Legislative tracker: cybersecurity and technology

February 10, 2020
Roadmap

**Legislation in the 115th Congress**
*Spotlight on S.3085: Federal Acquisition Supply Chain Security Act*
*10/226 cybersecurity bills signed into law*

Legislative forecast

**Legislation in the 116th Congress**
*Bill spotlights*
*Status of current cybersecurity legislation*
*Focus on election security legislation*
*Comparison of legislation by provisions*

State legislation spotlight: privacy laws

White House and executive actions
**Federal Acquisition Supply Chain Security Act**

*S.3085*

**Law at a glance**

- **Passed Senate:** December 18, 2018
- **Passed House:** December 19, 2018
- **Signed into law:** December 21, 2018

**Sen. Claire McCaskill (D-MO)**
*Senate sponsor*

**Rep. Will Hurd (R-TX-23)**
*House sponsor*

**Co-sponsors:**
- **Dem:** 2
- **GOP:** 2

- **Co-sponsors:**
- **Dem:** 3
- **GOP:** 2

**Law overview**

- The law establishes the Federal Acquisition Supply Chain Security Council (FASC), which will work with the National Institute of Standards and Technology to develop guidelines on federal supply chain risk management.
- The FASC will also help develop information sharing standards for federal and non-federal officials regarding supply chain cybersecurity.
- Rep. Hurd introduced the Federal Acquisition Supply Chain Security Act in the House on December 19 as part of H.R. 7327, the SECURE Technology Act. The SECURE Technology Act required DHS to establish both a security vulnerability disclosure policy and a bug bounty pilot program.

**Key actions regarding supply chain security**

**Nov. 2018:** DHS held the first meeting of the ICT Supply Chain Risk Management Task Force, which it formed as a P3 to create recommendations for global ICT supply chain cybersecurity.

**Dec. 2018:** President Trump signed the SECURE Act (which contains the Federal Acquisition Supply Chain Security Act) into law; the council’s membership and first meeting have yet to be announced.

**March 2019:** At an Atlantic Council event, DHS and ODNI officials publicly stated that the task force and security council are meant to complement, and not overlap, each other.

Sources: Congress.gov; Department of Homeland Security; Covington & Burling; FCW.
Legislation in the 115th Congress: cybersecurity
The 115th Congress introduced 226 cybersecurity bills; 10 were signed into law.

S.442: National Aeronautics and Space Administration Transition Authorization Act of 2017
Sponsor: Sen. Ted Cruz (R-TX)
- Authorizes appropriations to NASA for FY2017 for exploration; space operations; science; aeronautics; space technology; education; safety, security, and mission services; construction and environmental compliance and restoration; and the NASA Inspector General.

S.782: PROTECT Our Children Act of 2017
Sponsor: Rep. Thomas Rooney (R-FL-17)
- Amends the PROTECT Our Children Act of 2008 to reauthorize through FY2022 the National Internet Crimes Against Children Data System and the National Strategy for Child Exploitation Prevention and Interdiction

H.R.3364: Countering America’s Adversaries Through Sanctions Act
- Provides congressional review regarding the termination/waiver of sanctions against Russia and counters aggression by Iran, Russia, and North

H.R.1616: Strengthening State and Local Cyber Crime Fighting Act of 2017
Sponsor: Rep. John Ratcliffe (R-TX-4)
- Amends the Homeland Security Act of 2002 to authorize a National Computer Forensics Institute within the U.S. Secret Service to disseminate information related to the investigation and prevention of cyber and electronic crime and related threats and to educate and train

Sponsor: Mac Thornberry (R-TX-13)
- Authorizes FY2019 appropriations and sets forth policies regarding the military activities of the Department of Defense, military construction, and the national security programs of the Department of Energy

H.R.1625: Consolidated Appropriations Act, 2018
- Appropriates funds to cybersecurity initiatives and their respective federal departments and agencies

Sources: Congress.gov
Legislation in the 115th Congress: cybersecurity
The 115th Congress introduced 226 cybersecurity bills; 10 were signed into law.

H.R.3359: Cybersecurity and Infrastructure Security Agency Act of 2018
Sponsor: Rep. Michael McCaul (R-TX-10)
• Re-designates the Department of Homeland Security’s National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency, to be headed by the Director of National Cybersecurity and Infrastructure Security.
• CISA’s responsibilities include leading cybersecurity and critical infrastructure security programs, operations, and associated policy; and carrying out DHS’s responsibilities concerning chemical facility antiterrorism standards

H.R.7327: SECURE Technology Act
Sponsor: Rep. Will Hurd (R-TX-23)
• Directs the Department of Homeland Security to establish a policy applicable to individuals, organizations, and companies to report security vulnerabilities on DHS information systems and to develop a process to address the mitigation of remediation of the vulnerabilities reported
• Directs DHS to establish a bug bounty pilot program to minimize security vulnerabilities

