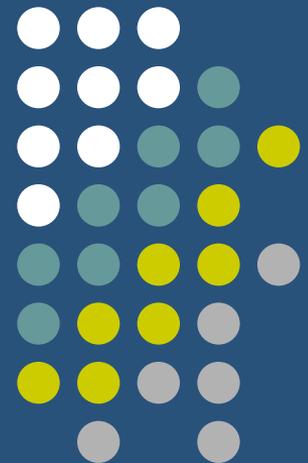


Virginia Joint Commission on Technology and Science

Cybersecurity Legislation





Pending Legislation

- Widespread agreement of need for legislation
- Three approaches
 - CISPA
 - Cybersecurity Act of 2012
 - SECURE IT
- Information Sharing

Information Sharing



- Fed. Gov. to share cybersecurity intelligence with private entities
- Authorizes private entities to monitor and investigate their networks and systems for cybersecurity related information
- Share that information with other private entities and the Federal Government

The Cyber Intelligence Sharing and Protection Act (CISPA)



- H.R. 3523
- Rep. Mike Rogers
- Passed House
- Referred to Senate Committee on Intelligence
- White House has threatened Veto

CISPA



- Director Of National Intelligence
 - Establish procedures to allow intelligence community to share cyber threat intelligence with private sector entities and utilities
- Intelligence agency heads may grant temporary or permanent security clearance

CISPA



Information Shared with Federal Government
may be used for:

- Cybersecurity purposes
- The investigation and prosecution of cybersecurity crimes
- For the protection of individuals from death or bodily harm
- To protect minors from child pornography
- To protect national security

Cybersecurity Act 2012 (CSA)



- S 3414
- Senator Joe Lieberman
- Backed by White House
- Not enough support to defeat filibuster

CSA



- Establishes National Cybersecurity Council
 - Chaired by the Secretary of Homeland Security
 - Conduct sector-by-sector risk assessments and identify categories of critical cyber infrastructure
 - Develop procedures to inform critical infrastructure owners and operators of cyber threats, vulnerabilities, and consequences
 - Provide technical assistance requested by owners and operators.

CSA



- Critical Cyber Infrastructure if damage can cause:
 - Interruption of life sustaining services (energy, water, food, etc.)
 - Catastrophic economic damage
 - Severe degradation of national security
- Requires owners and operators of critical cyber infrastructure to report significant cyber incidents affecting the infrastructure

CSA



- Information may be disclosed to cybersecurity exchanges approved by the Department of Homeland Security
- Cybersecurity exchange may use information for cybersecurity purposes
- May disclose to law enforcement for cybersecurity purposes or if it appears to pertain to a cybersecurity crime or if imminent threat to life or limb

CSA



- Research & Development
- Federal Agencies and Policy Coordination
- Education

SECURE IT



- Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012
- S 3342
- Senator McCain
- No major action after introduction

SECURE IT



- Designates six existing federal entities as cybersecurity centers:
 - Department of Defense Cyber Crime Center
 - Intelligence Community Incident Response Center
 - United States Cyber Command Joint Ops. Center
 - National Cyber Investigative Joint Task Force
 - National Security Agency Central Security Service Threat Operation Center
 - National Cybersecurity and Communications Integration Center

SECURE IT



Information given to cybersecurity centers

- A cybersecurity purpose
- A national security purpose
- To prevent, investigate, or prosecute certain offenses
- Disclosed to State or local government for cybersecurity purpose or criminal investigation

SECURE IT



- Coordination of Federal Agencies and Policies
- Criminal Penalties
- Research & Development
- Education



Criticisms

- Privacy Concerns
 - Overrides protections in various privacy laws
- Contractual Obligations
- Cybersecurity Act -mandated reporting by critical cyber infrastructure owner/operators