Byers, Dave

From:	Brian de Vallance <brian.devallance@gmail.com>
Sent:	Friday, February 3, 2023 5:11 AM
To:	Brian de Vallance*
Subject:	FYI: The Center for Internet Security's DC Report
Attachments:	CIS DC Report (December 2022) (PDF).pdf

Good morning. I'm attaching the latest regular edition of the CIS DC Report, which contains select executive and legislative branch cyber policy developments, including a final recap of key bills that were considered and passed in the 117th Congress.

If you have any questions or recommendations, please let me know.

Thank you!

Brian

CIS D.C. REPORT

DECEMBER 2022

(117th Congress, 2nd Session)

This report summarizes the latest developments through December 2022 impacting cybersecurity in and around the nation's capital and beyond.
Items added since the previous report are in red.

TABLE OF CONTENTS

MULTIMEDIA

CYBERSECURITY QUARTERLY (by the Center for Internet Security)

- **Winter 2021:** CIS Cybersecurity Quarterly (Winter 2021)

PODCASTS

Center for Internet Security: Cybersecurity Where You Are

- Cybersecurity affects us all whether we are at home, managing a company, supporting clients, or even running a state or local government. Join the Center for Internet Security's Sean

Atkinson and Tony Sager as they discuss trends and threats, ways to implement controls and infrastructure, explore best practices, and interview experts in the industry.

- **Available on the following platforms:**
  - Apple
  - Spotify
  - Google

NASCIO

- The National Association of State Chief Information Officers podcast focuses on issues relating to their members.
- Link

TALKING CYBERSECURITY (The Tripwire Podcast)

- Link

SECURITY SLICE (also by Tripwire)

- Tripwire's Security Slice, hosted by Shelley Boose, is a longstanding favorite that tackles the biggest current issues and events, and interviews prominent guests for their take on the state of cybersecurity.
- Link

THE CYBERWIRE DAILY

- CyberWire Daily distills the day's critical cyber security news into a concise daily podcast. The daily podcast includes interviews with a wide spectrum of experts from industry, academia, and research organizations all over the world.
- Link

CYBER

- Motherboard's first-ever cybersecurity- and infosec-focused podcast. Each week, Ben, Lorenzo, Joseph Cox, and their sources walk through the stories they're working on and break down the biggest topics in the cybersecurity world.
- Link

CYBERSECURITY TODAY

- Updates on the latest cybersecurity threats to businesses, data breach disclosures, and how you can secure your firm in an increasingly risky time.
- Link

BRAKEING DOWN SECURITY

- Bryan Brake and Brian Boettcher host this popular weekly podcast featuring news, analysis and interviews with prominent InfoSec pros.
- Link

RISKY BUSINESS

- Risky Business is an Information Security news show hosted by journalist Patrick Gray. Gray has been running Risky Business since 2007 and keeps up with (and explains) the latest security concepts. Show notes are also provided with links for each story and concept covered.
- Link

SECURITY NOW!

- Security Now! is a weekly security column and podcast from Steve Gibson and Leo Laporte. Every week Gibson and Laporte catch up on the week's most interesting security events before embarking on a more in-depth discussion of the week's topic. Typical topics include security vulnerabilities, firewalls, virtual private networks (VPNs), password security and more.
- Link

FEDERAL ACTION

JUDICIAL DECISIONS:

ACA Connects v. Bonta (U.S. Court of Appeals for the 9th Circuit) (January 28, 2022):
Holding: California's net neutrality law is not preempted by federal law, allowing California to continue enforce it.
Opinion text: https://cdn.ca9.uscourts.gov/datastore/opinions/2022/01/28/21-15430.pdf

U.S. v. Soybel (U.S. Court of Appeals for the 9th Circuit) (September 8, 2021):
Holding: A user has no expectation of privacy in the IP address associated with their communications, and therefore a warrant is not needed for its acquisition from the providers of the communication services
Opinion text: Here

EXECUTIVE ACTION: AUTHORITIES & RESOURCES (REGULATIONS, EXECUTIVE ORDERS, STRATEGIES, POLICIES, REPORTS, WHITE PAPERS, ETC.)

RELEVANT PRESIDENTIAL EXECUTIVE ORDERS

EXECUTIVE ORDER 14086: Providing for New EU-U.S. Data Privacy Framework (Oct 7, 2022):

- On October 7, 2022, President Biden signed Executive Order (EO) 14086, "Enhancing Safeguards for United States Signals Intelligence Activities," which provides a new framework for legal data transfers between the European Union (EU) and the United States.
- **Link:** https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf
- **Analysis:** https://www.natlawreview.com/article/president-biden-issues-executive-order-providing-new-eu-us-data-privacy-framework

EXECUTIVE ORDER 14028: Improving the Nation's Cybersecurity (May 12, 2021)

- **Fact sheet:** FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks | The White House
- **Link:** Executive Order on Improving the Nation's Cybersecurity - The White House

EXECUTIVE ORDER 14017: America's Supply Chains (February 24, 2021)

- **Link:** Executive Order on America's Supply Chains | The White House

- **Final report on EO 14017** (June 2021): https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf

OTHER EXECUTIVE ACTION[1]

White House Hosts the Second International Counter Ransomware Initiative (CRI) Summit (Oct 31-Nov 1, 2022):

- **Fact sheet:** https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/
- **Joint statement:** https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/
- **Participating nations:** International Counter Ransomware Initiative (CRI)— Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Croatia, Czech Republic, Dominican Republic, Estonia, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Norway, Poland, Republic of Korea, Romania, Singapore, South Africa, Spain, Sweden, Switzerland, United Arab Emirates, United Kingdom, United States, and Ukraine, and the European Union.

FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers (Oct 31, 2022):

- FTC order against Chegg will require company to shore up its security against data breaches, and delete unnecessary data: https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-chegg-careless-security-exposed-personal-data-millions

CISA, FBI, MS-ISAC Issue Joint Guidance for Responding to DDoS attacks. (Oct 28, 2022):

- https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf

CISA Cross-Sector Performance Goals (Oct 27, 2022):

- https://www.cisa.gov/cpg
- Background:
  In July 2021, President Biden signed National Security Memorandum (NSM)-5: Improving Cybersecurity for Critical Infrastructure Control Systems. This memorandum required CISA, in coordination with the National Institute of Standards and Technology (NIST) and the

[1] "The President is free to revoke, modify, or supersede his own orders or those issued by a predecessor." Congressional Research Service, Executive Orders: Issuance, Modification, and Revocation, Vivian S. Chu & Todd Garvey at page 7 (April 16, 2014).

interagency community, to develop baseline cybersecurity goals that are consistent across all critical infrastructure sectors. This document contains the first iteration of the Cross-Sector Cybersecurity Performance Goals (CPGs). CISA, in coordination with NIST, will regularly update the goals, and starting in late 2022, CISA will begin working with Sector Risk Management Agencies (SRMAs) to build on this foundation to develop sector-specific goals.

FCC Proposes Rule Changes to Protect the Nation's Communications Systems from Cybersecurity Threats (recommending the CIS Critical Security Controls) (Oct 27, 2022):

- At its October 27, 2022, Open Meeting, the Federal Communications Commission adopted a Notice of Proposed Rulemaking proposing rule changes aimed at improving the operational readiness and security of the national Emergency Alert System and Wireless Emergency Alerts programs.
- The proposed rule would require that EAS participants and commercial mobile service providers who are a part of the WEA system to create and implement regularly updated cybersecurity risk management plans ("annually certify to having a cybersecurity risk management plan in place and to employ sufficient security measures to ensure the confidentiality, integrity and availability of their respective alerting systems").
- The FCC concludes that "[w]hile we believe there are numerous methods to satisfy this aspect of the requirement, **we have proposed to allow the requirement to be satisfied by providing evidence of the successful implementation of an established set of cybersecurity best practices, such as applicable Center for Internet Security (CIS) Critical Security Controls** or the Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Baseline" (emphasis added) (paragraph 66 at page 52).

TSA issues new cybersecurity requirements for passenger and freight railroad carriers (Oct 18, 2022):

- Security Directive: https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf
- The security directive requires that TSA-specified passenger and freight railroad carriers take action to prevent disruption and degradation to their infrastructure to achieve the following critical security outcomes:
  - Develop network segmentation policies and controls to ensure that the Operational Technology system can continue to safely operate in the event that an Information Technology system has been compromised and vice versa;
  - Create access control measures to secure and prevent unauthorized access to critical cyber systems;
  - Build continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect critical cyber system operations; and
  - Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on critical cyber systems in a timely manner using a risk-based methodology.
- Passenger and freight railroad carriers are required to:
  - Establish and execute a TSA-approved Cybersecurity Implementation Plan that describes the specific cybersecurity measures the passenger and freight rail carriers are utilizing to achieve the security outcomes set forth in the security directive.

- Establish a Cybersecurity Assessment Program to proactively test and regularly audit the effectiveness of cybersecurity measures and identify and resolve vulnerabilities within devices, networks, and systems.
- To view TSA's security directives and guidance documents, visit the TSA cybersecurity toolkit.

Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks (Oct 3, 2022):

- Binding Operational Directive: https://www.cisa.gov/binding-operational-directive-23-01

FERC: NOPR Regarding Incentivizing Advanced Cybersecurity Investment (Sep 22, 2022):

- On September 22, 2022, the Federal Energy Regulatory Commission (FERC) issued a Notice of Proposed Rulemaking (NOPR) that would revise the Commission's regulations to provide incentive-based rate treatments for the transmission of electric energy in interstate commerce and the sale of electric energy at wholesale in interstate commerce by utilities for the purpose of benefitting consumers by encouraging:
  - (1) investments by utilities in advanced cybersecurity technology; and
  - (2) participation by utilities in cybersecurity threat information sharing programs.
- https://www.ferc.gov/media/e-1-rm22-19-000

DHS CISA Strategic Plan 2023-2025 (Sep 2022):

- https://www.cisa.gov/sites/default/files/publications/StrategicPlan_20220912-V2_508c.pdf

TSA revises and reissues cybersecurity requirements for pipeline owners and operators (July 21, 2022):

- Although Security Directive Pipeline-2021-02C relaxes some of the overly rigid requirements and timelines established in earlier iterations, it continues to emphasize the need for companies to address potential threats to IT and OT system environments. Security Directive Pipeline-2021-02C also introduces several new requirements for TSA-specified owners and operators of critical pipelines and LNG facilities, including:
  - Establishing and executing a TSA-approved Cybersecurity Implementation Plan that specifically describes the cybersecurity measures being adopted by each owner or operator;
  - Developing a Cybersecurity Incident Response Plan that outlines the specific measures that owners and operators will take following a cybersecurity incident; and
  - Creating an annual Cybersecurity Assessment Program to proactively test and audit the effectiveness of any cybersecurity measures adopted by each owner or operator and identify and address vulnerabilities.
- Press release: https://www.tsa.gov/news/press/releases/2022/07/21/tsa-revises-and-reissues-cybersecurity-requirements-pipeline-owners
- Security Directive Pipeline-2021-02C: https://www.tsa.gov/sites/default/files/tsa_sd_pipeline-2021-02-july-21_2022.pdf

CISA Seeks Public Input Regarding the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (September 12, 2022)

- The RFI provides a "non-exhaustive" list of topics on which CISA seeks public input
- The public comment period will close on November 14th, 2022.

Cyber Safety Review Board Releases Report of its Review into Log4j Vulnerabilities and Response (July 14, 2022)

- The recommendations from the CSRB – an unprecedented public-private initiative that brings together government and industry leaders to review and assess significant cybersecurity events to better protect our nation's networks and infrastructure – address the continued risk posed by vulnerabilities discovered in late 2021 in the widely used Log4j open-source software library. These are among the most serious vulnerabilities discovered in recent years
- Cyber Safety Review Board Releases Report of its Review into Log4j Vulnerabilities and Response | Homeland Security

CISA Flags Election System Threats Ahead of Midterms (July 11, 2022)

- To help state and local officials with election security, CISA flagged key election threats including the danger of insider threats to election systems. Using Zero-Trust Architecture can help minimize the potential for insider threats.
- Supply Chain Risks to Election Infrastructure

CISA Instructs Federal Agencies to Address Microsoft Bug (July 5, 2022)

- Federal Agencies must apply Microsoft's June 2022 patch to protect against anonymous connection attempts to all Windows endpoints
- CISA instructs federal agencies to address Microsoft bug - FedScoop

CISA Releases Version 2.0 of its Cloud Security Technical Reference Architecture (June 23, 2022)

- The Cybersecurity and Infrastructure Security Agency (CISA) released the second version of its Cloud Security Technical Reference Architecture (TRA) guidance on June 22, 2022. "Section 3(c)(ii) of the Cyber EO provides that the purpose of the Cloud Security TRA is to outline recommended approaches to cloud migration and data protection and to provide guidance for agencies' secure migration to the cloud.. Contributing authors were CISA, the United States Digital Service and the Federal Risk and Authorization Management (FedRAMP) program."
- June 2022 Developments Under President Biden's Cybersecurity Executive Order | Inside Government Contracts

NIST Issues Guidance and Discussion Paper Regarding its Cybersecurity Internet of Things (IoT) Program (June 17, 2022)

- NIST took several steps in June 2022 in furtherance of its IoT Cybersecurity Program. First, NIST issued draft guidance for public comment on the baseline criteria for consumer IoT product labelling that it developed pursuant to the Cyber EO. Second, NIST issued for public comment a draft Discussion Essay titled "Ideas for the Future of IoT Cybersecurity at NIST: IoT Risk Identification Complexity", which sets forth various considerations and approaches for identifying and addressing risks for IoT devices.