Sponsor: Rep. Mac Thornberry (R-TX-13)
• Authorizes appropriations to the Department of Defense for procurement; research, development, test and evaluation; operation and maintenance; working capital funds; the Joint Operational Needs Fund; chemical agents and munitions destruction; drug interdiction and counter-drug activities; the Defense Inspector General; the Defense Health Program; the Armed Forces Retirement Home; overseas contingency operations; and military construction

H.R.3243: FITARA Enhancement Act of 2017
Sponsor: Rep. Gerald Connelly (D-VA-11)
• Makes permanent several provisions related to transparency and risk management assessment of major information technology investments and agency reviews of information technology portfolios to reduce duplication and realize savings

Sources: Congress.gov
Roadmap

Legislation in the 115th Congress
Spotlight on S.3085: Federal Acquisition Supply Chain Security Act
10/226 cybersecurity bills signed into law

Legislative forecast

Legislation in the 116th Congress
Bill spotlights
Status of current cybersecurity legislation
Focus on election security legislation
Comparison of legislation by provisions

State legislation spotlight: privacy laws

White House and executive actions
Legislative forecast: cybersecurity

Potential legislative actions regarding cybersecurity

Consumer security:

The Senate will continue to consider major privacy bills from Sens. Maria Cantwell (D-WA) and Ron Wicker (R-MS) on the federal level. On the state level, the California Consumer Privacy Act (CCPA) went into effect on January 1st, 2020, and other states are expected to pass similar legislation in the next year. Over the summer, the FTC announced it would undertake an early review of the Children’s Online Privacy Protection Act and is looking to update its rule on internet privacy for children.

Election cybersecurity:

The FY 20 spending bill allots an increase in federal spending from the FY 18 spending bill, from $380 million to $425 million for state improvements to the administration of federal elections. This funding can be used for various improvements on the state level, including audit systems and replacing electronic systems with voter-verified paper records. While federal budget has increased, legislation has lagged and the NDAA has instituted no comprehensive reform since the 2016 election interference.

Federal agency cybersecurity:

In September 2018, the House passed the Advancing Cybersecurity Diagnostics and Mitigation Act (H.R.6443), but the bill stalled in the Senate. Congress has awarded $25 million for the Technology Modernization Fund in FY 2020, the same amount allocated in FY 19, however less than the $150 million requested in the White House budget; agencies can apply for TMF loans to fund cybersecurity and other IT projects.

Sources: Congress.gov, Meritalk
Roadmap

- Legislation in the 115th Congress
  - Spotlight on S.3085: Federal Acquisition Supply Chain Security Act
  - 10/226 cybersecurity bills signed into law
- Legislative forecast

- Legislation in the 116th Congress
  - Bill spotlights
  - Status of current cybersecurity legislation
  - Focus on election security legislation
  - Comparison of legislation by provisions
- State legislation spotlight: privacy laws
- White House and executive actions
The FY20 National Defense Authorization Act included key cybersecurity provisions

**Election security**
- Requires the director of National Intelligence and DHS to brief Congress, state and local governments, campaigns, and parties when there is a significant cyber intrusion or attack
- Expands and speeds up security clearances for election officials
- Requires the development of strategy to counter foreign influence
- ODNI is required to designate a lead counterintelligence official for election security

**Military operations organization**
- Further separates leadership of Cyber Command and NSA by requiring the designation of a senior military adviser for cyber policy in the office of the Defense Secretary
- Calls on the Pentagon’s cyber adviser to conduct a study of the strategy, structure and personnel of various cyber and defense operations entities
- Orders a Northern Command and Cyber Command exercise in 2020

**Cyber infrastructure**
- Sens. Angus King (I-ME) and Jim Risch (R-ID) put forward a proposal to establish a program to test analog and other methods of protecting the grid from cyberattack
- Authorizes the use of military construction funds to make cyber and other improvements to utility systems serving military installations

**Defense cyber acquisition and the CIO**
- Requires the Defense secretary to designate three test networks for cybersecurity products and services
- Expands the role of the CIO

Sources: Politico
The Cyber Diplomacy Act of 2019
H.R.739

Bill at a glance

Bill overview

• Would create an ambassador for cyberspace, who would lead the Department of State’s cyber diplomacy efforts and direct the UN ambassador to promote an international cyberspace policy based on the values of openness, reliability, security, human rights, democracy, economic prosperity, freedom, and right to privacy
• Would implement an international cyber policy
• Would encourage cooperation with foreign governments who support US international cyberspace policy
• Would require annual country reports from the State Department on human rights and internet freedoms

By introducing the bill, Rep. McCaul’s goal is to establish American leadership on the world stage by keeping the internet open, secure, and reliable.

