

# Cybersecurity: The U.S. Legislative Agenda

Melissa E. Hathaway  
Senior Advisor

Belfer Center for Science and International Affairs  
Harvard University  
14 May 2010



HARVARD Kennedy School

**BELFER CENTER**

for Science and International Affairs



# US Legislative Agenda

- ❖ Over 35 pieces of legislation have been introduced in 111th Congress, addressing Cybersecurity, 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



# Other Key Activities

- ❖ Senate Select Committee on Intelligence (SSCI) established a Task Force on Cybersecurity (12-9-09). It is 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 is expected to complete its work by June 2010.
- ❖ Committee on Armed Services has established a new subcommittee on Terrorism and Unconventional Threats which is covering cybersecurity. It is chaired by Rep. Sanchez (D-CA).
- ❖ Former Congressman Bob Livingston sent appeal letter to Speaker Pelosi and Minority Leader Boehner (23 November 2009) recommending the establishment of a Special Committee for Cybersecurity (similar to Y2K).
- ❖ 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.
- ❖ House Committee on Foreign Relations has become quite active given the recent Google/PRC incident.
- ❖ Senate Commerce Committee held a public hearing regarding their legislation on 23 February 2010.
- ❖ GAO March 2010 report on Progress Made and Challenges to Date with Coordinating (and executing) CNCI.
- ❖ House Committee on Oversight and Government Reform held an open hearing on FISMA II legislation on 24 March 2010.



# Legislation to Watch

- ❖ Data Breach Legislation (S. 139). It will normalize the 46 State Data breach laws into one national umbrella. It may be expanded to include more than Personal Identifiable Information (PII). One issue with this bill is that it would consolidate all reporting to the US Secret Service, which is not helpful for broader information sharing with industry or across government.
- ❖ Data Accountability and Trust Act (H.R. 2221). It was voted out of the House of Representatives in early December 2009. It requires the ISPs to make victims aware of infection if seeing breach across network. I believe the Comcast Denver, CO pilot program could be anticipatory market movement associated with this bill (to better understand costs). It will be interesting to see if this is extended to those services who may also be able to determine if there is anomalous behavior on the broader backbone. As you may know, Germany just passed a law requiring their ISPs to inform their citizens/consumers if they have been infected.
- ❖ International Cybercrime Reporting and Cooperation Act (S. 1438 and H.R. 4692): This bill was introduced by Sen Gillibrand, and co-sponsored by Sen Hatch, which will give it strength in the Judiciary Committee. The bill requires the President to produce an annual report to Congress providing an assessment of every country's level of ICT utilization and development; assesses how each country's legal, law enforcement and judicial systems address cyber crime and protect commerce and consumers. This bill met discord from software and hardware companies and their associated lobbying organizations (e.g., BSA, Tech America) because there is language that there will be imposed sanctions on countries who have demonstrated 5 years of "bad behavior". This Bill and any hearing around it will certainly draw attention to the recent Google/PRC debacle. It has a sister bill in the House of Representatives, H.R. 4692 mirrors the areas of focus. \*\*Note Sen Kerry and Sen. Gillibrand have also introduced S. 3193 (International Cyberspace and Cybersecurity Coordination Act of 2010) to authorize the creation of a senior coordinator at the State Department, with the rank and status of Ambassador at Large.



# Legislation to Watch

- ❖ Cybersecurity Enhancement Act (H.R. 4061). It passed the House of Representatives in February (2/2/10). In addition to providing additional responsibility to NIST, it creates an office for a national coordinator for the networking and information technology research and development program to improve cybersecurity research and development and coordination between the federal government, academia and private sector. The NITRD office (within the Office of Science and Technology Policy) already coordinates all of the Cyber R&D which for this year is well over \$4B. While this is non-controversial piece of legislation because it supports R&D efforts focused on identity management technologies and usability, authentication methods, and privacy, its not clear how the new office will interact with the current OSTP responsibilities.
- ❖ FISMA II (S. 921): It updates FISMA I from compliance driven (check-list) to measures that are performance based. It uses the State Department's Risk Scoring tool which measures its systems on a continuous basis against known vulnerabilities and offers meaningful feedback in the form of actionable remediation techniques to the operators and high level feedback to senior managers to ensure accountability is one example that could serve as a model for the rest of government. It also affords the department and agency chief information security officer the focus and attention it need and deserve. Finally, it is possible that FISMA II will address procurement reform.
- ❖ Intelligence Authorization Act (H.R. 2071): 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. Contains multiple Congressionally Directed Actions for CNCI.