- June 2022 Developments Under President Biden's Cybersecurity Executive Order | Inside Government Contracts

NIST Issues Final Draft Guidance on Engineering Secure Systems (June 7, 2022)

- "The updated draft publication provides a "renewed emphasis on the importance of systems engineering and viewing systems security engineering as a critical sub-discipline necessary to achieving trustworthy secure systems." The draft provides systems engineers with design principles and a methodology for developing trustworthy secure systems, it clarifies key systems engineering and systems security engineering terminology, and provides additional references to international standards and technical guidance to support the security aspects of the systems engineering process."
- June 2022 Developments Under President Biden's Cybersecurity Executive Order | Inside Government Contracts

NIST Releases Initial Summary Analysis of Responses to the Request for Information (RFI) on Evaluating and Improving the NIST Cybersecurity Framework (June 3, 2022)

- "The RFI sought information on the use of the NIST Cybersecurity Framework as well as recommendations to improve the effectiveness of the Framework and its alignment with other cybersecurity resources. The RFI also sought suggestions to inform other cybersecurity efforts at NIST, especially related to supply chain cybersecurity risks."
- NIST Cybersecurity RFI Summary Analysis
  "The comments will inform improvements to the CSF, as well as guide our efforts under the National Initiative for Improving Cybersecurity in Supply Chains (NIICS), our recently launched public-private partnership to build on our efforts in supply chain cybersecurity."
- Setting off on the Journey to the NIST Cybersecurity Framework (CSF) 2.0

U.S. Government Agencies' Progress and Challenges with Implementing the Cyber EO (May 12, 2022)

- "The Advanced Technology Academic Research Center ("ATARC") hosted a webinar with panelists representing multiple U.S. Government agencies and other stakeholders to commemorate the one year anniversary of the Cyber EO. Some of the agencies represented included the Department of Homeland Security ("DHS"), the U.S. Army, and TRANSCOM. The agency representatives expressed uniform support for implementing the Cyber EO, discussed the significant progress that their respective agencies have made in cybersecurity, and described areas for improvement."
- May 2022 Developments Under President Biden's Cybersecurity Executive Order: One Year Anniversary Update | Inside Government Contracts

NIST Issues New Guidance for Cybersecurity Supply Chain Risk Management (May 5, 2022)

- "NIST released the final version of Special Publication 800-161, Revision 1, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." NIST removed from SP 800-161 several Cyber EO-directed guidance documents that had previously appeared in Appendix F to earlier drafts of that document and moved these and other EO-directed software supply chain security documents to a NIST website dedicated to EO documents. The

documents placed on NIST's EO website include both existing standards, tools, and recommended practices and evolving standards, tools, and practices."

- May 2022 Developments Under President Biden's Cybersecurity Executive Order: One Year Anniversary Update | Inside Government Contracts

NIST Seeks Public Comment on Safeguarding 5G Cybersecurity (April 26, 2022)

- "Special Publication 1800-33B is meant to assist organizations with the challenge of securing technologies that use 5G while the development and usage of these technologies remains ongoing. The draft publication provides a sample solution for addressing challenges unique to 5G cybersecurity, which incorporates a "risk analysis." The solution will provide "actionable and prescriptive guidance" for how to use "standards and recommended practices" to safeguard 5G technologies under various scenarios. NIST expects to release at least one updated draft for public comment."
- April 2022 Developments Under President Biden's Cybersecurity Executive Order | Inside Government Contracts

NIST Updates Guidance for Securing Operational Technology (April 26, 2022)

- "On April 26, 2022, NIST released Special Publication 800-82 Revision 3, "Guide to Operational Technology (OT) Security," the third iteration of NIST's guidance on securing OT. The publication supplies guidance for how to implement secure OT while simultaneously "addressing OT's unique performance, reliability, and safety requirements." The third revision surveys "methods and techniques" for protecting OT systems. Specifically, the publication analyzes typical threats and vulnerabilities associated with OT systems and advocates for certain "security countermeasures" to combat the relevant OT risks."
- April 2022 Developments Under President Biden's Cybersecurity Executive Order | Inside Government Contracts

NCCoE Releases Three Publications on Trusted Cloud and Hardware-Enabled Security (April 20, 2022)

- "NIST Special Publication (SP) 1800-19 presents an example of a trusted hybrid cloud solution that demonstrates how trusted compute pools leveraging hardware roots of trust can provide the necessary security capabilities for cloud workloads in addition to protecting the virtualization and application layers. NIST IR 8320B explains an approach based on hardware-enabled security techniques and technologies for safeguarding container deployments in multi-tenant cloud environments. NIST IR 8320C presents an approach for overcoming security challenges associated with creating, managing, and protecting machine identities, such as cryptographic keys, throughout their lifecycle."
- Three Publications on Trusted Cloud and Hardware-Enabled Security | CSRC

CISA Releases Secure Cloud Business Applications Reference Documents (April 19, 2022)

- "As a part of the Secure Cloud Business Applications project, the Cybersecurity and Infrastructure Security Agency (CISA) released two publications in April 2022: Secure Cloud Business Applications (SCuBA) Technical Reference Architecture (TRA) and Extensible Visibility Reference Framework (eVRF) Program Guidebook. Cloud Service Providers (CSPs) for incorporation into agency modernization efforts. The SCuBA was established to develop

effective, modern, and manageable security configurations to help secure agency information assets stored within cloud environments. To implement the program, CISA released the SCuBA TRA, which is a security guide for agencies to use to adopt technology for cloud deployment, adaptable solutions, secure architecture, and zero trust frameworks."

- April 2022 Developments Under President Biden's Cybersecurity Executive Order | Inside Government Contracts

The Government Moves Forward Towards Proposing Federal Acquisition Regulation Updates (April 13, 2022):

- "Sections 2(b)-(c) of the Cyber EO require the Department of Homeland Security (DHS) to recommend to the FAR Council contract language and requirements for IT and OT service providers regarding reporting of cyber incidents and related information preservation requirements. Section 2(g)(i) of the Cyber EO requires DHS to recommend to the FAR Council contract language that identifies the nature of cyber incidents that require reporting by federal contractors. The FAR Council opened Federal Acquisition Regulation (FAR) Case No. 2021-017 to consider the recommended contract language and requirements and to develop proposed FAR amendments based thereon."
- April 2022 Developments Under President Biden's Cybersecurity Executive Order | Inside Government Contracts

State Department Announces Establishment of the Bureau of Cyberspace and Digital Policy (April 4, 2022):

- Announcement of establishment of office (April 4, 2022): https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/
- On Oct 27, 2021, Secretary of State Blinken formally announced the creation of the Bureau.
- Webpage: https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/

President Releases FY2023 Federal Budget (Mar 28, 2022):

- Information Technology & Cybersecurity Funding: https://www.whitehouse.gov/wp-content/uploads/2022/03/ap_16_it_fy2023.pdf
- Main budget page: https://www.whitehouse.gov/omb/budget/

Federal Government Indicts Russian Government Employees Who Targeted U.S. Energy Sector, Issues Advisory (March 24, 2022):

- On March 24, 2022, the U.S. Department of Justice revealed indictments charging four Russian government employees involved in targeting American critical infrastructure in the energy sector.
- Also on March 24, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE) jointly published a Cybersecurity Advisory (CSA) relating to those efforts.

President Bident Reiterating Warnings based on evolving intelligence that the Russian Government is exploring options for potential cyberattacks; urges private sector partners to harden cyber defenses, information sharing, public-private partnerships (March 21, 2022):

- https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

NIST Issues Guidance for Securing Industrial Control Systems (March 17, 2022)

- "On March 17, 2022, NIST's National Cybersecurity Center of Excellence issued Special Publication 1800-10, "Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector." This publication is intended to guide manufacturers in mitigating risks to their operational technology (OT) systems as they integrate those systems with IT systems to boost productivity and gain efficiencies."
- March 2022 Developments Under President Biden's Cybersecurity Executive Order | Inside Government Contracts

Security & Exchange Commission Regulatory Actions (Feb and Mar, 2022):

- On March 9, 2022, the Security & Exchange Commission (SEC) proposing new rules to standardize disclosures by publicly traded companies related to cybersecurity risk management, strategy, governance, and incident reporting. The new rules, if adopted, would compel public companies to report cyberattacks within four days of discovering the incident. The proposed rules would also require that publicly traded companies periodically disclose their policies for managing and identifying cybersecurity risk, management's role in managing cybersecurity, and the board of directors' oversight role and cybersecurity expertise.
  - The official statement by SEC Chair Gensler (Mar 9, 2022): https://www.sec.gov/news/statement/gensler-cybersecurity-20220309utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202
- On February 9, 2022, the SEC on February 9 acted to require advisers and funds to adopt cybersecurity protections including: a risk assessment; user security and access controls; information protection and monitoring to protect systems from unauthorized use; and an annual written review of cybersecurity risks and policies (which would require review by a board of directors).
  - Official SEC press release (Feb 9, 2022): https://www.sec.gov/news/press-release/2022-20

CISA Issues Paper On Integrating Zero Trust Principles Into Federal Mobile Device Security at Enterprise Level (March 7, 2022)

- "Section 3 of the Cyber EO requires agencies to modernize their approach to cybersecurity, including by advancing towards Zero Trust Architecture. Pursuant to that section, DHS's Cybersecurity and Infrastructure Security Agency (CISA) issued a draft paper on March 7, 2022 to guide Government agencies in applying Zero Trust principles to mobile devices at the enterprise level. The draft paper presents architectural frameworks, principles, and capabilities for attaining Zero Trust, and maps mobile security approaches into these

frameworks, principles, and capabilities that an agency can use to align its current mobile security capabilities with a Zero Trust approach"

- March 2022 Developments Under President Biden's Cybersecurity Executive Order | Inside Government Contracts

OMB Tells Agencies to Begin Implementing Secure Software Acquisition and Development Practices (March 7, 2022)

- "On March 7, 2022, OMB issued a document entitled "Implementation of Software Supply Chain Security Guidance under Executive Order (EO) 14028 Section 4(k)." The document states that "Agencies should begin integrating the NIST Software Supply Chain Security Guidance into their existing software lifecycle management and acquisition practices to ensure purchase of only secure and trustworthy products." The document notes that "[f]ollowing SSDF practices should help software producers reduce the number of vulnerabilities in released software, reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent recurrence."
- March 2022 Developments Under President Biden's Cybersecurity Executive Order | Inside Government Contracts

National Security Agency (NSA) Cybersecurity Technical Report Network Infrastructure Security Guidance (Mar 1, 2022):

- The NSA's report highlights the importance of zero trust principles for network security and covers specific steps network administrators should take to keep their infrastructure safe from compromise
- Document:https://media.defense.gov/2022/Mar/01/2002947139/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDANCE_20220301.PDF

NIST Issues Criteria for Cybersecurity Labelling of Consumer Software and Consumer Internet-of-Things Products for Pilot Programs (February 4. 2022):

- "The Software Labeling Criteria identify the key elements for a potential consumer software cybersecurity labeling program that would be established by an organization other than NIST. The purposes of such a program would be to "aid consumers in their software selection decisions by enabling comparisons among products and educating them about software security considerations," and potentially also "encourage [software] providers to consider cybersecurity aspects of their software and ways to achieve greater trust and confidence in the software, and, ultimately, to improve the management of related cybersecurity risks." The Software Labeling Criteria recommend considerations for three key aspects of a potential consumer software cybersecurity labeling program. These key aspects are: (1) Baseline Product Criteria, (2) Labeling, and (3) Conformity Assessments."
- February 2022 Developments Under President Biden's Cybersecurity Executive Order | Inside Government Contracts

NIST Publishes Guidance to Federal Agencies on Practices to Enhance Supply Chain Security When Procuring Software (February 4, 2022):

- "Section 4(e) of the Cyber EO requires the National Institute of Standards and Technology (NIST) to publish guidelines on practices for software supply security for use by U.S. Government acquisition and procurement officials. Section 4(k) of the EO requires the Office of Management and Budget, within 30 days of the publication of this guidance (or March 4, 2022), to "take appropriate steps to require that agencies comply with such guidelines with respect to software procured after the date of the EO. Section 4(n) of the EO states that within one year of the date of the EO (or May 12, 2023), the Secretary of Homeland Security…shall recommend to the FAR Council contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, any requirements issued pursuant to subsections (g) through (k) of this section."
- February 2022 Developments Under President Biden's Cybersecurity Executive Order | Inside Government Contracts

Establishment of Cyber Safety Review Board (February 3, 2022):

- "The Board was established by the Department of Homeland Security on February 3, 2022, to review "threat activity, vulnerabilities, mitigation activities, and agency responses" after "significant cyber incidents." and is composed of federal government and private sector leaders. The Board's first task, anticipated this summer, will focus on the widespread Log4j vulnerabilities."
- DHS Launches First-Ever Cyber Safety Review Board | Homeland Security

Federal Zero Trust Architecture Strategy (January 26, 2022):

- "This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government."
- M-22-09 Federal Zero Trust Strategy

Federal Energy Regulatory Commission Proposed Rules [NPRM] Internal Network Security Monitoring for High & Medium Impact Bulk Electric System Cyber Systems (January 27, 2022):

- https://www.govinfo.gov/content/pkg/FR-2022-01-27/html/2022-01537.htm

Election Infrastructure Government Coordinating Council and the Subsector Coordinating Council's (SCC) Joint Mis/Disinformation Working Group release two guides (Jan 27, 2022):

- Link here to *Rumor Control Page Start-Up Guide*
- Link here to *Mis-, Dis, and Malinformation (MDM) Planning and Incident Response Guide for Election Officials*

CISA, FBI, and NSA Release Cybersecurity Advisory on Russian Cyber Threats to U.S. Critical Infrastructure (Jan 11, 2022):

- Link to Advisory text here.