Co-sponsors: 29
Dem 13
GOP 16

Sources: Congress.gov
National Cybersecurity Preparedness Consortium Act  
H.R.1062/S.333

Bill at a glance

Bill overview
- Would establish a consortium of nonprofit and academic institutions to develop, update, and deliver cybersecurity training in support of homeland security
- Would authorize the Secretary of Homeland Security to work with the consortium to assist the National Cybersecurity and Communications Integration Center by:
  - Providing cybersecurity training to state and local officials and first responders
  - Developing and updating a cybersecurity curriculum, using existing programs and models for state and local first responders and officials
  - Providing technical assistance to prepare and respond to threats or acts of terrorism
  - Conducting cross-sector cybersecurity training and simulation exercises
  - Helping states and communities develop cybersecurity information sharing programs
  - Incorporating cybersecurity risks and incident responses into existing state and local emergency plans

Co-sponsors: 7
Dem 4  
GOP 3

Co-sponsors: 3
Dem 1  
GOP 2

Sources: Congress.gov
IoT Cybersecurity Improvement Act of 2019
H.R.1668/S.734

Bill at a glance

Bill overview
• Would require the National Institute of Standards and Technology (NIST) director to oversee efforts involving secure development, identity management, patching, and configuration management for Internet of Things devices
• Would require the NIST director to develop recommendations for the use and management of Internet of Things devices owned or controlled by federal agencies
• Would instruct the director of the Office of Management and Budget (OMB) to ensure that the guidelines issued by NIST are consistent with information security requirements
• Would require the NIST director to publish guidelines on policies and procedures concerning security vulnerabilities
• Would order the OMB director, in consultation with the administrator of the General Services Administration, to issue guidelines for each agency concerning security vulnerabilities

Sources: Congress.gov
Data Breach Prevention and Compensation Act of 2019
H.R.2545/S.1336

Bill at a glance

Rep. Elijah Cummings
(D-MD-7)
Bill sponsor

Sen. Elizabeth Warren
(D-MA)
Bill sponsor

Co-sponsors: 20
Dem 20
GOP 0

Co-sponsors: 1
Dem 1
GOP 0

Bill overview

• Would create an Office of Cybersecurity at the Federal Trade Commission for the supervision of data security at consumer reporting agencies
• Would require the creation of regulations on standards for effective cybersecurity measures at consumer reporting agencies
• Would impose penalties on credit reporting agencies for cybersecurity breaches that put sensitive consumer data at risk
• Would annually examine the data security measures of covered consumer reporting agencies for compliance with outlined requirements
• Would submit to Congress an annual report on the findings of each investigation carried out by the Office, and inform Congress of how enhancements can be made to the Office

Introduced in House 5/7/19
Passed committee
Passed House
Differences resolved
Signed into law

Passed in Senate 5/7/19
Passed committee
Passed Senate

Sources: Congress.gov
Legislation in the 116th Congress: cybersecurity
Current Status

H.R.618/S.29: To establish the Office of Critical Technologies and Security, and for other purposes
House sponsor: Rep. C.A. Dutch Ruppersberger (D-MD-2)
Senate sponsor: Sen. Mark Warner (D-VA)
• Would address state-sponsored cyber activities against the United States

H.R.1493/S.602: Cyber Deterrence and Response Act of 2019
House sponsor: Rep. Ted Yoho (R-FL-3)
Senate sponsor: Sen. Cory Gardner (R-CO)
• Would address state-sponsored cyber activities against the United States

H.R.1644/S.682: Save the Internet Act of 2019
House sponsor: Rep. Mike Doyle (D-PA-18)
Senate sponsor: Sen. Ed Markey (D-MA)
• Would restore the open internet order of the Federal Communications Commission

H.R.1649/S.771: Small Business Development Center Training Act of 2019
House sponsor: Rep. Steve Chabot (R-OH-1)
Senate sponsor: Sen. Marco Rubio (R-FL)
• Would amend the Small Business Act to require cyber certification for small business development center counselors

Sources: Congress.gov
**Legislation in the 116th Congress: cybersecurity**

*Current Status*

**H.R.1731/S.592: Cybersecurity Disclosure Act**
- House sponsor: Rep. James Himes (D-CT-4)
- Senate sponsor: Sen. Jack Reed (D-RI)
  - Would require businesses to publicly disclose whether their board members have cybersecurity expertise; and, if none do, disclose how the company considers cybersecurity issues when choosing board members

**H.R.1934/S.917: Stop HATE Act of 2019**
- Senate sponsor: Sen. Robert Casey, Jr. (D-PA)
  - Would direct the Assistant Secretary of Commerce for Communications and Information to submit reports on the role of telecommunications in hate crimes

**H.R.2130/S.1065: State Cyber Resiliency Act**
- House sponsor: Rep. Derek Kilmer (D-WA-6)
- Senate sponsor: Sen. Mark Warner (D-VA)
  - Would establish a grant program to help state and local governments mitigate cybersecurity risks or threats

- Sponsor: Rep. Will Hurd (R-TX-23)
  - Would give the federal Chief Information Officer authority over the Office of Management and Budget’s cybersecurity efforts