# Legislation to Watch

- ❖ Cybersecurity Act of 2009 (S. 773). : The bill combines audits, industry-developed and government-backed standards, increased information-sharing, and other mechanisms to bolster private sector cybersecurity. It establishes a Cybersecurity Advisory Panel (Presidential Level) and a National Clearinghouse for information sharing. Additionally, it extends the Scholarship for Service program (increases to 1000 scholarships) and increases the National Science Foundation's budget for R&D.
- ❖ The Grid Reliability and Infrastructure Defense Act (H.R. 5026). The bill amends the Federal Power Act and directs 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.
- ❖ Energy and Water Appropriations Act 2010 (Law). It appropriates additional funds for Cybersecurity: \$46.5 million for energy delivery cyber security, an increase of \$34.5 million from 2009, to develop secure grid technologies as cyber attacks increase worldwide and the grid becomes increasingly network-connected. It also establishes a National Cyber Center for the grid.



# 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				



	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. 50 -- Social Security Identity Theft Prevention Act		XX	XX				
H.R. 123 -- Credit Agencies Identity Theft Responsibilities Act of 2009		XX	XX				
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			



# Description of Bills



## US Legislative Agenda: Overview of Bills

- ❖ S. 139 -- The Data Breach Notification Act. Introduced by Sen. Feinstein (D-CA), Senate Judiciary Committee; Voted out of committee, early December 2009.
  - ❖ Establishes requirement for notification, including method, content, and timing. Mostly focused on PII.
- ❖ H.R. 2221 -- Data Accountability and Trust Act. Introduced by Rep. Rush (D-IL) in Energy and Commerce Committee; Voted out of House of Representatives, 8 December 2009.
  - ❖ Requires the FTC to promulgate regulations requiring each person engaged in interstate commerce that owns or possesses electronic data containing personal information to establish security policies and procedures.
  - ❖ Establishes requirement for CISO; reasonable security measures; requires ISPs to make victim aware if seeing breach across network; consumer protection mechanisms (credit monitoring for victim)
  - ❖ Note Comcast Denver, CO pilot program could be anticipatory market movement associated with this bill



## US Legislative Agenda: Overview of Bills

- ❖ S. 773. Cybersecurity Act of 2009. Introduced by Sen. Rockefeller (D-WVA) and Sen. Snowe (R-ME). Voted out of the Commerce, Science, and Transportation Committee March 2010.
  - ❖ Designed to address full spectrum of cybersecurity issues, from national vulnerabilities to offensive programs. It includes NIST performance and compliance; training and certification-workforce development; Cyber education e.g., K-12; increases R&D at National Science Foundation, and establishes an Cyber Advisory Board as well as an Information Sharing Clearinghouse.
  - ❖ Has been heavily influenced by industry and has broad support as it moves into mark-up.
- ❖ S.778. Office of National Cybersecurity Advisor. Introduced by Sen. Rockefeller (D-WVA) and Sen. Snowe (R-ME) in the Commerce, Science, and Transportation Committee.
  - ❖ Creates a cybersecurity advisor position and places it under the President (AP)



## US Legislative Agenda: Overview of Bills

- ❖ H.R. 266 -- Cybersecurity Education Act of 2009. Introduced by Representative Jackson-Lee (D-TX) in the Science and Technology Committee.
  - ❖ Directs DHS to establish, in conjunction with NSF, a program to award grants to institutions of higher education for: (1) cybersecurity professional development programs; (2) associate degree programs in cybersecurity; and (3) the purchase of equipment to provide training in cybersecurity for either professional development or degree programs.
- ❖ H.R. 2020 -- Networking and Information Technology Research and Development Act of 2009. Introduced by Rep. Gordon (D-TN). Voted out of House of Representatives 5/09 and received in Senate
  - ❖ Updates the High Performance Computing Act of 1991 to include networking and IT, requires recurring assessments and continual improvement of program
- ❖ S. 920 -- Information Technology Investment Oversight Enhancement and Waste Act of 2009. Introduced by Sen. Carper (D-DE).
  - ❖ Defines CIO reporting requirements for project management efforts associated with critical IT projects