FTC Warns Companies to Remediate Log4j Security Vulnerability (Jan 4, 2022):

- "The FTC intends to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities in the future."
- Link to FTC announcement here

CISA Issues Emergency Directive 22-02 to Mitigate Apache LOG4J Vulnerability (Dec 17, 2021):

- On December 17, 2021, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive requiring all civilian Federal government agencies to protect against it by December 23.
- Emergency Directive 22-02: here.

TSA Announces Two Security Directives Regarding Rail (Dec 2, 2021):

- On Dec 2, 2021, the Transportation Security Administration ("TSA") announced that it issued two security directives requiring higher-risk freight railroads, passenger rail and rail transit to implement measures to strengthen cybersecurity within the sector. Key among the requirements in the security directives is a requirement to report cybersecurity incidents to CISA within 24 hours. The directives also require these rail transportation owners and operators to (1) designate a cybersecurity coordinator, (2) develop and implement a cybersecurity incident response plan, and (3) conduct a cybersecurity vulnerability assessment to identify potential gaps or vulnerabilities in their systems.
- TSA press release with link to directives: DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators

GAO Warns That U.S. Critical Infrastructure is "In Jeopardy" If the Government Fails to Take Action (Dec 2, 2021):

- GAO report: GAO-22-105530, CYBERSECURITY: Federal Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure

Department of Commerce Releases Notice of Proposed Rulemaking Regarding Amendments to the Information and Communications Technology and Services ("ICTS") Supply Chain Interim Final Rule (Nov 26, 2021):

- Federal Register Notice: https://www.federalregister.gov/documents/2021/11/26/2021-25329/securing-the-information-and-communications-technology-and-services-supply-chain-connected-software

CISA's Binding Operational Directive 22-01 - Reducing the Significant Risk of Known Exploited Vulnerabilities (Nov 3, 2021):

- CISA binding operational directive 22-01: Binding Operational Directive 22-01 | CISA

FTC Strengthens Security Safeguards for Consumer Financial Information (Oct 27, 2021):

- On October 27, 2021, Director of the Federal Trade Commission's (FTC) Bureau of Consumer Protection Samuel Levine announced that the FTC has updated its Safeguards Rule.
- Press Release, Federal Trade Commission (includes links): https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial
- FTC final rule in the Federal Register (Dec 9, 2021): Federal Register :: Standards for Safeguarding Customer Information

U.S. Department of Commerce publishes new export controls on cybersecurity (Oct 21, 2021):

- On October 21, 2021, the U.S. Department of Commerce's Bureau of Industry and Security (BIS), published new export controls on certain cybersecurity tools that could be used by foreign malign interests. The interim final rule takes effect on January 19, 2022.
- Federal Register notice here:

DOJ Announces New Civil Cyber-Fraud Initiative (Oct 6, 2021):

- Deputy Attorney General press release: here

Critical Infrastructure Controls Systems Cybersecurity Performance Goals and Objectives (September 21, 2021):

- CISA webpage: Control Systems Goals and Objectives

U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments:

- Advisory text here (September 21, 2021): Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments

Warning from FTC Regarding Scope of Health Breach Notification Rule (September 15, 2021):

- FTC policy statement: Federal Trade Commission On Breaches by Health Apps and Other Connected Devices September 15, 2021 In recognition of the prolife

NIST Draft Cybersecurity Framework Profile for Ransomware Risk Management (September 2021):

- Text
  - Citing the joint CISA MS-ISAC Ransomware Guide
  - See, esp, the MS-ISAC resources cited at pages 5, 8, 10, 11.

SEC Actions Up the Ante for Cybersecurity Disclosures

- SEC press release (August 30, 2021): SEC Announces Three Actions Charging Deficient Cybersecurity Procedures

Biden Administration Announces Private-Sector Initiatives to Bolster Cybersecurity (August 25, 2021):

- **Fact Sheet:** FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity | The White House

The Joint Cyber Defense Collaborative (August 5, 2021):

- Cybersecurity and Infrastructure Security Agency (CISA) Director Easterly announced the creation of the Joint Cyber Defense Collaborative (JCDC) today, a new agency effort to lead the development of cyber defense operations plans, and to execute those plans in coordination with partners from the federal interagency, private sector, and state, local, tribal, territorial (SLTT) government stakeholders to drive down risk before an incident and to unify defensive actions should an incident occur.
- Joint Cyber Defense Collaborative

Fact Sheet: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure (July 28, 2021):

- Text

National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (July 28, 2021)

- President Joseph Biden's fifth national security memorandum launched a new public-private initiative that creates performance controls for cybersecurity at America's most critical companies, including water treatment and electrical power plants).
- Text

CISA Zero Trust Maturity Model (pre-decisional draft) (June 2021):

- "[D]esigned to be a stopgap solution to support Federal Civilian Executive Branch (FCEB) agencies in designing their zero trust architecture (ZTA) implementation plans in accordance with Section 3,b,ii of Executive Order 14028, *Improving the Nation's Cybersecurity*."
- CISA Zero Trust Maturity Model

The President's Industrial Control System Cybersecurity (ICS) Initiative (April 2021):

- The national security memo of July 28, 2021, states that "the President's ICS Initiative [is] a voluntary, collaborative effort between the federal government and the critical infrastructure community to facilitate the deployment of technology and systems that provide threat visibility, indicators, detections, and warnings.
- The Initiative began in mid-April with an Electricity Subsector pilot, and already over 150 electricity utilities representing almost 90 million residential customers are either deploying or

have agreed to deploy control system cybersecurity technologies. The action plan for natural gas pipelines is underway, and additional initiatives for other sectors will follow later this year.

Department of Energy Updated Cybersecurity Capability Maturity Model (July 21, 2021):

- The Department of Energy released Version 2.0 of the Cybersecurity Capability Maturity Model (C2M2) that includes information about developing threats like ransomware and supply chain disruptions. The model helps businesses and organizations assess and improve their cybersecurity capabilities. The original C2M2 model was released in 2012, and the update is built on input from over 70 energy companies and more than 140 cyber experts.
- Press release here.
- Link to C2M2: Cybersecurity Capability Maturity Model (C2M2)

TSA's Second Security Directive for Pipeline Owners and Operators (July 20, 2021):

The U.S. Department of Homeland Security's Transportation Security Administration (TSA) announced a second Security Directive for critical pipeline owners and operators. This second Security Directive will require owners and operators of pipelines that transport hazardous liquids and natural gas to implement a number of urgently needed protections, including:

- Implementing specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems within prescribed timeframes.
- Developing and implementing a cybersecurity contingency and recovery plan.
- Conducting an annual cybersecurity architecture design review.
- Announcement: DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators

TSA's First Security Directive for Pipeline Owners and Operators (May 27, 2021):

Following the ransomware attack on a major petroleum pipeline in May 2021, TSA issued an initial Security Directive requiring critical pipeline owners and operators to report cybersecurity incidents, designate a Cybersecurity Coordinator, and conduct a review of their current cybersecurity practices. Specifically, the Directive requires owners and operators of critical pipelines to:

- Immediately confirm receipt of the Directive by sending an email to the TSA;
- By June 4, 2021, designate and provide contact information to the TSA for one primary and at least one alternate Cybersecurity Coordinator, who must be available 24 hours a day, 7 days a week to liaise with the TSA and the Cybersecurity and Infrastructure Security Administration (CISA) regarding incidents and cybersecurity-related activities and communications;
- Assess the pipeline's existing security measures against Section 7 of the TSA's 2018 *Pipeline Security Guidelines*, identify any gaps, develop remediation measures, and submit a TSA assessment form to the TSA and the CISA by June 27, 2021; and
- Notify CISA of "cybersecurity incidents" via the agency's Reporting System form or by calling a CISA hotline as soon as practicable, but no later than 12 hours after an incident is identified. The Directive defines a "cybersecurity incident" broadly, including events that are "under investigation as a possible cybersecurity incident without successful determination of the event's root cause or nature" that may affect the integrity, confidentiality, or availability of resources.

- If an owner or operator is unable to implement these requirements, the Directive instructs them to immediately notify the TSA in writing, seek TSA approval of alternative cybersecurity measures, and provide the rationale for those alternative cybersecurity measures.
- **Announcement:** DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators | Homeland Security
- **Text of Security Directive:** number subject effective date expiration date cancels and supersedes applicability authority location security directive

CARBIS BAY G7 SUMMIT COMMUNIQUÉ:

- **Released:** June 13, 2021
- **Link:** (most relevant cyber provisions at paragraphs 31-34): https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/carbis-bay-g7-summit-communique/

SELECT PREVIOUS EXECUTIVE ACTION

PREVIOUS EXECUTIVE ORDERS

EXECUTIVE ORDER 13870: America's Cybersecurity Workforce

- **Released:** May 2, 2019
- Link to E.O:

EXECUTIVE ORDER 13848: Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election

- **Released:** September 12, 2018
- **Overview:** President Trump signed an executive order placing sanctions on any foreign company, individual, or government that meddles in U.S. elections. The executive order mandates an assessment conducted by the Director of National Intelligence (with consultation of the appropriate agencies) to occur no later than 45 days after the election for any evidence of foreign interference. If there is interference, those involved will be placed with a sanction and possible other punishments from the Department of Treasury. The report of the assessment results will be shared with the appropriate parties.
- **Key Actions/Aims:**
  - Authorizes the President to sanction bodies meddling in US elections.
  - DNI to author reports after federal elections presenting any evidence of foreign interference.
- Link to E.O:
- Executive Order 13848: Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election (open html

EXECUTIVE ORDER 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

- **Released:** May 11, 2017
- Link to E.O:

NATIONAL STRATEGIES AND FRAMEWORKS

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC):

- CMMC 2.0 (Nov 4, 2021): OUSD A&S - Cybersecurity Maturity Model Certification (CMMC)
- DoD site on CMMC model v1.0 (Controls mentioned but focused on UK & Australia) (March 18, 2020): Link
- Pentagon Announces Final Version of Cyber Standards for Contractors (CMMC), article w link to 1.0 (Jan 31, 2020): Link to Article

CISA #PROTECT2020 STRATEGIC PLAN

- **Released on:** February 7, 2020
- **Overview:**
  - This report from the Cybersecurity and Infrastructure Security Agency, released the day after the GAO criticized the agency (see below) for its failure to publish a comprehensive plan regarding the 2020 election, provides insight into the CISA's #Protect2020 initiative to combat cybersecurity concerns during the 2020 election cycle.
  - The CISA also outlines their actions to work with state election officials, local jurisdictions, and independent actors to ensure that each has access to the resources necessary to guard the American electorate from interference by hostile entities.
- **Key Action/Aim:**
  - Coming on the heels of the GAO's criticism, this report seeks to educate the public on the steps the CISA is taking to mitigate the cybersecurity risks America faces as it goes into the 2020 election cycle.
- Link to Strategic Plan

TRUMP ADMINISTRATION'S NATIONAL CYBER STRATEGY

- **Released on:** September 20, 2018
- **Overview:** The strategy outlines the federal government's efforts to strengthen the United States' cybersecurity and to prevent cyber attacks. Efforts include cyber offensive operations against foreign interferences and are mainly using a risk management approach. The new strategy is a mix of new proposals and work from previous administrations. In the strategy, there is no mention of cyber offensive operations but it did state that the administration will use all entrustment of their power to punish those who interfere in the U.S. elections.
- **Key Actions/Aims:**
  - Ensuring the Joint Force can achieve its mission in a contested cyberspace environment.
  - Strengthening the Joint Force by conducting cyberspace operations that enhance U.S.

military advantages.
    - Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident.
    - Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks.
    - Expanding DoD cyber cooperation with interagency, industry, and international partners.
- Complete Strategy, Factsheet, and Summary

DEPARTMENT OF ENERGY: CYBERSECURITY STRATEGY (2018-2020)

- **Released on:** June 12, 2018
- **Overview:** The latest iteration of DoE's Cybersecurity Strategy introduces a multiyear plan to reduce the risk of energy disruptions caused by cyber incidents. With the fallout and risk of cyber incidents today places greater emphasis on dynamic cyberdefense strategies that leverages and engages stakeholders at all levels. DoE - "Anticipating and reacting to the latest cyber threat is a ceaseless endeavor that requires ever more resources and manpower. This approach to cybersecurity is not efficient, effective, nor sustainable in light of escalating cyber threat capabilities. We must recognize today's realities: resources are limited, and cyber threats continue to outpace our best defenses. To gain the upper hand, we need to pursue disruptive changes in cyber risk management practices."
- **Key Actions/Aims:**
    - Share cyber threats data in real-time
    - Mitigate threats by evaluating and expediting analysis of data.
    - Develop common identity services to more efficient collaboration and visibility.
    - Partner with other agencies to establish better cyber security practices.
    - Implement Continuous Diagnostics and Mitigation (CDM) tools to provide better cyber security solutions.
    - Enhance the Integrated Joint Cybersecurity Coordination Center (iJC3) to secure the ability to remain a step ahead of adversaries.
    - To create a system that connects all DOE employees to the cloud system.
    - Implement a cyber risk management framework to improve the responses to the evolving threats.
    - Continue to mitigate, identify, and investigate cyber threats.
- Link to Strategy

