Cybersecurity Act of 2015

- Provides liability protection, anti-trust exceptions, and FOIA exemptions to encourage private entities to voluntarily share information with each other and the government. Liability protection does not extend to use of defensive measures.

- Voluntary by nature--does not create duty to share info with federal or non-federal entities, and assigns no liability for non-participation.

- Authorizes non-federal entities to monitor, share, and receive cyber threat information for cyber purposes, and authorizes use of defensive measures under certain circumstances.

- Information provided to the federal government may be used for certain law enforcement purposes, but not to regulate lawful activity (incl. enforcement activities).

- Requires PII scrub of info ‘known at the time of sharing’ to be “not directly related” to a cyber threat, or configure a technical capability to automatically remove such info. Applies to both public and private entities.

- Establishes DHS portal (housed under NCCIC).
**Data Breach Legislation**

- **Major issues:** state preemption, knowledge / exploitability standard, consumer harm, cybersecurity requirements, third-party service providers.
- **Interest groups split**—financial industry favors Neugebauer/Carney, retail industry favors Langevin, consumer/digital rights groups favor Cicilline.
- **Financial Services Committee** will likely work with Energy & Commerce Committee to combine bills and achieve added industry consensus.

<table>
<thead>
<tr>
<th>Bill</th>
<th>Sponsor</th>
<th>Summary</th>
<th>Major Differences</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Data Notification and Protection Act (H.R. 1704)</td>
<td>Rep. Langevin (D-RI)</td>
<td>Establishes national data breach notification standard. Requires customer notification within 30 days. Establishes DHS office to accept data breach notifications and share with federal law enforcement under certain circumstances.</td>
<td>No creation of federal data security standard for private companies. Requires notification of major media outlets and consumer reporting agencies under certain circumstances.</td>
<td>4/29/15 Referred to Energy &amp; Commerce and Judiciary Committees.</td>
</tr>
</tbody>
</table>
Cybersecurity Issues In 2016

EXECUTIVE BRANCH
• Monitoring of U.S.-China Cyber Agreement; OFAC Implementation of Sanctions (EO 13694) Against Malicious Foreign Cyber Activity
• Policy Repercussions From Russian Cyber Attack on Ukraine Power Grid
• Encryption Debates
• Wassenaar Export Controls on Intrusion Detection and Cyber Surveillance Software
• International Cyber Norms
• NIST Cyber Framework Update, International Strategy, and Cyber-Physical Systems Workshops; Opportunity to Participate/Refine
• Implementation Process and Politics of EU NIS Directive
• OMB/DOD Acquisition Guidance for Cyber Incident Reporting and Security Controls Requirements
• Operationalization of DHS Einstein 3
• Vulnerability Disclosure Coordination Protocols Between Industry and Government (NTIA Lead)
• Financial Sector Developments in FFIEC Regulatory Uniformity/Rationalization
• Increased Enforcement and Security Guidance From Agencies Such as FTC, FCC, SEC
• Cybersecurity R&D Priorities Coordination and Grant Funding

CONGRESSIONAL
• Data Breach Notification Legislation – State Preemption, and Cyber Control Requirements Or Not
• Appropriations/Program and Policy Riders
• Hearings On:
  • Encryption
  • Oversight of Implementation of CISA Data Minimization and Other Requirements
  • DHS Cyber Strategy
  • Cyber Insurance
  • Internet of Things