## US Legislative Agenda: Overview of Bills

- ❖ S. 921 -- United States Information and Communications Enhancement Act of 2009. Introduced by Sen. Carper (D-DE) in the Homeland Security and Government Affairs Committee.
  - ❖ Amends FISMA and centralizes government wide oversight of implementation of information security policies and practices
  - ❖ Amend chapter 35 of title 44, United States Code, to recognize the interconnected nature [of networks], improve situational awareness, enhance Federal information security, and establish security standards for government
- ❖ H.R. 4900 -- Federal Information Security Amendments Act of 2010. Introduced by Rep. Watson (D-CA) in the House Government Management, Organization and Procurement Subcommittee of the House Committee on Oversight and Government Reform.
  - ❖ Updates the 2002 Federal Information Security Management Act by shifting to real-time threat monitoring to the Federal IT Infrastructure; it maintains the distinction between national security systems and non-national security systems; and builds security into the procurement process through standards and thresholds.
  - ❖ Establishes a National Office of Cyberspace within the Executive Office of the President and mandates that its director be a permanent Presidential appointed positions subject to Senate Confirmation.
  - ❖ Establishes a new oversight body to be called the Cybersecurity Practice Board within the Office of Cyberspace (similar to the CIO Council) and establishes a National Incident Response Center



## US Legislative Agenda: Overview of Bills

- ❖ S. 946 -- Critical Electric Infrastructure Protection Act of 2009. Introduced by Sen. Lieberman (I-CT) in the Homeland Security and Governmental Affairs Committee.
  - ❖ Amends the Federal Power Act to establish new reporting requirements to DHS on cyber compromises of critical electric infrastructure and directs FERC to establish mandatory interim measures to protect against known cyber vulnerabilities
  - ❖ Directs DHS to conduct an investigation to determine if the security of federally owned programmable electronic devices and communication networks (including hardware, software, and data) essential to the operation of critical electric infrastructure have been compromised
- ❖ H.R. 2195 -- Electric Grid Vulnerability Analysis. Introduced by Rep. Thompson (D-MS) in the Energy and Commerce Committee. (Equivalent of S. 946)
  - ❖ Directs DHS, working with other national security and intelligence agencies, to conduct research and determine if the security of federally owned programmable electronic devices and communication networks (including hardware, software, and data) essential to the operation of critical electric infrastructure has been compromised.



## US Legislative Agenda: Overview of Bills

- ❖ H.R. 2165 -- Bulk Power System Protection Act of 2009. Introduced by Rep. Barrow (D-GA) in the Energy and Commerce Committee.
  - ❖ Calls for FERC to promptly order measures to address known cybersecurity threats and states that FERC must have authorities to respond to cyber emergencies. Amends the Federal Power Act to require the Federal Energy Regulatory Commission (FERC) to establish measures to protect the bulk power system against cybersecurity threats
- ❖ H.R. 5026 -- The Grid Reliability and Infrastructure Defense Act. Introduced by Rep Markey (D-MA). Voted out of House Energy and Environment Subcommittee (3/24/2010) of the House Energy and Commerce Committee. (Revised version of H.R. 2165)
  - ❖ Amends the Federal Power Act and directs the Federal Energy Regulatory Commission to protect the electric transmission and distribution grid from vulnerabilities.
  - ❖ Gives FERC the power to issue orders for emergency measures under the directive of the president and requires the agency to enforce privacy measures and prohibit the disclosure of protected information, but states that "the commission shall protect from disclosure only the minimum amount of information necessary to protect the reliability of the bulk-power system and of defense critical electric infrastructure." 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



## US Legislative Agenda: Overview of Bills

- ❖ S. 1438 -- International Cybercrime Reporting and Cooperation Act. Introduced by Sen. Gillibrand (D-NY) and Sen. Hatch (R-UT) in the Foreign Relations Committee.
  - ❖ Requires the President to produce an annual report to Congress providing an assessment of every country's level of ICT utilization and development; assesses how each country's legal, law enforcement and judicial systems address cyber crime and protect commerce and consumers.
  - ❖ Identifies countries with low ICT penetration and assesses multilateral efforts to develop cybersecurity standards, cooperate to prevent cybercrime, and develop safeguards for the protection of privacy, Intellectual Property Rights, freedom of speech, safety of children and others, and commercial transactions.
- ❖ H.R. 4692 -- International Cybercrime and Cooperation Act. Introduced by Rep. Clarke (D-NY) and Rep. King (R-NY) in the House Foreign Affairs, Ways and Means and Financial Services Committees.
  - ❖ Includes 5 Key provisions: (1) Requires an Annual Presidential Report (same as S. 1438); (2) Requires foreign assistance programs to prevent cybercrime havens to be prioritized; (3) Requires the President to identify countries of concern and produce evidence of cybercrime offenses; (4) Requires benchmarks to be set and establishes penalties to countries who don't meet benchmark; and (5) Requires the Secretary of State to designate a senior official at the State Department to coordinate and focus activities, policies, and opportunities to combat cybercrime internationally.