DEPARTMENT OF HOMELAND SECURITY: CYBERSECURITY STRATEGY (MAY 2018)

- **Released on:** May 15, 2018
- **Overview:** Department of Homeland released a 2018 Cybersecurity Strategy plan with five main actions the department will take to secure our nation's cybersecurity. In the report, the Department predicted that by 2020 more than 20 billion devices would be connected to the internet. The creation report was mandated by Congress to be released by March 2017 but was delayed until now.
- **Key Actions/ Aims:**
    - To better identify digital risks
    - To reduce threats and vulnerabilities

- To mitigate the consequences of cyber attacks
- To make infrastructure more resilient
- To improve DHS's management of its cyber portfolio

- Link to Strategy, Summary, Fact Sheet

REPORTS, WHITE PAPERS, & OTHER RESOURCES

CRS REPORT: Federal Cybersecurity: Background and Issues for Congress (September 29, 2021):

- **Link:** Federal Cybersecurity: Background and Issues for Congress

NATIONAL SECURITY AGENCY, CYBERSECURITY INFORMATION SHEET: Securing Wireless Devices in Public Settings (July 2021):

- **Link:** Securing Wireless Devices in Public Settings

HOUSE ARMED SERVICES COMMITTEE SUPPLY CHAIN TASK FORCE REPORT:

- **Released:** July 22, 2021
- **Link:** https://armedservices.house.gov/_cache/files/e/5/e5b9a98f-9923-47f6-a5b5-ccf77ebbb441/7E26814EA08F7F701B16D4C5FA37F043.defense-critical-supply-chain-task-force-report.pdf
- **Committee press release:** Defense Critical Supply Chain Task Force Releases Final Report

CRS REPORT: Department of Justice Efforts to Counter Ransomware (July 2021):

- **Link:** https://crsreports.congress.gov/product/pdf/IN/IN11698

FBI 2020 INTERNET CRIME REPORT (2021):

- **Link:** 2020 Internet Crime Report - IC3
- **Article:**https://www.alstonprivacy.com/fbi-releases-ic3-2020-internet-crime-report-showing-record-increase-in-cybercrime/

FTC PRIVACY & DATA PROTECTION

- Federal Trade Commission, Privacy & Data Security, Update: 2019 (March 2020)
- Link to Report

DOJ REPORT ON CHINESE INVOLVEMENT IN EQUIFAX BREACH

- DOJ Press Release that includes a link to the indictment (Feb 10, 2020)
- Link to Press Release

GAO: ELECTION SECURITY: DHS PLANS ARE URGENTLY NEEDED TO ADDRESS IDENTIFIED CHALLENGES BEFORE THE 2020 ELECTIONS

- **Released on:** February 6, 2020

- **Overview:**
  - This report from the Government Accountability Office alleges that the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency in particular are not prepared to properly defend the 2020 elections from cyber threats.
  - The report also details the unease at the GAO that the CISA has not adequately addressed security concerns previously identified publicly.
- **Key Action/Aim:**
  - This report brought attention to the CISA's failure to release their strategy to combat whatever cybersecurity threats may arise with February marking the beginning of the primaries. The CISA would release their #Protect2020 strategic plan (see above) the day after this report.
- Link to Report

REPORT OF THE SELECT COMMITTEE ON INTELLIGENCE, UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION VOLUME 3: U.S. GOVERNMENT RESPONSE TO RUSSIA ACTIVITIES

- **Released on:** February 6, 2020
- **Key Action/Aim:**
  - This report is a part of an ongoing effort to understand Russian interference in the 2016 presidential election in the hopes of developing safeguards to combat similar efforts in the future.
- Link to Report

THE PRESIDENT'S NATIONAL INFRASTRUCTURE ADVISORY COUNCIL: TRANSFORMING THE U.S. CYBER THREAT PARTNERSHIP

- **Released on:** December 2019
- **Overview:**
  - This report highlights the need for dramatic changes to improve the United States' defensive cybersecurity capabilities and provides recommendations to achieve this goal while emphasizing the urgency with which changes need to be made.
  - The NIAC recommends an Executive Order establishing the Federal Cybersecurity Commission (FCSC) to protect key cyber systems and streamline regulatory authorities.
- **Key Action/Aim:**
  - Establishment of the FCSC
  - This report also underscores the need to analyze and evaluate the government's ability to regulate cybersecurity issues as the first step towards the modernization of the country's legal authorities.
  - Security of the supply chain of cyber components including hardware and software is an essential part of any comprehensive cybersecurity strategy.
- Link to Report

HOMELAND SECURITY ADVISORY COUNCIL: INTERIM REPORT OF THE COUNTERING FOREIGN INFLUENCE SUBCOMMITTEE (May 21, 2019):

- Link to Report

HOMELAND SECURITY ADVISORY COUNCIL: INTERIM REPORT OF THE STATE, LOCAL, TRIBAL AND TERRITORIAL CYBERSECURITY SUBCOMMITTEE (May 21, 2019):

- **Released on:** May 21, 2019
- **Overview:**
  - In this report, the State, Local, Tribal and Territorial Cybersecurity Subcommittee puts forth a number of recommendations with the objective of improving the capabilities of entities outside of the federal government to combat cybersecurity threats. The report makes clear the important role of SLTT organizations in the United States' cybersecurity strategy.
- **Key Actions/Aims:**
  - Provide more cybersecurity resources to SLTT groups including employee training and funding in the form of grants.
  - Facilitate cooperation between groups and using successful organizations as models for underperforming counterparts in other localities.
  - Empower state and local election officials to combat threats
  - Put in place a strategy to mitigate the risks to public safety and critical infrastructure associated with the proliferation of smart cities.
- Link to Report

FTC, DATA BREACH RESPONSE: A GUIDE FOR BUSINESS (May 2019):

- Link to Guide

INTERAGENCY REPORT ON THE STATUS OF INTERNATIONAL CYBER SECURITY STANDARDIZATION FOR THE INTERNET OF THINGS (IoT)

- **Released on:** February 2018
- **Overview:** This report by the Interagency International Cybersecurity Standardization Working Group (IICS WG) is intended for member agencies to assist them in their standards planning and to help to coordinate U.S. government participation in international cybersecurity standardization for IoT. Other organizations may also find this useful in their planning.
- **Key Actions/Aims:**
  - Demonstrate the basic protections afforded by adhering to best practices.
  - Understand the cybersecurity implications of increasing connectedness in society.
- Link to Report

DHS CISA CYBER RESOURCE HUB: https://www.cisa.gov/cyber-resource-hub

CONGRESSIONAL BILLS (117th Congress)

OF SPECIAL INTEREST TO CIS

S. 2520, State and Local Government Cybersecurity Act of 2021
Overview: This bill codifies the functions of the MS-ISAC.
Committee Report: S. Rept. 117-42
Status: Signed by the President and became Public Law No: 117-150 (June 21, 2022).
Link: S.2520 - 117th Congress (2021-2022): State and Local Government Cybersecurity Act of 2021 | Congress.gov | Library of Congress

S. 3894, Advancing Cybersecurity Through Continuous Diagnostics and Mitigation Act
Overview: To amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to establish a continuous diagnostics and mitigation program in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes.
The use of the CIS Critical Security Controls is to be used as a factor to permit an SLTT government to participate in a CDM pilot program.
Status: 03/22/2022 Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
Link: S.3894 - 117th Congress (2021-2022): Advancing Cybersecurity Through Continuous Diagnostics and Mitigation Act

H.R. 4005, Enhancing K-12 Cybersecurity Act
Overview: CIS provided technical assistance to this bill that would create a school cybersecurity information exchange, a cybersecurity incident registry, and a K-12 cybersecurity technology improvement program.
Status: Introduced on 06/17/2021 and referred to both the Committee on Homeland Security, and in addition to the Committee on Education and Labor.
Link: HR4005 - 117th Congress (2021-2022): Enhancing K-12 Cybersecurity Act

H.R. 4691, K-12 Cybersecurity Act
Overview: CIS provided technical assistance to this bill that directs CISA to collaborate with teachers, school administrators, other Federal agencies, and private sector organizations to conduct a study of the cybersecurity risks facing K-12 educational institutions.
Status: This bill is identical to S. 1917, which became law on October 8, 2021.
Link: HR4691 - 117th Congress (2021-2022): K-12 Cybersecurity Act of 2021 | Congress.gov | Library of Congress

H.R. 4910, State Cyber Resiliency Act
Overview: This bill would have benefited our MS-ISAC members by establishing the State Cyber Resiliency Grant Program to assist state, local, and tribal governments in preventing, preparing for,

protecting against, and responding to cyber threats. A version of this bill was passed in H.R. 3684, Infrastructure Investment and Jobs Act (IIJA).
Status: Introduced (August 4, 2021).
Link: 117th Congress (2021-2022): State Cyber Resiliency Act

S. 2585, State and Local Cybersecurity Grant Program

Overview: This bill would create a state and local cybersecurity grant program at DHS. In particular, it would:

- Authorize $1 billion over four years to enable state, local, and tribal governments to prioritize cybersecurity investments.
- Require states to distribute at least 80 percent of funds to local governments, including 25 percent of funds to rural areas.
- Require states and tribes to submit to CISA a cybersecurity plan, which outlines how the state or tribe will improve its cybersecurity.
- This plan must be approved by the state or tribes' Cybersecurity Planning Committee, which includes representatives from local entities that will help bring more diverse perspectives to the table and improve coordination.

Link: S.2585 - 117th Congress (2021-2022): State and Local Cybersecurity Improvement Act
Status: A version of this bill was incorporated in the Senate-passed infrastructure bill and later incorporated into H.R. 3684, the Infrastructure Investment and Jobs Act (IIJA) and signed into law on November 15, 2021: 117th Congress (2021-2022): Infrastructure Investment and Jobs Act.

SIGNED INTO LAW

H.R. 3684, Infrastructure Investment and Jobs Act (IIJA)

Overview: This bill provides new funding for infrastructure projects, including significant investment in cybersecurity.
Selected cyber provisions: Good overview from Rapid 7:
https://www.rapid7.com/blog/post/2021/08/31/cybersecurity-in-the-infrastructure-bill/
Status: Became Public Law No: 117-58 (Nov 15, 2021)
Link: 117th Congress (2021-2022): Infrastructure Investment and Jobs Act

H.R. 4346, CHIPS Act of 2022

Overview: This bill provides funds to support the domestic production of semiconductors and authorizes various programs and activities of the federal science agencies. The bill:

- provides funding for wireless supply chain innovation;
- establishes an advanced manufacturing investment tax credit;
- requires a research and development program to expand theoretical and fundamental knowledge relevant to understanding nuclear materials and matter for the benefit of commerce, medicine, and national security;
- establishes the Carbon Materials Science Initiative;
- establishes the Quantum User Expansion for Science and Technology program;
- establishes the Carbon Sequestration Research and Geologic Computational Science Initiative;

- requires a research program to improve the understanding of the fundamental properties of the universe, including the nature of space and time;
- requires research activities on the nature of the primary contents of the universe, including the nature of dark energy and dark matter;
- provides for the construction of an Electron Ion Collider;
- establishes a high intensity laser research initiative;
- establishes a Center for Greenhouse Gas Measurements, Standards, and Information;
- establishes a program for measurement research to support biometric identification systems, including facial recognition systems;
- sets forth provisions concerning PreK-12, undergraduate, and graduate STEM education;
- requires the coordination of federal science and technology efforts to ensure secure, reliable, and environmentally sustainable supplies of critical materials to the United States;
- establishes a Clean Energy Incubator Program; and
- provides for space exploration activities.

Status: Became Public Law No: 117-167 (Aug 9, 2022).
Link: H.R.4346 - 117th Congress (2021-2022): Supreme Court Security Funding Act of 2022

H.R. 2471, Consolidated Appropriations Act of 2022 (including the Cyber Incident Reporting for Critical Infrastructure Act)

Overview: This bill provides appropriations to federal agencies for FY22. In addition, this bill included the Cyber Incident Reporting for Critical Infrastructure Act, which creates significant new requirements for American critical infrastructure organizations to report cybersecurity incidents and ransom payments to the Federal government.
Status: Became Public Law No: 117-103 (Mar 15, 2022)
Link: H.R.2471 - 117th Congress (2021-2022): Consolidated Appropriations Act, 2022
Public Law 117–103 117th Congress An Act (the Cyber Incident Reporting for Critical Infrastructure Act is in Division Y, which is at pages 990-1011 of this PDF).