*Sources: Congress.gov*
### Legislation in the 116th Congress: cybersecurity

**Current Status**

#### H.R. 269 / S.1379: Pandemic and All-Hazards Preparedness and Advancing Innovation Act

- **Senate sponsor:** Sen. Richard Burr (R-NC)
- **House sponsor:** Anna Eshoo (D-CA-18)
- Would direct the Secretary of Health and Human Services to submit a report on health preparedness and response to cybersecurity threats

#### H.R. 328: Hack Your State Department Act

- **Sponsor:** Rep. Ted Lieu (D-CA-33)
- Would require the Secretary of State to establish a Vulnerability Disclosure Process to improve Department of State cybersecurity and a bug bounty program to identify and report vulnerabilities

#### H.R. 360: Cyber Sense Act of 2019

- **Sponsor:** Rep. Robert Latta (R-OH-5)
- Would require the Department of Energy to establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system

#### H.R. 1158: DHS Cyber Incident Response Teams Act of 2019

- **Sponsor:** Rep. Michael McCaul (R-TX-10)
- Would authorize the cyber incident response teams at the Department of Homeland Security

Sources: Congress.gov

* Denotes considered under suspension of the rules
Legislation in the 116th Congress: cybersecurity
Current Status

**H.R.1359: Digital GAP Act**
Sponsor: Rep. Ron Wright (R-TX-6)
- Would promote Internet access in developing countries and update foreign policy towards the Internet

**H.R.1592: Cybersecurity Skills Integration Act**
Sponsor: Rep. James Langevin (D-RI-2)
- Would establish a pilot program to award grants for cybersecurity postsecondary career and technical education programs

**H.R.1648: Small Business Advanced Cybersecurity Enhancements Act**
Sponsor: Rep. Steve Chabot (R-OH-1)
- Would establish a new federal unit for the government and small businesses to share cybersecurity threats and defensive measures

**H.R.1975: Cybersecurity Advisory Committee Authorization Act**
- Would establish a committee, consisting of up to 35 industry representatives and state/local government officials to advise the CIA on cybersecurity matters

Sources: Congress.gov  * Denotes considered under suspension of the rules
## Legislation in the 116th Congress: cybersecurity

### Current Status

**H.R.2331: SBA Cyber Awareness Act**  
**Sponsor:** Rep. Jason Crow (D-CO-6)  
- Would require an annual report on the cybersecurity of the Small Business Administration

<table>
<thead>
<tr>
<th>Introduced in House</th>
<th>Passed committee</th>
<th>Passed House</th>
<th>Differences resolved</th>
<th>Signed into law</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/18/19</td>
<td>6/13/19</td>
<td>7/15/19</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**H.R.2476: Securing American Nonprofit Organizations Against Terrorism Act of 2019**  
**Sponsor:** Rep. Bennie Thompson (D-MS-2)  
- Would authorize DHS to grant nonprofit organizations funds to institute new physical and cyber security measures

<table>
<thead>
<tr>
<th>Introduced in House</th>
<th>Passed committee</th>
<th>Passed House</th>
<th>Differences Resolved</th>
<th>Signed into law</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/2/19</td>
<td>5/30/19</td>
<td>6/10/19</td>
<td></td>
<td>1/24/20</td>
</tr>
</tbody>
</table>

**H.R.2488: U.S.-Israel Cybersecurity Center of Excellence Act**  
**Sponsor:** Rep. David Cicilline (D-RI-1)  
- Would require the Secretary of State to report on the potential benefits to the United States of establishing a joint United States-Israel cybersecurity center

<table>
<thead>
<tr>
<th>Introduced in House</th>
<th>Passed committee</th>
<th>Passed House</th>
<th>Differences resolved</th>
<th>Signed into law</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/2/19</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**S.315: DHS Cyber Hunt and Incident Response Teams Act of 2019**  
**Sponsor:** Sen. Margaret Hassan (D-NH)  
- Would authorize DHS to maintain cyber hunt and incident response teams to assist federal and non-federal entities, including in critical infrastructure sectors

<table>
<thead>
<tr>
<th>Introduced in House</th>
<th>Passed committee</th>
<th>Passed House</th>
<th>Differences resolved</th>
<th>Signed into law</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/18/19</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*While S. 315 has not passed, a related House bill (H.R. 1158) passed both houses and became law on 12/20/19*
Legislation in the 116th Congress: cybersecurity

Current Status

**S.406: Federal Rotational Cyber Workforce Program Act of 2019**
Sponsor: Sen. Gary Peters (D-MI)
- Would develop rules and policies for a program to rotate cybersecurity employees among federal agencies

**S.429: Cyber Security Exchange Act**
Sponsor: Sen. Amy Klobuchar (D-MN)
- Would establish a rotation program for cybersecurity employees in the private sector and federal agencies

**S.1289: Measuring the Economic Impact of Broadband Act of 2019**
Sponsor: Sen. Amy Klobuchar (D-MN)
- Would require the Secretary of Commerce to conduct an assessment and analysis of the effects of broadband deployment and adoption on the US economy