## US Legislative Agenda: Overview of Bills

- ❖ S. 3193 -- International Cyberspace and Cybersecurity Coordination Act of 2010. Introduced by Sen. Kerry (D-MA) and Sen. Gillibrand (D-NY) in the Senate Foreign Relations Committee.
  - ❖ Strengthens the ability of the United States to develop a clear and coordinated strategy for international cyberspace and cybersecurity policy by authorizing the creation of a senior coordinator at the State Department, with the rank and status of Ambassador at Large.
  - ❖ Senate Confirmed Coordinator (Ambassador) will be the principal advisor to the Secretary of State on international cyberspace and cybersecurity issues. The coordinator will provide strategic direction for United States government policy and programs aimed at addressing cyberspace and cybersecurity issues overseas.



## US Legislative Agenda: Overview of Bills

- ❖ S. 1490 (S. 495) -- Personal Data Privacy and Security Act. Introduced by Sen. Leahy (D-VT) in the Judiciary Committee
  - ❖ Makes fraud in connection with the unauthorized access of sensitive personally identifiable information (in electronic or digital form) a predicate for racketeering charges; and prohibits concealment of security breaches involving such information
  - ❖ Directs the U.S. Sentencing Commission to review and amend its guidelines relating to fraudulent access to, or misuse of, digitized or electronic personally identifiable information (including identify theft)
  - ❖ Establishes in the Federal Trade Commission (FTC) an Office of Federal Identity Protection
- ❖ H.R. 3498 -- Internet Freedom Preservation Act of 2009. Introduced by Rep. Markey (D-MA) and Rep Eshoo (D-IL) at House Energy and Commerce Committee.
  - ❖ Amends the Communications Act of 1934 to establish a national broadband policy, safeguard consumer rights, spur investment and innovation, and for related purposes.



## US Legislative Agenda: Overview of Bills

- ❖ H.R. 1292 -- To Amend title I of the Omnibus Crime Control and Safe Streets Act of 1968. Introduced by Rep. Scott (D-VA) in the House Judiciary Committee.
  - ❖ Authorizes the Director of the Bureau of Justice Assistance to make grants ...to improve the identification, investigation, and prosecution of multi-jurisdictional criminal conspiracies or activities involving terrorism, economic crime, including financial fraud and mortgage fraud, and high-tech crime, including Internet-based crime against children and child pornography.
- ❖ H.R. 2271 -- Global Online Freedom Act of 2009. Introduced by Rep. Smith (R-NJ) in the Foreign Affairs Committee and referred to the Energy and Commerce Committee.
  - ❖ Makes it U.S. policy to: (1) promote the freedom to seek, receive, and impart information and ideas through any media; (2) use all appropriate instruments of U.S. influence to support the free flow of information without interference or discrimination; and (3) deter U.S. businesses from cooperating with Internet-restricting countries in effecting online censorship.
- ❖ S 1070 -- Establish Small Business Information Security Task Force to Address INFOSEC Concerns. Introduced by Sen Snowe (R-ME) in the Senate Small Business and Entrepreneurship Committee.
  - ❖ Directs the Administrator of the SBA to establish the Small Business Information Security Task Force to address Small Business INFOSEC concerns relating to credit card data and other proprietary information.