H.R. 2617, Consolidated Appropriation Act of 2023:

Overview: This bill provides appropriations to federal agencies for FY23. Selected cyber provisions include:

- providing $2.9 billion for the Cybersecurity and Infrastructure Security Agency (CISA), $313.5 million or 12% above the fiscal year 2022 levels and $396.4 million above the President's budget request;
- prohibiting the use of TikTok on executive agency phones;
- limiting Chinese, North Korean, and Iranian procurement by the Federal government
- requiring medical device makers meet specific cybersecurity standards; and
- incorporating the provisions of the House-passed Ransomware Act, which requires the Federal Trade Commission (FTC) to report on cross-border complaints received that involve ransomware or other cyber-related attacks committed by certain foreign individuals, companies, and governments. The report must focus specifically on attacks committed by (1) Russia, China, North Korea, or Iran; or (2) individuals or companies that are located in or have ties to those countries. H.R. 4551, the Ransomware Act: https://www.congress.gov/bill/117th-congress/house-bill/4551

Status: Signed into law (December 29, 2022)

Link: H.R.2617 - 117th Congress (2021-2022): Consolidated Appropriations Act, 2023

H.R. 7776, National Defense Authorization Act for FY23

Selected cyber provisions:

- The U.S. intelligence community granted authority to maintain a list of foreign spyware vendors that pose a counterintelligence risk to the U.S and allows the DNI to prohibit intelligence agencies from purchasing or using such software.
- Cyber Command granted new authority to share hacking tools with partners and a license to conduct offensive cyber operations — given presidential direction — in response to an "active, systemic and ongoing" attack against the U.S.
- DOD granted a new assistant secretary of defense dedicated to the department's cyber policy — currently the responsibility of the official overseeing nuclear weapons, space, missile defense, and WMD deterrence.
- The State Department's new cyber bureau is codified.
- Cybersecurity grants for schools. Permits grants and cooperative agreements for the purpose of funding cybersecurity and infrastructure security education and training programs and initiatives.
- The Intragovernmental Cybersecurity Information Sharing Act, which requires the Federal executive branch to share "timely and urgent tactical and operational information to ensure that Congress can protect the constitutional officers, personnel, and facilities of Congress and the institution of Congress more broadly."
- DIVISION G—HOMELAND SECURITY
    - TITLE LXXI—HOMELAND SECURITY MATTERS
        - Subtitle A—Strengthening Security in Our Communities
            - Sec. 7104. Cybersecurity grants for schools.
        - Subtitle C—Enhancing Cybersecurity Training and Operations
            - Sec. 7121. President's Cup Cybersecurity Competition.
            - Sec. 7122. Industrial control systems cybersecurity training.
            - Sec. 7123. National Computer Forensics Institute reauthorization.
            - Sec. 7124. Report on cybersecurity roles and responsibilities of the Department of Homeland Security.

Status: Became Public Law No: 117-263 (Dec 23, 2022).

Link: Text - H.R.7776 - 117th Congress (2021-2022): James M. Inhofe National Defense Authorization Act for Fiscal Year 2023

S. 1605, National Defense Authorization Act for FY22

Selected cyber provisions :

- TITLE XV—CYBERSPACE-RELATED MATTERS,
- Strengthening DOD's Cybersecurity Posture
    - Requires the development of a joint zero trust strategy and a model architecture for the Department of Defense Information Network and a data management strategy.
    - Requires a program to demonstrate and assess an automated security validation capability to assist the Department in cybersecurity efforts.
    - Directs an assessment of the utility and cost-benefits of using capabilities to make risk-based vulnerability remediation decisions, identify key cyber terrain and assets,

identify single-node mission dependencies, and monitor for changes in mission threat execution.
    - Requires an assessment of the impact of the Cybersecurity Maturity Model Certification program on small businesses.
- Enhancing CYBERCOM's Authorities and Capabilities
    - Authorizes full funding for U.S. Cyber Command (CYBERCOM).
    - Assigns to the Commander, CYBERCOM, responsibility for directly controlling and managing the planning, programming, budgeting, and execution of the resources to maintain the Cyber Mission Forces.
    - Requires the Commander, CYBERCOM, to establish a voluntary process for engaging with the commercial information technology and cybersecurity companies to develop methods of coordination to protect against foreign malicious cyber actors.
- Strengthening the Federal Government's Cybersecurity Posture
    - Creates a pilot program led by the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Secretary of Defense and the National Cyber Director, to assess the feasibility and advisability of entering into voluntary public-private partnerships with internet ecosystem companies to facilitate actions by such companies to discover and disrupt the use of the platforms, systems, services, and infrastructure of such companies by malicious cyber actors.
    - Requires the Department of Homeland Security to take a variety of steps to improve cybersecurity, including by developing a strategy to improve cybersecurity, enhance cyber incident response, establish a national cyber exercise program, and establish a competition related to cybersecurity vulnerabilities.
    - Requires a CyberSentry program to provide continuous monitoring and detection of cybersecurity risks to certain critical infrastructure entities.
- Responding to the Cyber Threat Environment
    - Requires an assessment of the current and emerging offensive cyber posture of adversaries of the United States and the plans of the military services for offensive cyber operations during potential conflict.
    - Requires an assessment of the policy, capacity, and capabilities of DOD to defend the United States from ransomware attacks.
    - Strengthens the university cyber consortium of academic institutions that have been designed as Cyber Centers of Academic Excellence for cyber operations, cyber research, and cyber defense.
    - Directs the Comptroller General to assess DOD's efforts to address information and communications technology supply chain risks.
    - Expands eligibility for Department of Defense support and services to owners of critical infrastructure, including National Guard training on protection of critical infrastructure in the event of a cyber attack.

Status: Became Public Law No: 117-81 (Dec 27, 2021).
Link: S.1605 - 117th Congress (2021-2022): National Defense Authorization Act for Fiscal Year 2022 | Congress.gov | Library of Congress

H.R. 3462, SBA Cyber Awareness Act

Overview: This bill requires the Small Business Administration (SBA) to annually report specified information related to cybersecurity awareness.

Reports: S. Rept. 117-102 H. Rept. 117-138)
Status: Became Public Law No: 117-259 (Dec 21, 2022).
Link: H.R.3462 - 117th Congress (2021-2022): SBA Cyber Awareness Act

H.R 7299, SVAC Act of 2022

Overview: This bill requires the Department of Veterans Affairs (VA) to seek to enter into an agreement with a federally funded research and development center to provide a cybersecurity assessment of five high-impact VA information systems and the effectiveness of the VA's information security program and information security management system. The VA must submit a plan to Congress to address the findings of the assessment.
The Government Accountability Office must review the assessment and the VA's response to the assessment and report its findings to Congress.
Status: 12/27/2022 Became Public Law No: 117-302.
Link: H.R.7299 - 117th Congress (2021-2022): SVAC Act of 2022

H.R. 7535, Quantum Computing Cybersecurity Preparedness Act

Overview: This bill addresses the migration of executive agencies information technology systems to post-quantum cryptography. Post-quantum cryptography is encryption strong enough to resist attacks from quantum computers developed in the future.
Status: 12/21/2022 Became Public Law No: 117-260.
Link: 117th Congress (2021-2022): Quantum Computing Cybersecurity Preparedness Act

S. 658, National Cybersecurity Preparedness Consortium Act

Overview: This bill allows the Department of Homeland Security to work together with a consortium composed of nonprofit entities to develop, update, and deliver cybersecurity training in support of homeland security.
Status: Became Public Law No: 117-122 (May 12, 2022).
Link: S.658 - 117th Congress (2021-2022): National Cybersecurity Preparedness Consortium Act of 2021

S. 1097, Federal Rotational Cyber Workforce Program Act

Overview: To establish a Federal rotational cyber workforce program for the Federal cyber workforce.
Status: Became Public Law No: 117-149 (June 21, 2022). Passed the Senate (December 14, 2021). Passed the House (May 10, 2022). Signed by the President and became Public Law 117-149 (June 21, 2022).
Link: S.1097 - 117th Congress (2021-2022): Federal Rotational Cyber Workforce Program Act of 2021

S. 1687, Small Business Cyber Training Act of 2022

Overview: This bill requires the Small Business Administration to establish a program for certifying at least 5 or 10% of the total number of employees of a small business development center to provide cybersecurity planning assistance to small businesses.
Status: 12/27/2022 Became Public Law No: 117-319. (All Actions)
Link: S.1687 - 117th Congress (2021-2022): Small Business Cyber Training Act of 2022

S. 1917, K–12 Cybersecurity Act of 2021

Overview: This bill requires the Cybersecurity and Infrastructure Security Agency (CISA) to study the cybersecurity risks facing elementary and secondary schools and develop recommendations that include cybersecurity guidelines designed to assist schools in facing those risks. The use of such recommendations shall be voluntary. The study must evaluate the challenges that schools face in securing (1) information systems owned, leased, or relied upon by those schools; and (2) sensitive student and employee records. Further, the bill requires CISA to (1) develop an online training toolkit designed for school officials; and (2) make available on the Department of Homeland Security website the study's findings, the cybersecurity guidelines, and the toolkit.
Status: Became Public Law No: 117-47 (October 8, 2021).
Committee report:
https://www.congress.gov/congressional-report/117th-congress/senate-report/32/1?loclr=cga-search
Link: S.1917 - 117th Congress (2021-2022): K-12 Cybersecurity Act of 2021

S. 2629, Better Cybercrime Metrics Act

Overview: To establish cybercrime reporting mechanisms, and for other purposes.
Status: Became Public Law No: 117-116 (May 5, 2022).
Link: S.2629 - 117th Congress (2021-2022): Better Cybercrime Metrics Act

S. 2991, Countering Human Trafficking Act

Overview: This bill provides statutory authority for the Center for Countering Human Trafficking (CCHT) within the Department of Homeland Security (DHS). The CCHT coordinates DHS efforts to combat human trafficking and the importation of goods produced with forced labor.
Status: 12/27/2022 Became Public Law No: 117-322.
Link: https://www.congress.gov/bill/117th-congress/senate-bill/2991/

S. 4834, PROTECT Our Children Act of 2022

Overview: This bill reauthorizes through FY2024 the National Strategy for Child Exploitation Prevention and Interdiction.
Status: 12/21/2022 Became Public Law No: 117-262.
Link: S.4834 - 117th Congress (2021-2022): PROTECT Our Children Act of 2022

PASSED 1 HOUSE

H.R. 1, For The People Act of 2021

Overview: This bill (886 pages) addresses voter access, election integrity and security, campaign finance, and ethics for the three branches of government.
Status: Passed the House (March 3, 2021). Received in the Senate (March 11, 2021).
Link: HR1 - 117th Congress (2021-2022): For the People Act of 2021 | Congress.gov | Library of Congress

H.R. 4, John R. Lewis Voting Rights Advancement Act

Overview: This bill establishes new criteria for determining which states and political subdivisions must obtain preclearance before changes to voting practices may take effect. Preclearance is the process of receiving preapproval from the Department of Justice (DOJ) or the U.S. District Court for the District of Columbia before making legal changes that would affect voting rights. States and political subdivisions that meet certain thresholds regarding minority groups must preclear covered practices before implementation, such as changes to methods of election and redistricting.
Status: Passed the House (August 24, 2021). Received in the Senate (September 14, 2021).
Link: H.R.4 - 117th Congress (2021-2022): John R. Lewis Voting Rights Advancement Act of 2021

H.R. 21, FedRAMP Authorization Act

Overview: This bill provides statutory authority for the Federal Risk and Authorization Management Program (FedRAMP) within the General Services Administration (GSA).
Status: Passed the House (January 5, 2021). Received in the Senate and referred to the Committee on Homeland Security and Governmental Affairs (January 6, 2021).
Link: HR21 - 117th Congress (2021-2022): FedRAMP Authorization Act | Congress.gov | Library of Congress

H.R. 397, CBRN Intelligence and Information Sharing Act of 2021

Overview: To establish chemical, biological, radiological, and nuclear intelligence and information sharing functions of the Office of Intelligence and Analysis of the Department of Homeland Security.
Status: Passed the House (04/20/21). Received in the Senate and referred to the Senate Homeland Security and Government Affairs Committee (04/22/21).
Link: H.R.397 - 117th Congress (2021-2022): CBRN Intelligence and Information Sharing Act of 2021

H.R. 1251, Cyber Diplomacy Act of 2021

Overview: This bill establishes requirements related to diplomatic engagement with foreign countries on matters of U.S. cyberspace policy.
Status: Passed the House on April 20, 2021. Received in the Senate and referred to the Committee on Foreign Relations on April 22, 2021.
Link: HR1251 - 117th Congress (2021-2022): Cyber Diplomacy Act of 2021 | Congress.gov | Library of Congress

H.R. 1833, DHS Industrial Control Systems Capabilities Enhancement Act of 2021

Overview: This bill requires the Cybersecurity and Infrastructure Security Agency (CISA) to maintain certain capabilities to identify and address threats to industrial control systems. Specifically, the bill requires CISA's National Cybersecurity and Communications Integration Center to ensure that its activities address the security of both information and operational technology, including industrial control systems. Additionally, CISA must maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes by (1) leading efforts to identify and mitigate cybersecurity threats to industrial control systems; (2) maintaining threat hunting and incident response capabilities to respond to cybersecurity risks and incidents; (3) providing cybersecurity technical assistance to stakeholders; and (4) collecting, coordinating, and providing vulnerability information to the industrial control systems community.