**S.772: SBA Cyber Awareness Act**
Sponsor: Sen. Marco Rubio (R-FL)
- Would require an annual report on the cybersecurity of the Small Business Administration

Sources: Congress.gov
**Legislation in the 116th Congress: cybersecurity**

*Current Status*

<table>
<thead>
<tr>
<th>Bill Number</th>
<th>Bill Title</th>
<th>House Sponsor</th>
<th>Senate Sponsor</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.842</td>
<td>Improving Broadband Mapping Act of 2019</td>
<td>Sen. Amy Klobuchar (D-MN)</td>
<td></td>
<td>Introduced in Senate 3/14/19</td>
</tr>
<tr>
<td>S.846</td>
<td>Transit Infrastructure Vehicle Security Act</td>
<td>Sen. John Cornyn (R-TX)</td>
<td></td>
<td>Introduced in Senate 3/14/19</td>
</tr>
<tr>
<td>S.890</td>
<td>Senate Cybersecurity Protection Act</td>
<td>Sen. Ron Wyden (D-OR)</td>
<td></td>
<td>Introduced in Senate 3/27/19</td>
</tr>
</tbody>
</table>

**Sources:** Congress.gov
Legislation in the 116th Congress: cybersecurity
Current Status

**H.R. 2881/S.893: Secure 5G and Beyond Act of 2019**
- House sponsor: Rep. Abigail Davis Spanberger (D-VA-7)
- Senate sponsor: Sen. John Cornyn (R-TX)
- Would require the White House to develop a 5G strategy to include cybersecurity issues

**H.R. 1931/S.894: Domestic Terrorism Prevention Act of 2019**
- House sponsor: Rep. Bradley Scott Schneider (D-IL-10)
- Senate sponsor: Sen. Richard Durbin (D-IL)
- Would designate offices within the Department of Homeland Security, the Department of Justice, and the Federal Bureau of Investigation to monitor and prevent potential domestic terrorist activity

**H.R. 1328/S.1046: ACCESS BROADBAND Act**
- House sponsor: Rep. Paul Tonko (D-NY-20)
- Senate sponsor: Sen. Catherine Cortez Masto (D-NV)
- Would establish the Office of Internet Connectivity and Growth within the National Telecommunications and Information Administrations

**S.1167: Digital Equity Act of 2019**
- Sponsor: Sen. Patty Murray (D-WA)
- Would require the Assistant Secretary of Commerce for Communications and Information to establish a State Digital Equity Capacity Grant Program

---

### Differences Resolved
- **Passed in House**: 1/8/20
- **Passed in Senate**: 1/7/20
- **Passed Committee**: 12/19/19
- **Signed into Law**: 6/27/19

### Passed Committee
- **Introduced in House**: 5/21/19
- **Passed Committee**: 1/7/20
- **Passed House**: 1/8/20
- **Passed Committee**: 1/2/20
- **Passed Senate**:
- **Passed Committee**: 3/27/19
- **Passed Senate**:
- **Passed Committee**: 3/27/19
- **Passed Senate**:
- **Passed Committee**: 4/4/19
- **Passed Senate**:
- **Passed Committee**: 4/11/19
- **Passed Senate**:

* Denotes considered under suspension of the rules
For the People Act of 2019
H.R.1

Bill at a glance

Bill overview
- Codifies DHS “critical infrastructure” designation for US election systems
- Authorizes federal funds to help states improve election security
- Includes electronic poll book in HAVA voting systems standards
- Requires paper ballots in federal elections
- Requires election-threat reports among federal and state governments
- Requires the development of a national strategy to protect US democratic institutions
- Expedites security clearances for election officials
- Amends the FECA foreign national prohibition to include state and local ballot initiatives
- Requires FEC to report to Congress on the presence of foreign funds in federal elections

Rep. John Sarbanes
(D-MD-3)
House bill sponsor

Co-sponsors: 236
- GOP 1
- Dem 235

Sources: Congress.gov
Legislation in the 116th Congress: election security

**Current Status**

**S. 1540 / H.R. 2660: Election Security Act of 2019**
- House sponsor: Rep. Bennie Thompson (D-MS-2)
- Senate sponsor: Sen. Amy Klobuchar (D-MN)
- Would provide $1 billion to the states to shore up election security efforts
- Would require states use paper ballots
- Establishes cybersecurity standards for voting machine vendors

**H.R. 2722 / S. 2053: SAFE Act**
- Senate sponsor: Sen. Amy Klobuchar (D-MN)
- Would require that voting systems use individual, durable, voter-verified paper ballots, as well as meet specified cybersecurity requirements, including blocking voting machines from connecting to the internet, among other provisions securing voting systems.

