I. EXECUTIVE ORDERS

In February 2013, President Obama signed an Executive Order and a Policy Directive on cybersecurity. The Order set up the framework for the Public Sector to share information with private companies and entities regarding cyber attacks and breaches. The order does not direct private companies to share sensitive or classified information with the government.

II. BILLS PASSED IN ONE CHAMBER

A. HOUSE

1. **H.R.624**: Cyber Intelligence Sharing and Protection Act (CISPA)
   
   Sponsor: Rep Rogers, Mike J. [MI-8] (introduced 2/13/2013)
   
   - Latest Major Action: 4/10/13 Reported favorably out of Committee on Intelligence
   
   - Status: Referred to Senate committee: Received in the Senate and Read twice and referred to the Select Committee on Intelligence.

   **Bill Summary:**

   - Amends the National Security Act of 1947 to add provisions concerning cyber threat intelligence and information sharing. Defines "cyber threat intelligence" as intelligence in the possession of an element of the intelligence community directly pertaining to: (1) a vulnerability of a system or network of a government or private entity; (2) a threat to the integrity, confidentiality, or availability of such a system or network or any information stored on, processed on, or transiting such a system or network; (3) efforts to deny access to or degrade, disrupt, or destroy such a system or network; or (4) efforts to gain unauthorized access to such a system or network, including for the purpose of exfiltrating information. Excludes intelligence pertaining to efforts to gain unauthorized access to such a system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

2. **H.R.756**: Cybersecurity Enhancement Act of 2013
   
   Sponsor: Rep McCaul, Michael T. [TX-10] (introduced 2/15/2013)
   
   - Latest Major Action: 2/15/2013 Referred to House committee.
   
   - Status: Referred to Senate committee: Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation.

   **Bill Summary:**
• Directs specified federal agencies participating in the National High-Performance Computing Program to: (1) transmit to Congress a cybersecurity strategic research and development plan and triennial updates, and (2) develop and annually update an implementation roadmap for such plan.

**Bill Highlights:**
• Provides for the award of computer and network security research grants by the National Science Foundation (NSF) in the research areas of social and behavioral factors, including human-computer interactions, identity management, as well as the detection, investigation, and prosecution of cyber-crimes involving organized crime and crimes against children.
• Amended in committee: Cybersecurity R&D Agencies required to track and publicize both past and ongoing federal projects

### III. BILLS PENDING IN COMMITTEE

#### A. SENATE

1. **S. 21:** Latest Title: Cybersecurity and American Cyber Competitiveness Act of 2013  
   Sponsor: Sen Rockefeller, John D. IV [WV] (introduced 1/22/2013)  
   - Latest Major Action: 1/22/2013 Referred to Senate committee  
   - Status: Read twice and referred to the Committee on Homeland Security and Governmental Affairs.

**Bill Summary:**
• Calls for the enactment of bipartisan legislation to improve communication and collaboration between the private sector and the federal government to secure the United States against cyber attack, enhance the competitiveness of the United States and create jobs in the information technology industry, and protect the identities and sensitive information of U.S. citizens and businesses by: (1) enhancing the security and resiliency of public and private communications and information networks against cyber attack; (2) establishing mechanisms for sharing cyber threat and vulnerability information between the government and the private sector; (3) developing a public-private system to improve the capability of the United States to assess cyber risk and prevent, detect, and respond to cyber attacks against critical infrastructure such as the electric grid, the financial sector, and telecommunications networks; (4) promoting research and development investments and professional training; (5) preventing and mitigating identity theft; (6) enhancing U.S. diplomatic capacity and public-private international cooperation to respond to emerging cyber threats; (7) expanding resources for investigating and prosecuting cyber crimes in a manner that respects privacy rights and civil liberties and promotes U.S. innovation; and (8) maintaining robust protections of the privacy of U.S. citizens and their online activities and communications.
B. HOUSE OF REPRESENTATIVES

1. **H.R. 86**: Latest Title: Cybersecurity Education Enhancement Act of 2013
   - Status: Referred to the Committee on Science, Space, and Technology, and in addition to the Committees on Education and the Workforce, and Homeland Security, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.

**Bill Summary:**
- The Secretary of Homeland Security, acting through the Assistant Secretary of Cybersecurity, shall establish, in conjunction with the National Science Foundation, a program to award grants to institutions of higher education (and consortia thereof) for the establishment or expansion of cybersecurity professional development programs; the establishment or expansion (or both) of associate degree programs in cybersecurity; and the purchase of equipment to provide training in cybersecurity for either professional development programs or degree programs.