## US Legislative Agenda: Overview of Bills

- ❖ S. 1047 -- SAFE Internet Act. Introduced by Sen. Menendez (D-NJ) in the Judiciary Committee.
  - ❖ Promotes Internet safety education and cybercrime prevention initiatives and requires electronic record retention for business, schools, individuals, and libraries.
  - ❖ Authorizes \$175 million in funding over five years to programs educating children on how to safely, securely and ethically use the Internet and mobile technologies.
- ❖ H.R. 4061 -- Cybersecurity Enhancement Act of 2009. Introduced by Rep. Lipinski (D-IL) and Rep. McCaul (R-TX) in the Science and Technology Committee. Voted out of the House of Representatives 2/2/10.
  - ❖ Combined the [Cybersecurity Coordination and Awareness Act](#) and the Cybersecurity Research and Development Amendments Act.
    - ❖ Creates an office for a national coordinator for the networking and information technology research and development program to improve cybersecurity research and development and coordination between the federal government, academia and private sector. R&D efforts will focus on identity management technologies and useability, authentication methods, and privacy.
    - ❖ Increases the role of the National Institute of Standards and Technology in developing international cybersecurity technical standards; and charges NIST with creating IT security awareness and education campaigns for the public.



## US Legislative Agenda: Overview of Bills

- ❖ H.R. 1910 -- Chief Technology Officer Act of 2009. Introduced by Rep. Connoly (D-VA) in the Committee on Oversight and Government Reform
  - ❖ Creates the Office of the Federal Chief Technology Officer within the Executive Office of the President: (1) to analyze and advise the President and agency officials regarding the government's information technology infrastructures, strategy, and use; (2) to ensure the security and privacy of the federal information technology infrastructure and networks; (3) to promote technological innovation in the federal government; (4) to establish public-private sector partnership initiatives; and (5) to lead specified interagency efforts, including a planning process to ensure the use best-in-class technologies, share best practices, and improve the use of technology in support of government requirements. Requires the Office to serve as a source of analysis and advice for the President and agency heads regarding major government policies, plans, and programs associated with information technology.
  - ❖ Requires the FCTO to: (1) be a member of the Domestic Policy Council; and (2) publish an annual report on programs to promote technological innovations, recommendations for policies to encourage the generation of such innovations, and information on the Office's activities and accomplishments.



## US Legislative Agenda: Overview of Bills

- ❖ S. 1494 -- Intelligence Authorization Act for Fiscal Year 2010. Introduced by Sen Feinstein (D-CA) and Sen. Bond (R-WVA). Voted out of Senate.
  - ❖ An original bill to authorize appropriations for fiscal year 2010 for intelligence and intelligence-related activities... Includes cybersecurity oversight provision (Sec 340)
- ❖ S. 1475 -- Reduce Iranian Cyber Suppression Act. Introduced by Sen. Schumer (D-NY) in the Senate Homeland Security and Governmental Affairs Committee.
  - ❖ Prohibits the heads of executive agencies from entering into or renewing procurement contracts with persons that export certain computer or telecommunications technologies to Iran, and for other purposes.
- ❖ H.R. 3284 -- Reduce Iranian Cyber Suppression Act. Introduced by Rep. Sherman (D-CA) in the House Oversight and Government Reform Committee.
  - ❖ Prohibit the heads of executive agencies from entering into or renewing procurement contracts with persons that export certain computer or telecommunications technologies to Iran, and for other purposes



## US Legislative Agenda: Overview of Bills

- ❖ H.R. 4098 -- Secure Federal File Sharing Act. Introduced by Rep. Towns (D-NY).
  - ❖ Requires the Director of the Office of Management and Budget to issue guidance on the use of peer-to-peer file sharing software to prohibit the personal use of such software by Government employees, and for other purposes.
- ❖ H.R. 1319 -- Informed P2P User Act. Introduced by Rep. Mack (R-CA). Passed the House of Representatives by voice vote on 12/8/09.
  - ❖ Prevents the inadvertent disclosure of information on a computer through the use of certain "peer-to-peer" file sharing programs without first providing notice and obtaining consent from an owner or authorized user of the computer



## US Legislative Agenda: Overview of Bills

- ❖ H.R. 122 -- Protecting the Privacy of Social Security Numbers Act of 2009. Introduced by Rep Frelinghuysen (R-NJ) in the House Judiciary Committee.
  - ❖ Amends title 18, United States Code, and the Social Security Act to limit the misuse of Social Security numbers, to establish criminal penalties for such misuse, and for other purposes
- ❖ S. 141 -- Protecting the Privacy of Social Security Numbers Act. Introduced by Sen. Feinstein (D-CA) in the Judiciary Committee.
  - ❖ Amends title 18, United States Code, to limit the misuse of Social Security numbers, to establish criminal penalties for such misuse, and for other purposes
- ❖ H.R. 50 -- Social Security Identity Theft Prevention Act. Introduced by Rep. Kirk (R-IL) in the Ways and Means Committee.
  - ❖ Protect seniors from identity theft and strengthen our national security by providing for the issuance of a secure Social Security card.