**H.R. 2592 / S. 1356: Honest Ads Act**
- House sponsor: Rep. Derek Kilmer (D-WA-6)
- Senate sponsor: Sen. Amy Klobuchar (D-MN)
- Would require online political ads publicly disclose who paid for the ad
- Intended to ensure foreign entities do not buy political ads

Sources: Congress.gov
Legislation in the 116th Congress: election security

Current Status

S.825: Protect our Elections Act
Sponsor: Sen. Chris Van Hollen (D-MD)
- Would amend the Help America Vote Act of 2002 to require states to take steps to ensure domestic ownership and control of election service providers

S.482: Defending American Security From Kremlin Aggression Act of 2019
Sponsor: Sen. Lindsey Graham (R-SC)
- Would strengthen the North Atlantic Treaty Organization, combat international cybercrime, and impose additional sanctions with respect to Russia

Sources: Congress.gov
## Comparison of cybersecurity legislation by provision (1/5)

<table>
<thead>
<tr>
<th>Bill No.</th>
<th>Short Title</th>
<th>Critical infrastructure</th>
<th>Information sharing</th>
<th>Agency roles</th>
<th>Regulatory reform</th>
<th>Workforce</th>
<th>R&amp;D</th>
<th>Cybercrime &amp; terrorism</th>
<th>Data breach notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.R.269 / S.1379</td>
<td>Pandemic and All-Hazards Preparedness and Advancing Innovation Act</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>H.R.328</td>
<td>Hack Your State Department Act</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.R.360</td>
<td>Cyber Sense Act of 2019</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.R.739</td>
<td>Cyber Diplomacy Act of 2019</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.R.1158</td>
<td>DHS Cyber Incident Response Teams Act of 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.R.1359</td>
<td>Digital GAP Act</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.R.1592</td>
<td>Cybersecurity Skills Integration Act</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sources: Congress.gov
## Comparison of cybersecurity legislation by provision (2/5)

<table>
<thead>
<tr>
<th>Bill No.</th>
<th>Short Title</th>
<th>Critical infrastructure</th>
<th>Information sharing</th>
<th>Agency roles</th>
<th>Regulatory reform</th>
<th>Workforce</th>
<th>R&amp;D</th>
<th>Cybercrime &amp; terrorism</th>
<th>Data breach notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.R.1648</td>
<td>Small Business Advanced Cybersecurity Enhancements Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>H.R.2331</td>
<td>SBA Cyber Awareness Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>H.R.2476</td>
<td>Securing American Non-profit Organizations Against Terrorism Act of 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>H.R.2488</td>
<td>U.S.-Israel Cybersecurity Center of Excellence Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>H.R. 2545/</td>
<td>Data Breach Prevention and Compensation Act of 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>S.1336</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.R. 2722/</td>
<td>SAFE Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>S. 2053</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.R. 2592/</td>
<td>Honest Ads Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>S. 1356</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sources: Congress.gov
## Comparison of cybersecurity legislation by provision (3/5)

<table>
<thead>
<tr>
<th>Bill No.</th>
<th>Short Title</th>
<th>Critical infrastructure</th>
<th>Information sharing</th>
<th>Agency roles</th>
<th>Regulatory reform</th>
<th>Workforce</th>
<th>R&amp;D</th>
<th>Cybercrime &amp; terrorism</th>
<th>Data breach notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.R.618/S.29</td>
<td>To establish the Office of Critical Technologies and Security, and for other purposes.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.R.1493/S.602</td>
<td>Cyber Deterrence and Response Act of 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>H.R.1644/S.682</td>
<td>Save the Internet Act of 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>H.R.1668/S.734</td>
<td>IoT Cybersecurity Improvement Act of 2019</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>H.R.1731/S.592</td>
<td>Cybersecurity Disclosure Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>H.R.1934/S.917</td>
<td>Stop HATE Act of 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>H.R.2130/S.1065</td>
<td>State Cyber Resiliency Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Sources: Congress.gov
## Comparison of cybersecurity legislation by provision (4/5)

<table>
<thead>
<tr>
<th>Bill No.</th>
<th>Short Title</th>
<th>Critical infrastructure</th>
<th>Information sharing</th>
<th>Agency roles</th>
<th>Regulatory reform</th>
<th>Workforce</th>
<th>R&amp;D</th>
<th>Cybercrime &amp; terrorism</th>
<th>Data breach notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.482</td>
<td>Defending American Security From Kremlin Aggression Act of 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>S.772</td>
<td>SBA Cyber Awareness Act</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.825</td>
<td>Protect our Elections Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>S.842</td>
<td>Improving Broadband Mapping Act of 2019</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.846</td>
<td>Transit Infrastructure Vehicle Security Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>S.890</td>
<td>Senate Cybersecurity Protection Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>S.893/H.R. 2881</td>
<td>Secure 5G and Beyond Act of 2019</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.894/H.R. 1931</td>
<td>Domestic Terrorism Prevention Act of 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Sources: Congress.gov
## Comparison of cybersecurity legislation by provision (5/5)

