judiciary.

- H.R. 6351 Strengthening Cybersecurity for Critical Infrastructure Act. Introduced by Rep. Langevin (D-RI) on 29 September 2010 and has been referred to the Committee on Homeland Security and the Committee on Oversight and Government Reform for consideration.

- H.R. 6423 Homeland Security Cyber and Physical Infrastructure Protect Act of 2010. Introduced by Rep. Thompson (D-MS) on 17 November 2010 and has been referred to the House Committee on Homeland Security and the House Committee on Oversight and Government Reform for consideration.

Analysis of Bills

	Organizational Responsibility	Compliance & Accountability	Data Accountability & Identity Theft	Education, Awareness and R&D	Critical Infrastructure & Electric-Power	International Cooperation & Cyber Crime	Procurement, Acquisition, Supply Chain Integrity
S. 139 -- The Data Breach Notification Act	XX	XX	XX				
H.R. 2221 -- Data Accountability and Trust Act	XX	XX	XX				
S. 773. -- Cybersecurity Act of 2009	XX	XX		XX	XX	XX	XX
S.778 -- Office of National Cybersecurity Advisor.	XX						
H.R. 266 -- Cybersecurity Education Act of 2009				XX			
H.R. 2020 -- Networking and Information Technology Research and Development Act of 2009.		XX			XX		
S. 920 -- Information Technology Investment Oversight Enhancement and Waste Act of 2009	XX	XX					
S. 921 -- United States Information and Communications Enhancement Act of 2009	XX	XX					XX
H.R. 4900 -- Federal Information Security Amendments Act of 2010	XX	XX	XX				XX
S. 946 -- Critical Electric Infrastructure Protection Act of 2009				XX	XX		XX
H.R. 2195 -- Electric Grid Vulnerability Analysis				XX	XX		XX
H.R. 2165 -- Bulk Power System Protection Act of 2009	XX				XX		
H.R. 5026 -- The Grid Reliability and Infrastructure Defense Act	XX				XX		
S. 1438 -- International Cybercrime Reporting and Cooperation Act	XX			XX		XX	
H.R. 4692 -- International Cybercrime Reporting and Cooperation Act	XX					XX	
S. 3193 -- International Cyberspace and Cybersecurity Coordination Act of 2010	XX					XX	

	Organizational Responsibility	Compliance & Accountability	Data Accountability & Identity Theft	Education, Awareness and R&D	Critical Infrastructure & Electric-Power	International Cooperation & Cyber Crime	Procurement, Acquisition, Supply Chain Integrity
S. 1490 (S. 495) -- Personal Data Privacy and Security Act.	XX		XX				
H.R. 3498 -- Internet Freedom Preservation Act of 2009			XX	XX			
H.R. 1292 -- To Amend title I of the Omnibus Crime Control and Safe Streets Act of 1968			XX			XX	
H.R. 2271 -- Global Online Freedom Act of 2009				XX		XX	
S 1070 -- Establish Small Business Information Security Task Force to Address INFOSEC Concerns	XX			XX			
S. 1047 -- SAFE Internet Act				XX		XX	
H.R. 4061 -- Cybersecurity Enhancement Act of 2009	XX			XX			
H.R. 1910 -- Chief Technology Officer Act of 2009	XX			XX			
S. 1475 -- Reduce Iranian Cyber Suppression Act.						XX	XX
H.R. 3284 -- Reduce Iranian Cyber Suppression Act						XX	XX
S. 1494 -- Intelligence Authorization Act for Fiscal Year 2010	XX						
H.R. 4098 -- Secure Federal File Sharing Act			XX				
H.R. 1319 -- Informed P2P User Act.			XX				
H.R. 122 -- Protecting the Privacy of Social Security Numbers Act of 2009		XX	XX				
S. 141 -- Protecting the Privacy of Social Security Numbers Act		XX	XX				
H.R. 50 -- Social Security Identity Theft Prevention Act		XX	XX				
H.R. 123 -- Credit Agencies Identity Theft Responsibilities Act of 2009		XX	XX				

	Organizational Responsibility	Compliance & Accountability	Data Accountability & Identity Theft	Education, Awareness and R&D	Critical Infrastructure & Electric-Power	International Cooperation & Cyber Crime	Procurement, Acquisition, Supply Chain Integrity
H.R. 133 -- Identity Theft Notification Act of 2009		XX	XX				
H.R. 2417 -- Identity Protection Act of 2009		XX	XX				
H.R. 2472 --Social Security Number Fraud and Identity Theft Prevention Act		XX	XX				
S. 30 -- Truth in Caller ID Act of 2009			XX				
H.R. 1110 -- The PHONE Act of 2009			XX				
H.R. 3817 -- Investor Protection Act of 2009	XX		XX	XX			
H.R. 1776 -- Consumers Right to Know Act				XX	XX		
H.R. 5247 -- Executive Cyberspace Authorities Act of 2010	XX	XX		XX			
H.R. 5136 -- National Defense Authorization Act of 2011	XX	XX		XX			XX
S. 3484 -- National Defense Authorization Act of 2011	XX			XX			XX
S. 3480 -- Protecting Cyberspace as a National Asset Act of 2010	XX	XX			XX		XX
H.R. 5548 -- Protecting Cyberspace as a National Asset Act of 2010	XX	XX			XX		XX
S. 3538 -- National Cyberspace Infrastructure Protection Act	XX			XX			XX
S. 3611 -- Intelligence Authorization Act of FY10 (formerly S. 1494)	XX	XX					
H.R. 5966 -- Cybersecurity Enhancement Act of 2010				XX			
S. 3579 -- Data Security Act of 2010		XX	XX				
S. 3742 -- Data Security and Breach Notification Act		XX	XX				
S. 3804 - Combating Online Infringement and Counterfeits Act			XX			XX	XX
H.R, 6351 -- Strengthening Cybersecurity for Critical Infrastructure Act	XX	XX			XX		
H.R, 6423 -- Homeland Security Cyber and Physical Infrastructure Protection Act of 2010	XX	XX			XX		

Proposed Focus Areas for the 112th Congress

- What is the national security threat to industry?
- Should the Economic Espionage Act of 1996 be reviewed due to the significant quantity of information being stolen or illegally copied from our companies that has reached a qualitatively unacceptable threshold?
- Should we consider a new statute that criminalizes the creation and distribution of malware?
- Is it time to review the need for an industrial policy that helps our companies maintain global competitiveness and continue to grow jobs in the United States by repatriating their foreign source income?
- Would strengthening the regulatory oversight of the SEC, FCC, FERC, or FTC help or hurt the situation? How are these regulatory bodies using their current authorities to address the situation? Are these regulatory bodies working together?
- As we continue to invest in digitizing our infrastructures and everything behind it, what are the attendant investment requirements needed to assure its integrity and security?
- Should Internet Service Providers assume more responsibility for providing enhanced security services to their customers and report all security incidents to an appropriate government entity?
- What are other countries doing to strengthen their information and communications infrastructures and posture?

Recommendations

- The 112th Congress should champion transparency and discourse on cybersecurity by holding public briefings and hearings encouraging a dialogue about what is really needed to address the problem comprehensively.

- Enlist and incentivize the private sector to understand and address the vulnerabilities and innovate our way through a solution.

- Develop and implement a broad-based awareness and education campaign for the U.S. population and other like-minded nations.