Status: Passed the House (July 20, 2021). Transmitted to the Senate on July 21, 2021.
Link: H.R.1833 - 117th Congress (2021-2022): DHS Industrial Control Systems Capabilities Enhancement Act of 2021

H.R. 2225, National Science Foundation for the Future Act

Overview: This bill reauthorizes the National Science Foundation (NSF) through FY2026 and authorizes programs and activities at the NSF.
Status: Passed the House 6/28/2021. 07/12/2021 Received in the Senate and Read twice and referred to the Committee on Health, Education, Labor, and Pensions.
Link: 117th Congress (2021-2022): National Science Foundation for the Future Act

H.R. 2685, Understanding Cybersecurity of Mobile Networks Act

Overview: This bill requires the National Telecommunications and Information Administration to examine and report on the cybersecurity of mobile service networks and the vulnerability of these networks and mobile devices to cyberattacks and surveillance conducted by adversaries. The report shall include (1) an assessment of the degree to which providers of mobile service have addressed certain cybersecurity vulnerabilities; (2) a discussion of the degree to which these providers have implemented cybersecurity best practices and risk assessment frameworks; and (3) an estimate of the prevalence and efficacy of encryption and authentication algorithms and techniques used in mobile service and communications equipment, mobile devices, and mobile operating systems and software.
Status: Passed the House on December 1, 2021. Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation (December 2, 2021).
Link: H.R.2685 - 117th Congress (2021-2022): Understanding Cybersecurity of Mobile Networks Act

H.R. 2928, Cyber Sense Act of 2021

Overview: A legislative analyst in the Congressional Research Service will begin analyzing this legislation after text becomes available.
House report: H. Rept. 117-92
Status: Passed the House on July 20, 2021. Transmitted to the Senate on July 21, 2021.
Link: H.R.2928 - 117th Congress (2021-2022): Cyber Sense Act of 2021

H.R. 2931, Enhancing Grid Security through Public-Private Partnerships Act

Overview: This bill directs the U.S. Department of Energy to implement a program to facilitate and encourage public-private partnerships in order to address and mitigate the physical security and cybersecurity risks of electric utilities..
Status: Passed the House (July 19, 2021). Received in the Senate (July 20, 2021).
Link: H.R.2931 - 117th Congress (2021-2022): Enhancing Grid Security through Public-Private Partnerships Act

H.R. 2980, Cybersecurity Vulnerability Remediation Act

Overview: This bill authorizes the Department of Homeland Security (DHS) to take certain actions with the goal of countering cybersecurity vulnerabilities.
The National Cybersecurity and Communications Integration Center of DHS may disseminate protocols to counter cybersecurity vulnerabilities, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor.

The Science and Technology Directorate may establish a competition to develop remedies for cybersecurity vulnerabilities.
Status: Passed the House (July 20, 2021). Received in the Senate and referred to the Committee on Homeland Security and Governmental Affairs (July 21, 2021).
Link: H.R.2980 - 117th Congress (2021-2022): Cybersecurity Vulnerability Remediation Act

H.R. 3119, Energy Emergency Leadership Act

Overview: This bill requires the Secretary of Energy to assign energy emergency and energy security functions to an Assistant Secretary, including responsibilities with respect to infrastructure and cybersecurity.
Status: Senate - 03/01/2022 Committee on Energy and Natural Resources. Hearings held. Passed the House (July 19, 2021).
Link: H.R.3119 - 117th Congress (2021-2022): Energy Emergency Leadership Act

H.R. 3138, State and Local Cybersecurity Improvement Act

Overview: This bill requires the Cybersecurity and Infrastructure Security Agency (CISA) to establish the State and Local Cybersecurity Grant Program to address cybersecurity risks and threats to the information systems of state, local, or tribal organizations.

Eligible grant applicants (i.e., states and certain Indian tribes) must submit a cybersecurity plan—to be approved by CISA as a condition of disbursement—that describes how the applicant will use the funds to address cybersecurity risks and threats to their information systems. Grant funds must be used to implement, develop, or revise the applicant's cybersecurity plan or to assist with activities that address imminent cybersecurity risks or threats.

CISA must establish a State and Local Cybersecurity Resilience Committee to provide state, local, and tribal stakeholder expertise, situational awareness, and recommendations to CISA on how to address cybersecurity risks and threats. One individual will be recommended to the Director by the Multi-State Information Sharing and Analysis Center.

CISA must develop and maintain a resource guide for state, local, tribal, and territorial government officials to assist with identifying, preparing for, detecting, protecting against, responding to, and recovering from cybersecurity risks, threats, and incidents. In addition, CISA must develop and make publicly available a Homeland Security Strategy to improve the Cybersecurity of State, Local, Tribal, and Territorial Governments.

Finally, CISA must assess the feasibility of implementing a short-term rotational program to detail approved state, local, tribal, and territorial government employees to CISA in cyber workforce positions.
Link: H.R.3138 - 117th Congress (2021-2022): State and Local Cybersecurity Improvement Act
Status: Passed the House on July 20, 2021. Transmitted to the Senate on July 21, 2021. **A version of this bill was included in H.R. 3684, the Infrastructure Investment & Jobs Act (IIJA) & was signed into law on Nov 15, 2021:** 117th Congress (2021-2022): Infrastructure Investment and Jobs Act

H.R. 3223, CISA Cyber Exercise Act

Overview: This bill establishes the National Cyber Exercise Program to evaluate the National Cyber Incident Response Plan and related plans and strategies. (The National Cyber Incident Response Plan outlines the roles and responsibilities, capabilities, and coordinating structures that support how the United States responds to and recovers from significant cyber incidents posing risks to critical

infrastructure.) Based on current risk assessments, the exercise program shall be designed to (1) simulate partial or complete incapacitation of a government or critical infrastructure network resulting from a cyber incident, (2) provide for the systematic evaluation of cyber readiness and enhance operational understanding of the cyber incident response system and relevant information sharing agreements, and (3) develop after-action reports and plans that can incorporate lessons learned into future operations.
Status: Passed the House (July 20, 2021). Received in the Senate and referred to the Committee on Homeland Security and Governmental Affairs (July 21, 2021).
Link: HR3223 - 117th Congress (2021-2022): CISA Cyber Exercise Act | Congress.gov | Library of Congress

H.R. 3599, Federal Rotational Cyber Workforce Program Act

Overview: This bill establishes a rotational cyber workforce program under which certain federal employees may be detailed among rotational cyber workforce positions at other agencies.
Status: 04/06/2022 Read twice. Placed on the Senate Legislative Calendar under General Orders. Calendar No. 343. Passed the House on 09/29/2021.
Link: H.R.3599 - 117th Congress (2021-2022): Federal Rotational Cyber Workforce Program Act of 2021

H.R. 4028, Information and Communication Technology Strategy Act

Overview: The Information and Communication Technology Strategy Act would require the DOC to report on and develop a whole-of-Government strategy with respect to the economic competitiveness of the information and communication technology supply chain.
Status: Passed the House (October 20, 2021). Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation. (October 21, 2022).
Link: HR4028 - 117th Congress (2021-2022): Information and Communication Technology Strategy Act

H.R. 4032, Open RAN Outreach Act

Overview: The Open RAN Outreach Act would strengthen the diversity of U.S. wireless networks and protect the supply chain from reliance on untrusted technology companies.
Status: Passed the House (October 20, 2021). Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation. (October 21, 2022).
Link: HR4032 - 117th Congress (2021-2022): Open RAN Outreach Act

H.R. 4045, FUTURE Networks Act

Overview: This bill requires the Federal Communications Commission to establish the 6G Task Force to report on sixth-generation wireless technology, including the status of setting standards for and possible uses of such technology. The task force shall be composed of representatives of (1) trusted companies in the communications industry; (2) trusted public interest organizations or academic institutions; and (3) federal, state, local, and tribal governments.
Status: Passed the House on 12/01/2021. Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation on 12/02/2021.
Link: HR4045 - 117th Congress (2021-2022): FUTURE Networks Act

H.R 4055, American Cybersecurity Literacy Act

Overview: This bill requires the National Telecommunications and Information Administration to develop and conduct a cybersecurity literacy campaign to increase knowledge and awareness of best practices to reduce cybersecurity risks.
Status: Passed the House on 12/01/2021. Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation on 12/02/2021.
Link: 117th Congress (2021-2022): American Cybersecurity Literacy Act

H.R. 4350, National Defense Authorization Act for Fiscal Year 2022

Overview: This bill authorizes FY2022 appropriations for military activities and programs of the Department of Defense (e.g., personnel; research, development, test, and evaluation; and procurement of items such as aircraft, missiles, and ammunition). It also prescribes military personnel strengths for FY2022.
Status: Passed the House on 09/23/21. **A related bill, S. 1605, the National Defense Authorization Act, passed both houses and became Public Law No: 117-81 (Dec 27, 2021).**
Link: H.R.4350 - 117th Congress (2021-2022): National Defense Authorization Act for Fiscal Year 2022

H.R. 4515, Small Business Development Center Cyber Training Act

Overview: This bill requires the Small Business Administration to establish a program for certifying at least 5 or 10% of the total number of employees of a small business development center to provide cybersecurity planning assistance to small businesses.
Status: Passed the House on 11/2/2021. Received in the Senate and Read twice and referred to the Committee on Small Business and Entrepreneurship on 11/03/2021
Link: H.R.4515 - 117th Congress (2021-2022): Small Business Development Center Cyber Training Act of 2021

H.R. 4521, United States Innovation and Competition Act

Overview: This bill addresses U.S. technology and communications, foreign relations and national security, domestic manufacturing, education, trade, and other matters.
Status: Passed the House and the Senate. **A version of the became law as H.R. 4346.**
Link: H.R.4521 - 117th Congress (2021-2022): United States Innovation and Competition Act of 2021

H.R. 4551, RANSOMWARE Act

Overview: This bill requires the Federal Trade Commission to report on cross-border complaints received that involve ransomware or other cyber-related attacks committed by certain foreign individuals, companies, and governments. The report must focus specifically on attacks committed by (1) Russia, China, North Korea, or Iran; or (2) individuals or companies that are located in or have ties to those countries.
Status: Passed House (07/27/2022). Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation (07/28/22)
Link: HR4551 - 117th Congress (2021-2022): RANSOMWARE Act | Congress.gov | Library of Congress

H.R. 4611, DHS Software Supply Chain Risk Management Act

Overview: This bill requires the Management Directorate of the Department of Homeland Security (DHS) to issue guidance regarding new and existing contracts relating to the procurement of

information and communications technology or services. The bill requires contractors to submit to DHS a bill of materials, a certification that each item in the bill of materials is free from certain security vulnerabilities, a notification of any identified vulnerability, and a plan to mitigate any identified vulnerability.
Status: Passed the House (October 20, 2021). Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (October 21, 2021)
Link: H.R.4611 - 117th Congress (2021-2022): DHS Software Supply Chain Risk Management Act of 2021

H.R. 5314, Protecting Our Democracy Act

Overview: This bill addresses issues involving (1) abuses of presidential power; (2) checks and balances, accountability, and transparency; and (3) election integrity and security.
Status: 12/13/2021 Received in the Senate. 12/08/2021 Passed in the House.
Link: 117th Congress (2021-2022): Protecting Our Democracy Act

H.R. 6824, President's Cup Cybersecurity Competition Act

Overview: This bill authorizes an annual competition to award prizes, including cash prizes, to U.S. government cybersecurity employees and teams.
Link: H.R.6824 - 117th Congress (2021-2022): President's Cup Cybersecurity Competition Act
Status: Passed the House (May 16, 2022). Passed Senate Homeland Security Committee(Sep. 28, 2022). **A version of this was included in H.R. 7776 at Section 7121 (signed into law on Fri, Dec 23, 2022) (became Public Law No: 117-263 on Dec 27, 2022):**
https://www.congress.gov/bill/117th-congress/house-bill/7776.

H.R. 6868, Cybersecurity Grants for Schools Act of 2022

Overview: This bill allows the Cybersecurity and Infrastructure Security Agency (CISA) to award grants or other financial assistance for cybersecurity and infrastructure security education and training programs at the elementary and secondary education levels. Entities eligible for the assistance include states, localities, institutions of higher education, and nonprofits. Additionally, CISA must include information about how the grants and assistance enhance cybersecurity education for underserved populations or communities in annual briefings.
Link: H.R.6868 - 117th Congress (2021-2022): Cybersecurity Grants for Schools Act of 2022
Status: Passed House on 5/17/2022. **A version of this was included in H.R. 7776 at Section 7104 (signed into law on Fri, Dec 23, 2022) (became Public Law No: 117-263 on Dec 27, 2022):**
https://www.congress.gov/bill/117th-congress/house-bill/7776

H.R.7174, National Computer Forensics Institute Reauthorization Act of 2022

Overview: Reauthorize the DHS National Computer Forensics Institute operated by the U.S. Secret Service in Alabama.
Link: HR7174 - 117th Congress (2021-2022): National Computer Forensics Institute Reauthorization Act of 2022
Status: A version of this was included in H.R. 7776 at Section 7123 (signed into law on Fri, Dec 23, 2022) (became Public Law No: 117-263 on Dec 27, 2022):
https://www.congress.gov/bill/117th-congress/house-bill/7776. Passed by the House (July 13, 2022).

H.R. 7777, Industrial Control Systems Cybersecurity Training Act
Overview: This bill establishes within the Cybersecurity and Infrastructure Security Agency an initiative to provide the cybersecurity workforce with no-cost training related to securing industrial control systems. These are information systems used to control industrial processes, such as manufacturing, product handling, production, and distribution.
Link: HR7777 - 117th Congress (2021-2022): Industrial Control Systems Cybersecurity Training Act
Status: A version of this was included in H.R. 7776 at Section 7122 (signed into law on Fri, Dec 23, 2022) (became Public Law No: 117-263 on Dec 27, 2022):
https://www.congress.gov/bill/117th-congress/house-bill/7776.