<table>
<thead>
<tr>
<th>Bill No.</th>
<th>Short Title</th>
<th>Critical infrastructure</th>
<th>Information sharing</th>
<th>Agency roles</th>
<th>Regulatory reform</th>
<th>Workforce</th>
<th>R&amp;D</th>
<th>Cybercrime &amp; terrorism</th>
<th>Data breach notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.315</td>
<td>DHS Cyber Hunt and Incident Response Teams Act of 2019</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>S.406</td>
<td>Federal Rotational Cyber Workforce Program Act of 2019</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.429</td>
<td>Cyber Security Exchange Act</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.1046</td>
<td>ACCESS BROADBAND Act</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.1167</td>
<td>Digital Equity Act of 2019</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>S.1241/H.R.3605</td>
<td>Protecting American Consumers from Robocalls Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.1289</td>
<td>Measuring the Economic Impact of Broadband Act of 2019</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.1540/H.R.2660</td>
<td>Election Security Act of 2019</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sources: Congress.gov
Roadmap

Legislation in the 115th Congress
Spotlight on S.3085: Federal Acquisition Supply Chain Security Act
10/226 cybersecurity bills signed into law

Legislative forecast

Legislation in the 116th Congress
Bill spotlights
Status of current cybersecurity legislation
Focus on election security legislation
Comparison of legislation by provisions

State legislation spotlight: privacy laws

White House and executive actions
The California Consumer Privacy Act went into effect on January 1, 2020

**AB 375: Consumer Privacy Act**

Establishes data privacy rights for California residents including the rights to access personal data, know what data are being collected, know how personal data are being used, and prevent the sale of personal data.

Allows consumers to request both the categories and details of specific personal data being collected, as well as the purposes for collecting the information and the categories of third parties with whom the information is shared.

**“Personal information” definition, according to the law**

Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

Sources: California Legislative Information, Jan. 2019
In June 2017, Nevada Governor Brian Sandoval signed legislation relating to internet privacy

SB 538: An act relating to internet privacy

Requires internet operators that collect personally identifiable information to provide a privacy notice that discloses the “categories of covered information” collected, as well as whether third parties may collect data and the process, if any, in which individuals may change their data collected.

“Covered information” definition, according to the law

1) A first and last name
2) A home or other physical address which includes the name of a street and the name of a city or town
3) An electronic mail address
4) A telephone number
5) A social security number
6) An identifier that allows a specific person to be contacted physically or online
7) Any other information concerning a person collected from the person through the internet website or online service of the operator and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable

Sources: Nevada Legislative Counsel Bureau, Jan. 2019
California, New York, and other states are drafting or have enacted legislation introducing patient privacy standards

States focusing on health data privacy in the 2020 legislative session

California

- Companies that handle health data in California will have to comply with the newest privacy provisions under the California Consumer Privacy Act
- The new rules allow patients to decline the sale of their data and gives patients the right to sue if their information is stolen, encompassing more companies in the healthcare ecosystem than what are covered under HIPAA

New York

- The New York Privacy Act is a similar all-encompassing privacy bill, but is broader than California’s and includes a wide-ranging definition of privacy risk and what exemptions it allows are unclear
- The measure has been introduced into the state Senate and is being reviewed by committee

Washington

- In January 2020, Washington state re-introduced the Washington Privacy Act into the state legislature
- Similar to California’s CCPA, this bill would act as comprehensive legislation including a broad set of privacy standards on companies in the healthcare ecosystem not currently covered by HIPAA, but would not conflict with its existing standards

Sources: Bloomberg Law, Becker’s Healthcare
Roadmap

Legislation in the 115th Congress

*Spotlight on S.3085: Federal Acquisition Supply Chain Security Act*

10/226 cybersecurity bills signed into law

Legislative forecast

Legislation in the 116th Congress

*Bill spotlights*

*Status of current cybersecurity legislation*

*Focus on election security legislation*

*Comparison of legislation by provisions*

State legislation spotlight: privacy laws

**White House and executive actions**
White House and DoD cybersecurity strategies

**White House**

*Cyber Strategy*

**Supply chain:**
- The *National Cyber Strategy* cites the need to improve the federal procurement system, including by streamlining activities and avoiding high risk vendors.
- It also outlines the need to improve information sharing within the federal government and establish a supply chain risk assessment shared service.

**Trade:**
- In their strategy, the White House criticizes nations that use national security concerns to justify data localization, stating that the administration will promote “global innovation and the free flow of data.”
- The strategy states the administration’s support for U.S. leadership in the emerging technologies market.

**Department of Defense**

*Cyber Strategy*

**National security:**
- In their *Cyber Strategy*, the Department of Defense states that China and Russia pose national security and economic concerns: China by allegedly stealing technology or other sensitive information, and Russia by challenging democratic processes.