## US Legislative Agenda: Overview of Bills

- ❖ H.R. 123 -- Credit Agencies Identity Theft Responsibilities Act of 2009. Introduced by Rep Gallegly (R-CA) in the Financial Services Committee.
  - ❖ Amends the Fair Credit Reporting Act to establish additional reporting requirements to enhance the detection of identity theft, and for other purposes
- ❖ H.R. 133 -- Identity Theft Notification Act of 2009. Introduced by Rep Gallegly (R-CA) in the Ways and Means Committee.
  - ❖ Amends title II of the Social Security Act to provide that individuals and appropriate authorities are notified by the Commissioner of Social Security of evidence of misuse of the Social Security account numbers of such individuals.



## US Legislative Agenda: Overview of Bills

- ❖ H.R. 2417 -- Identity Protection Act of 2009. Introduced by Rep Arcuri (D-NY) in the House Ways and Means Committee and Energy and Commerce Committee.
  - ❖ Amend title II of the Social Security Act to preclude use of the social security account number on Government-issued identification cards issued in connection with benefits under Medicare, Medicaid, and CHIP, and for other purposes.
- ❖ H.R. 2472 --Social Security Number Fraud and Identity Theft Prevention Act. Introduced by Rep Coffman (R-CO) in the Immigration, Refugees, Border Security, and International Law Subcommittee of the House Judiciary Committee.
  - ❖ Amends the Fair Credit Reporting Act to establish additional reporting requirements to enhance the detection of identity theft, and for other purposes
- ❖ S. 30 -- Truth in Caller ID Act of 2009. Introduced by Sen. Nelson (D-FL) in the Commerce, Science, and Transportation Committee.
  - ❖ Amends the Communications Act of 1934 to prohibit manipulation of caller identification information



## US Legislative Agenda: Overview of Bills

- ❖ H.R. 1110 -- The PHONE Act of 2009. Introduced by Rep Scott (D-VA). Voted out of House Judiciary Committee.
  - ❖ Amends title 18, United States Code, to prevent caller ID spoofing, and for other purposes
- ❖ H.R. 3817 -- Investor Protection Act of 2009. Introduced by Rep. Kanjorski (D-PA) . Voted out of House Financial Services Committee.
  - ❖ Provides the Securities and Exchange Commission with additional authorities to protect investors from violations of the securities laws, and for other purposes.
  - ❖ Section 508 requires ISPs to block certain scams
- ❖ H.R. 1776 -- Consumers Right to Know Act. Introduced by Rep Markey (D-MA).
  - ❖ Gives consumers the right to access their energy information. It also would require FERC to consult with appropriate federal agencies in issuing guidelines on how to facilitate this.



## US Legislative Agenda: Overview of Bills

- ❖ H.R. 5247 -- Executive Cyberspace Authorities Act of 2010. Introduced by Rep McCaul (R-TX) and Rep. Langevin (D-RI).
  - ❖ Establishes a National Cyberspace Office within the Executive Office of the President, with a Senate Confirmed Director.
  - ❖ Provides authority to the Director of the National Cyberspace Office to recommend that the President withhold awards and bonuses for specific agencies that fail to make adequate efforts to secure their IT infrastructure in their budgets. The cyberspace director also would be responsible for annually providing to Congress an assessment of agency progress in developing and implementing IT policies, significant agency deficiencies and planned remedial action.
  - ❖ Directs each civilian agency to include with its annual budget a:
    - ❖ Review of threats faced by the agency to its information security systems.
    - ❖ Plan to secure the agency's IT infrastructure, based upon National Institute of Standards and Technology guidelines and recommendations.
    - ❖ Description of agency compliance with its established IT practices, including compliance with the Federal Information Security Management Act.
    - ❖ Report on development of secure identity and authentication processes.



# Recommendations

- ❖ Need Congressional leadership to set the legislative priorities for cybersecurity
- ❖ Need to clearly articulate the direction for cybersecurity private-public engagement and responsibilities
- ❖ Need broad-based awareness and education campaign for the U.S. population and other like-minded nations