H.R. 8873, Presidential Election Reform Act
Overview: This bill revises the process of casting and counting electoral votes for presidential elections.
Status: Passed the House (September 21, 2022). Received in the Senate (September 22, 2022).
Link: H.R.8873 - 117th Congress (2021-2022): Presidential Election Reform Act

H.R. 8956, FedRAMP Authorization Act
Summary: This bill codifies and provides a legislative framework for the Federal Risk and Authorization Management Program (FedRAMP) and new authorities to the General Services Administration.
Status: Passed the House (September 29, 2022). Introduced in the House (September 22, 2022).
Link: H.R.8956 - 117th Congress (2021-2022): To amend chapter 36 of title 44, United States Code, to improve the cybersecurity of the Federal Government, and for other purposes.

—

S. 2322, CTPAT Pilot Program Act of 2021
Overview: This bill requires the Department of Homeland Security to carry out a pilot program that assesses whether allowing certain entities to participate in the Customs Trade Partnership Against Terrorism (CTPAT) would enhance port security, combat terrorism, prevent supply chain security breaches, or otherwise meet the goals of CTPAT.
Status: Passed the Senate (May 26, 2022).
Link: https://www.congress.gov/bill/117th-congress/senate-bill/2322/

S. 2875, Cyber Incident Reporting Act
Overview: This bill requires reporting and other actions to address cybersecurity incidents, including ransomware attacks.
Status: Passed Senate Homeland Security Committee (12/13/2022).
Link: S.2875 - 117th Congress (2021-2022): Cyber Incident Reporting Act of 2021

S. 2902, Federal Information Security Modernization Act

Overview: This bill addresses federal information security management, notification and remediation of cybersecurity incidents, and the role of the Office of Management and Budget (OMB) and the Cybersecurity and Infrastructure Security Agency (CISA).
Status: Passed Senate Homeland Security Committee (12/19/2022).
Link: S.2902 - 117th Congress (2021-2022): Federal Information Security Modernization Act of 2021

S. 2989, DHS Blue Campaign Enhancement Act

Overview: This bill requires reporting and other actions to address cybersecurity incidents, including ransomware attacks.
Status: Passed Senate Homeland Security Committee (12/13/2022).
Link: https://www.congress.gov/bill/117th-congress/senate-bill/2989

S. 3099, Federal Secure Cloud Improvement and Jobs Act

Overview: This bill provides statutory authority for the Federal Risk and Authorization Management Program (FedRAMP) within the General Services Administration (GSA).
Status: Passed Senate Homeland Security Committee (05/24/2022)
Link: S.3099 - 117th Congress (2021-2022): Federal Secure Cloud Improvement and Jobs Act of 2021

S. 3600, Strengthening American Cybersecurity Act

Overview: This bill addresses cybersecurity threats against critical infrastructure and the federal government.
Status: 03/02/2022 Received in the House. Held at the desk. 03/01/22 - Passed in the Senate.
Link: https://www.congress.gov/bill/117th-congress/senate-bill/3600

S. Res. 410, National Cybersecurity Awareness Month

Overview: This resolution recognizes October 2021 as National Cybersecurity Awareness Month and commits to continue working to enhance U.S. cybersecurity.
Status: Agreed to in the Senate (11/02/2021)
Link: S.Res.410 - 117th Congress (2021-2022): A resolution supporting the goals and ideals of National Cybersecurity Awareness Month to raise awareness and enhance the state of cybersecurity in the United States. | Congress.gov | Library of Congress

ELECTION-RELATED BILLS INTRODUCED

H.R. 102, Restoring Faith In Elections Act

Overview: To ensure election integrity and security and enhance Americans' access to the ballot box by establishing consistent standards and procedures for voter registration and voting in elections for Federal office, and for other purposes.
Status: Introduced and referred to the Subcommittee on Research and Technology (January 4, 2021).
Link: HR102 - 117th Congress (2021-2022): Restoring Faith in Elections Act | Congress.gov | Library of Congress

H.R. 2358, Voter Empowerment Act
Overview: To modernize voter registration, promote access to voting for individuals with disabilities, protect the ability of individuals to exercise the right to vote in elections for Federal office, and for other purposes.
Status: 10/19/2021 Referred to the Subcommittee on the Constitution, Civil Rights, and Civil Liberties.
Link: H.R. 2358 - 117th Congress (2021-2022): Voter Empowerment Act of 2021

H.R. 2844, Election Protection Act of 2021
Overview: A legislative analyst in the Congressional Research Service will begin analyzing this legislation after text becomes available.
Status: 04/26/2021 Referred to the House Committee on House Administration.
Link: H.R.2844 - 117th Congress (2021-2022): Election Protection Act of 2021

H.R. 2941, Accessible Voting Act
Overview: This bill addresses voting accessibility for individuals with disabilities and older individuals.
Status: 04/30/2021 Referred to the House Committee on House Administration.
Link: H.R.2941 - 117th Congress (2021-2022): Accessible Voting Act of 2021

H.R. 3867, Every Vote Counts Act
Overview: This bill requires states to take certain actions to facilitate absentee voting for federal elections.
Status: 06/14/2021 Referred to the Committee on House Administration, and in addition to the Committee on Science, Space, and Technology, 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.
Link: HR3867 - 117th Congress (2021-2022): Every Vote Counts Act

---

S.1, For the People Act of 2021
Overview: The Senate companion bill to H.R. 1, which addresses voter access, election integrity and security, campaign finance, and ethics for the three branches of government.
Status: Passed by the Senate Rules Committee and put on the Senate Legislative Calendar (August 11, 2021).
Hearing transcript & attachments: S.Hrg. 117-14 — S. 1, FOR THE PEOPLE ACT | Congress.gov
Link: S.1 - 117th Congress (2021-2022): For the People Act of 2021

S. 13, A bill to establish an advisory committee to make recommendations on improvements to the security, integrity, and administration of Federal elections.
Overview: This bill establishes a bipartisan advisory committee within the Election Assistance Commission (EAC) to study the integrity and administration of the November 2020 general election. The committee must also make recommendations to the EAC, state legislatures, and Congress on best

practices for administering federal elections, including best practices to prevent improper voting and increase the security of vote-by-mail ballots.
Status: Placed on Senate Legislative Calendar under General Orders. Calendar No. 2 (January 19, 2021).
Link: S.13 - 117th Congress (2021-2022): A bill to establish an advisory committee to make recommendations on improvements to the security, integrity, and administration of Federal elections.

S. 640, Invest in Our Democracy Act of 2021

Overview: This bill directs the Election Assistance Commission (EAC) to provide grants to institutions of higher education to reduce tuition for state or local election officials, employees of such election officials, and employees of the EAC who are enrolled in accredited certificate programs in election administration or cybersecurity at such institutions.
Status: Senate - 03/09/2021 Read twice and referred to the Committee on Rules and Administration.
Link: S.640 - 117th Congress (2021-2022): Invest in Our Democracy Act of 2021

S. 954, Voter Empowerment Act of 2021

Overview: This bill expands voter registration and voting access. Specifically, the bill expands voter registration by requiring states to (1) make available online voter registration, (2) establish automatic voter registration systems, (3) permit same-day voter registration, and (4) accept voter registration applications from individuals under age 18.
Status: 03/24/2021 Read twice and referred to the Committee on Rules and Administration.
Link: S.954 - 117th Congress (2021-2022): Voter Empowerment Act of 2021

S. 1470, Accessible Voting Act of 2021

Overview: This bill addresses voting accessibility for individuals with disabilities and older individuals.
Status: 04/29/2021 Read twice and referred to the Committee on Rules and Administration.
Link: S.1470 - 117th Congress (2021-2022): Accessible Voting Act of 2021

S. 2093, For the People Act of 2021

Overview: A newer version of S. 1. This bill addresses voter access, election integrity and security, campaign finance, and ethics for the three branches of government. Specifically, the bill:

- expands voter registration (e.g., automatic and same-day registration) and voting access (e.g., vote-by-mail and early voting).
- limits removing voters from voter rolls
- requires states to establish independent redistricting commissions to carry out congressional redistricting.
- sets forth provisions related to election security, including sharing intelligence information with state election officials, supporting states in securing their election systems, developing a national strategy to protect U.S. democratic institutions, establishing in the legislative branch the National Commission to Protect United States Democratic Institutions, and other provisions to improve the cybersecurity of election systems.
- addresses campaign finance, including by expanding the prohibition on campaign spending by foreign nationals, requiring additional disclosure of campaign-related fundraising and

spending, requiring additional disclaimers regarding certain political advertising, and establishing an alternative campaign funding system for certain federal offices.
- addresses ethics in all three branches of government, including by requiring a code of conduct for Supreme Court Justices, prohibiting Members of the House from serving on the board of a for-profit entity, and establishing additional conflict-of-interest and ethics provisions for federal employees and the White House.

Status: 09/15/2021 Cloture motion on the motion to proceed to the measure withdrawn by unanimous consent in the Senate.
Link: S.2093 - 117th Congress (2021-2022): For the People Act of 2021

S. 2747, Freedom to Vote Act

Overview: A bill to expand Americans' access to the ballot box and reduce the influence of big money in politics, and for other purposes.
Status: Cloture on the motion to proceed not invoked (Oct 29, 2021).
Link: https://www.congress.gov/bill/117th-congress/senate-bill/2747/

S.3142, Election Worker and Polling Place Protection Act

Overview: This bill addresses certain protections for election workers and polling places.
In particular, the bill prohibits, with enhanced penalties for certain types of threats and harms (1) intimidation of poll watchers, election officials, and election agents, vendors, and contractors involving violence or threats of harm; and (2) physical damage to or threats to physically damage a polling place, tabulation center, or other election infrastructure.
Status: 11/02/2021 Read twice and referred to the Committee on the Judiciary.
Link: S.3142 - 117th Congress (2021-2022): Election Worker and Polling Place Protection Act

S. 4573, Electoral Count Reform and Presidential Transition Improvement Act

Overview: This bill would revise the process of casting and counting electoral votes for presidential elections. The bill also revises provisions related to the presidential transition process.
Status: 10/18/2022 Placed on Senate Legislative Calendar under General Orders. Calendar No. 529.
Sen. Collins fact sheet: One Pager on Electoral Count Reform Act of 2022
Link: S.4573 - 117th Congress (2021-2022): Electoral Count Reform and Presidential Transition Improvement Act of 2022

S. 4574, Enhanced Election Security and Protection Act

Overview: This bill would increase penalties for threats and intimidation of election officials, seek to improve the Postal Service's handling of mail-in ballots, and renew for five years an independent federal agency that helps states administer and secure federal elections.
Status: Referred to Senate Homeland Security Committee (July 20, 2022).
Link: S.4574 - 117th Congress (2021-2022): Enhanced Election Security and Protection Act

CYBERSECURITY BILLS INTRODUCED

H.R. 117, DHS Cybersecurity On-The-Job Training & Employment Apprentice Program Act
Overview: This bill requires the Department of Homeland Security (DHS) to establish a DHS Cybersecurity On-the-Job Training and Employment Apprentice Program to identify and train DHS employees for cybersecurity work.
Status: House - 01/04/2021 Referred to the House Committee on Homeland Security.
Link: H.R.117 - 117th Congress (2021-2022): DHS Cybersecurity On-the-Job Training and Employment Apprentice Program Act

H.R. 118, Cyber Vulnerability Disclosure Reporting Act
Overview: This bill requires the Department of Homeland Security to submit a report describing the policies and procedures developed to coordinate the disclosure of cyber vulnerabilities. The report shall describe instances when these policies and procedures were used to disclose cyber vulnerabilities in the previous year. Further, the report shall mention the degree to which the disclosed information was acted upon by stakeholders.
Status: House - 01/04/2021 Referred to the House Committee on Homeland Security.
Link: HR118 - 117th Congress (2021-2022): Cyber Vulnerability Disclosure Reporting Act | Congress.gov | Library of Congress

H.R. 119, Cyber Defense National Guard Act
Overview: This bill requires the Office of the Director of National Intelligence to report to Congress regarding the feasibility of establishing a Cyber Defense National Guard.
Status: House - 01/04/2021 Referred to the House Committee on Intelligence (Permanent Select)
Link: HR119 - 117th Congress (2021-2022): Cyber Defense National Guard Act | Congress.gov | Library of Congress

H.R. 337, FADE Act
Overview: This bill revises the disclaimer requirements for informational materials transmitted by agents of foreign principals.
Article: House lawmakers reintroduce bipartisan bill to weed out foreign disinformation on social media
Status: 03/05/2021 - Referred to the subcommittee on the Constitution, Civil Rights, & Civil Liberties.
Link: HR337 - 117th Congress (2021-2022): FADE Act of 2021 | Congress.gov | Library of Congress

H.R. 474, Protecting Consumer Information Act
Overview: This bill requires the Federal Trade Commission to review whether current privacy standards are sufficient to protect consumer financial information against cyber threats. The bill includes provisions related to investigations, enforcement, and regulations that apply to consumer reporting agencies.
Status: House - 02/02/2021 Referred to the Subcommittee on Consumer Protection and Commerce.
Link: HR474 - 117th Congress (2021-2022): Protecting Consumer Information Act of 2021 | Congress.gov | Library of Congress

H.R. 807, Invest in Child Safety Act
Overview: This bill modifies the federal framework governing the prevention of online sexual exploitation of children.
Status: 04/23/2021 Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
Link: HR807 - 117th Congress (2021-2022): Invest in Child Safety Act | Congress.gov | Library of Congress

H.R. 1330, Patient Access to Higher Quality Health Care Act
Overview: This bill repeals provisions under the Stark law (i.e., the Physician Self-Referral Law) that limit, for purposes of Medicare participation, self-referrals by newly constructed or expanded physician-owned hospitals.
Status: 02/26/2021 Referred to the Subcommittee on Health.
Link: H.R.1330 - 117th Congress (2021-2022): Patient Access to Higher Quality Health Care Act of 2021