**Action items:**
- The Department of Defense outlined their strategic approach to improve cybersecurity, which includes:
  - Using automation to identify cyber threats
  - Working with public and private sector partners to share information and protect critical infrastructure
  - Crowd-sourcing (e.g. through hack-a-thons or bug bounty programs) to identify and mitigate threats
  - Working with industry and academic partners to promote STEM and foreign language education, especially at the primary and secondary education levels

Sources: National Cyber Strategy of the United States of America; Department of Defense Cyber Strategy.
The federal budget has increased funding for the states to improve election security following the 2016 election cycle.

Federal funding for state improvements to the administration of federal elections

DOLLARS IN MILLIONS

<table>
<thead>
<tr>
<th></th>
<th>FY18 spending bill</th>
<th>FY20 spending bill</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replacing electronic-only equipment with equipment that uses a voter-verified paper record</td>
<td>$380</td>
<td>$425</td>
</tr>
<tr>
<td>Implementing a post-election audit system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upgrading election-related computer systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilitating cybersecurity training for state and local election officials</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementing established cybersecurity best practices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other activities that might improve federal election security</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sources: Congressional Research Service
In May 2019, President Trump issued an executive order related to supply chain security

The order prohibits the government from any transaction or use of technology that poses a national security risk, specifically covering communications or information technology or services designed, developed, or manufactured by individuals connected to or controlled by foreign adversaries.

The order does not name China specifically and leaves room to add other countries to an eventual ban.

Directs the Commerce Department to issue regulations and procedures for reviewing transactions within 150 days.

On November 26, 2019, the Commerce Department issued a proposed rule that would allow the secretary to identify and assess transactions that pose national security risks to the ICTS supply chain, the digital economy, and those living in the US.

Companies would be notified and allowed to defend themselves before the decision is finalized.

BSA, a major group representing software makers, expressed extensive concerns that the rule was too broad and sought a supplemental NPRM for further collaboration between industry and Commerce.

Sources: The Hill, NextGov, Baker Mckenzie
On January 30, DOD released the Cybersecurity Maturity Model Certification Framework for government contractors

**Framework purpose:** The goal of the model is to evaluate the cybersecurity of the Defense Industrial Base (DIB), particularly the controlled unclassified information (CUI) in the supply chain, following a series of data breaches of DOD information.

**Framework overview**

- **Model**
- **Domains**
  - The model encompasses 17 domains related to different aspects of cybersecurity

- **Processes**
  - Within each domain, processes span a subset of the five levels ranging from basic to advanced cyber hygiene

- **Capabilities**
  - In each domain, there are between one and five capabilities spanning five levels ranging from basic to advanced cyber hygiene

- **Practices**
  - Within each capability, there are practices spanning a subset of the five levels ranging from basic to advanced cyber hygiene

**Accountability measures**

- Defense contractors will no longer be allowed to self-certify compliance with cybersecurity standards or rely on Plans of Action and Milestones to fill gaps in System Security Plans.

- Third-party auditors, regulated by a not-yet-determined NGO, will be responsible for certifying contractor compliance with the CMMC framework.

**Looking Forward:** DOD expects to issue proposed regulations in Spring 2020 and include certification requirements in 10 contracts before the end of the year.

Sources: Department of Defense, Inside Cybersecurity, National Law Review, Covington and Burlingon
DHS Information and Communications Technology Supply Chain Risk Management Task Force brings together the public and private sector to improve supply chain security

**Vision**
The task force was founded with the goal of tackling long-term foundational SCRM issues and build cooperation between the public and private sectors

**Activities**
Launched in 2018 by DHS to:
- Inventory existing supply chain risk management activities across government and industry
- Improve supply chain risk information sharing
- Identify processes and criteria for threat-based evaluation of ICT supplies, products, and services
- Offering recommendations for the Qualified Bidder and Manufacturer lists
- Develop policy recommendations to incentivize the purchase of ICT from secure sources

**Membership**
- The first public-private partnership for managing risks to the ICT supply chain, the task force includes 40 private partners and 20 federal partners

**Relationship with Federal Acquisition Security Council**
- The task force’s findings will serve as private-sector input for council efforts to shape and update procurement rules across the government
- Could help the council to determine the conditions that might justify barring a company or product from government networks

Sources: CISA, FCW
The Federal Acquisition Security Council (FASC) focuses on securing federal procurement rules across government agencies

**Authorization**
Mandated by the SECURE Technology Act, signed by President Trump in late 2018

**Activities**
Develops uniform criteria to assist department and agencies to:
- Determining the risk to the ICT supply chain
- Sharing supply chain risk information
- Determining appropriate action to mitigate supply chain risk, including excluding risky vendors from the supply chain

**Membership**
Chaired by OMB and includes members from the Office of the Director of National Intelligence and the departments of Commerce, Defense, Justice, and Homeland Security

**Relationship with DHS ICT SCRM Task Force**
- While the task force encourages collaboration between the public and private sectors, the council is meant to create consistency across the government
- Could receive input from the task force on the conditions that might justify barring a company or product from government networks

Sources: FCW, Inside Cybersecurity, The Hill