H.R. 1374, Enhancing State Energy Security Planning and Emergency Preparedness Act
Overview: This bill authorizes the Department of Energy (DOE) to provide financial assistance to states for the implementation, review, and revision of a state energy security plan that assesses the state's existing circumstances and proposes methods to strengthen the ability of the state to have a reliable, secure, and resilient energy infrastructure.
Status: 06/23/2021: Received in the Senate and Read twice and referred to the Committee on Energy and Natural Resources. Bill, Resolution, or Law Text: Engrossed in House (06/22/2021)
Link: H.R.1374 - 117th Congress (2021-2022): Enhancing State Energy Security Planning and Emergency Preparedness Act of 2021

H.R. 1616, Promoting Interagency Coordination for Review of Natural Gas Pipelines Act
Overview: This bill expands the authority of the Federal Energy Regulatory Commission (FERC) to act as the only lead agency for the purpose of coordinating the environmental review process under the National Environmental Policy Act of 1969 (NEPA) of natural gas pipeline project applications under the Natural Gas Act. Thus, federal, state, and local agencies involved in the environmental review process must defer to FERC's approved scope for a NEPA review.
Status: 03/09/2021 Referred to the Subcommittee on Energy.
Link: H.R.1616 - 117th Congress (2021-2022): Promoting Interagency Coordination for Review of Natural Gas Pipelines Act

H.R. 1672, Connect America Act
Overview: This bill requires the Federal Communications Commission to establish a funding program to expand broadband access for unserved areas, areas with low-tier or mid-tier service, and unserved anchor institutions (e.g., schools or libraries). The program shall consist of both national systems of competitive bidding and grants of specified amounts to states.
Status: 03/10/2021 Referred to the Subcommittee on Communications and Technology.
Link: H.R.1672 - 117th Congress (2021-2022): To amend the Communications Act of 1934 to provide for the establishment of a program to expand access to broadband service, and for other purposes.

H.R.1783, Accessible, Affordable Internet for All Act

Overview: This bill reauthorizes through FY2026, revises, and establishes grants and activities to promote access to broadband internet and other telecommunication services. (Related to H.R. 1841)
Status: 04/28/2021 Referred to the Subcommittee on Commodity Exchanges, Energy, and Credit.
Link: H.R.1783 - 117th Congress (2021-2022): Accessible, Affordable Internet for All Act

H.R. 1816, Information Transparency and Personal Data Control Act

Overview: This bill requires the Federal Trade Commission (FTC) to establish requirements for certain entities when they collect, transmit, store, process, use, or otherwise control sensitive personal information. Information relating to an identifiable individual is generally considered sensitive personal information. However, information that is publicly available is not considered sensitive.
Status: 03/12/2021 Referred to the Subcommittee on Consumer Protection and Commerce.
Link: H.R.1816 - 117th Congress (2021-2022): Information Transparency & Personal Data Control Act

H.R. 1841, Digital Equity Act

Overview: This bill requires the National Telecommunications and Information Administration to establish grant programs for promoting digital equity, supporting digital inclusion activities, and building capacity for state-led efforts to increase adoption of broadband by their residents. (Related Bill to H.R. 1783)
Status: 03/12/2021 Referred to the Subcommittee on Communications and Technology.
Link: HR1841 - 117th Congress (2021-2022): Digital Equity Act of 2021 | Congress.gov | Library of Congress

H.R. 1846, To amend the Public Health Service Act regarding hospital infrastructure.

Overview: This bill reauthorizes through FY2026 and makes changes to a grant program for constructing and modernizing health care facilities, including by prioritizing projects that address public health emergency preparedness or cybersecurity.
Status: 03/11/2021 Referred to the subcommittee on Health.
Link: H.R.1846 - 117th Congress (2021-2022): To amend the Public Health Service Act with respect to hospital infrastructure.

H.R. 1866, Quantum Network Infrastructure Act

Overview: This bill directs the Department of Energy (DOE) to carry out a research, development, and demonstration program to accelerate innovation in quantum network infrastructure in order to (1) facilitate the advancement of distributed quantum computing systems through the internet and intranet, (2) improve the precision of measurements of scientific phenomena and physical imaging technologies, and (3) develop secure national quantum communications technologies and strategies. DOE shall submit to Congress a four-year research plan that identifies and prioritizes basic research needs relating to quantum network infrastructure.
Status: 03/11/2021 Referred to the Subcommittee on Energy.
Link: HR1866 - 117th Congress (2021-2022): Quantum Network Infrastructure Act of 2021 | Congress.gov | Library of Congress

H.R. 2154, Protecting Americans from Dangerous Algorithms Act

Overview: This bill limits a social media company's immunity from liability if it promotes certain content on its platform.
Status: 03/24/2021 Referred to the Subcommittee on Communications and Technology.
Link: H.R.2154 - 117th Congress (2021-2022): Protecting Americans from Dangerous Algorithms Act

H.R. 2201, Computer and Internet Access Equity Act

Overview: This bill increases broadband service support for low-income consumers, establishes a grant program to provide Internet safety education or training, and provides a tax credit for certain computer and education costs.
Status: 03/29/2021 Referred to the Subcommittee on Communications and Technology.
Link: H.R.2201 - 117th Congress (2021-2022): Computer and Internet Access Equity Act

H.R.2326, Veterans' Cyber Risk Awareness Act

Overview: This bill requires the Office of Public and Intergovernmental Affairs of the Department of Veterans Affairs (VA) to conduct a communications and outreach campaign to educate veterans about *cyber risks*. These risks can include disinformation, identity theft, scams, and fraud spread via the internet or social media. Additionally, the VA must seek to enter an agreement with a federally funded research and development corporation to perform a study that assesses (1) the vulnerability of veterans to cyber risks, (2) the availability and efficacy of resources to assist veterans in combatting such risks, and (3) the efficacy of the VA's outreach campaign. The study must also recommend ways the VA can reduce cyber risks to veterans.
Status: Passed the House Committee on Veterans Affairs (04/06/2022).
Link: 117th Congress (2021-2022): Veterans' Cyber Risk Awareness Act

H.R. 2236, Cyber Shield Act

Overview: This bill requires the Department of Commerce to establish the Cyber Shield Program, a voluntary program to identify and certify covered products. These products are consumer-facing physical objects that meet industry-leading cybersecurity and data security benchmarks and that can (1) connect to the internet; and (2) collect, send, or receive data or control the actions of a physical object or system. Commerce must also establish a Cyber Shield Advisory Committee to recommend (1) the format and content of Cyber Shield labels for covered products; and (2) the process to identify, establish, report on, adopt, maintain, and promote compliance with industry-leading cybersecurity and data security benchmarks to enhance cybersecurity and protect data. On its website, Commerce must make publicly available (1) program information, (2) a database of covered products certified under the program, and (3) contact information for each manufacturer of a covered product certified under the program.
Status: 3/29/2021 Referred to the Subcommittee on Consumer Protection and Commerce.
Link: HR2236 - 117th Congress (2021-2022): Cyber Shield Act of 2021 | Congress.gov | Library of Congress

H.R. 2894, Civilian Cyber Security Reserve Act

Overview: This bill authorizes the Department of Homeland Security and the Department of Defense to each create a temporary Civilian Cyber Security Reserve within their agencies to address U.S. cybersecurity needs with respect to national security.

Status: 4/28/2021 Referred to the Committee on Armed Services, and in addition to the Committee on 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.
Link: H.R.2894 - 117th Congress (2021-2022): Civilian Cyber Security Reserve Act

H.R. 2982, National Guard Cybersecurity Support Act

Overview: This bill authorizes members of the National Guard to perform, at the request of a state and in connection with training or other duty, cybersecurity operations or missions to protect critical infrastructure.
Status: 05/04/2021 Referred to the House Committee on Armed Services.
Link: H.R.2982 - 117th Congress (2021-2022): National Guard Cybersecurity Support Act

H.R. 3000, Inspire to Serve Act of 2021

Overview: This bill establishes new and expands existing military and national service programs, and revises federal personnel provisions. The bill establishes programs relating to civic education and service learning, including by providing grants supporting these programs for grades K-12 and at institutions of higher education.
Status: 11/09/2021 Referred to the Subcommittee on Courts, Intellectual Property, and the Internet.
Link: HR3000 - 117th Congress (2021-2022): Inspire to Serve Act of 2021 | Congress.gov | Library of Congress

H.R. 3078, Pipeline and LNG Facility Cybersecurity Preparedness Act

Overview: This bill requires the Department of Energy to implement a program to ensure the security, resiliency, and survivability of natural gas pipelines, hazardous liquid pipelines, and liquefied natural gas facilities.
Status: 06/10/2021 Ordered to be Reported by Voice Vote.
Link: H.R.3078 - 117th Congress (2021-2022): Pipeline and LNG Facility Cybersecurity Preparedness Act

H.R. 3243, Pipeline Security Act

Overview: This bill revises the duties of the Transportation Security Administration (TSA) to include securing pipelines and pipeline facilities against cybersecurity threats, acts of terrorism, and other acts that jeopardize the physical security or cybersecurity of the pipelines or facilities.
Status: Passed out of the Committee on Homeland Security (July 13, 2021).
Link: H.R.3243 - 117th Congress (2021-2022): Pipeline Security Act

H.R. 3262, GUARD Act

Overview: This bill requires the Department of Transportation (DOT) to study the state of cybersecurity regarding motor vehicles, including by developing a comprehensive list of federal agencies with jurisdiction over cybersecurity and a brief description of the jurisdiction or expertise of such agencies.
Status: 05/17/2021 Referred to the Subcommittee on Consumer Protection and Commerce.
Link: H.R.3262 - 117th Congress (2021-2022): GUARD Act

H.R. 3608, Improving Contractor Cybersecurity Act
Overview: This bill prohibits an executive agency from entering into a contract for information technology unless the contractor maintains a vulnerability disclosure policy (VDP) and program.
Status: 05/28/2021 Referred to the House Committee on Oversight and Reform.
Link: H.R.3608 - 117th Congress (2021-2022): Improving Contractor Cybersecurity Act

H.R. 3723, Consumer Safety Technology Act
Overview: This bill requires various agencies to explore the use of emerging technologies in the context of consumer products and safety.
Status: Passed House (06/23/2021). 06/24/2021 Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation.
Link: H.R.3723 - 117th Congress (2021-2022): Consumer Safety Technology Act

H.R. 3747, Securing American Research from Cyber Theft Act
Overview: This bill establishes a pilot program and modifies a current program related to cybersecurity for federally supported research and data.
Status: 06/08/2021 Referred to the House Committee on Science, Space, and Technology.
Link: 117th Congress (2021-2022): Securing American Research from Cyber Theft Act

H.R. 4046, NTIA Policy and Cybersecurity Coordination Act
Overview: This bill establishes within the National Telecommunications and Information Administration the Office of Policy Development and Cybersecurity to oversee and conduct national communications and information policy analysis and development for the internet and communications technologies.
Status: 12/30/2022 Placed on the Union Calendar, Calendar No. 487.
Link: H.R.4046 - 117th Congress (2021-2022): NTIA Policy and Cybersecurity Coordination Act

H.R. 4355, Military Construction, Veterans Affairs, and Related Agencies Appropriations Act, 2022
Overview: This bill provides FY2022 appropriations for military construction, the Department of Veterans Affairs (VA), and related agencies.
Status: 07/02/2021 Placed on the Union Calendar, Calendar No. 56.
Link: 117th Congress (2021-2022): Military Construction, Veterans Affairs, and Related Agencies Appropriations Act, 2022

H.R. 4513, Small Business Advanced Cybersecurity Enhancements Act of 2021
Overview: This bill requires the Small Business Administration (SBA) to establish a central small business cybersecurity-assistance unit within the SBA and a regional cybersecurity-assistance unit within each small business development center. These units shall serve as the primary means for a small business to communicate cyber threats and defensive measures with the federal government, and the bill prohibits any cause of action against a small business for such communication or for any conduct in response to such communication.
Status: 10/12/2021 Placed on the Union Calendar, Calendar No. 102.
Link: HR4513 - Small Business Advanced Cybersecurity Enhancements Act of 2021117th Congress (2021-2022)

H.R. 4977, Better Cybercrime Metrics Act
Overview: This bill establishes various requirements to improve the collection of data related to cybercrime and cyber-enabled crime (cybercrime).
Status: 12/08/2021 Ordered to be Reported (Amended) by Voice Vote.
Link: HR4977 - 117th Congress (2021-2022): Better Cybercrime Metrics Act | Congress.gov | Library of Congress

H.R. 5138, Federal Cybersecurity Workforce Expansion Act
Overview: This bill establishes an apprenticeship program and a pilot program on cybersecurity.
Status: 9/21/2021 Referred to the Subcommittee on Technology Modernization.
Link: HR5138 - 117th Congress (2021-2022): Federal Cybersecurity Workforce Expansion Act | Congress.gov | Library of Congress

H.R. 5156, START Act
Overview: This bill directs the Department of Transportation (DOT), in coordination with any other applicable federal agencies to create, publish, and make available to the public online a Smart Community Resource Center to assist states and local communities in developing and implementing intelligent transportation system programs and smart city or community transportation programs.
Status: 09/07/2021 Referred to the Subcommittee on Highways and Transit.
Link: https://www.congress.gov/bill/117th-congress/house-bill/5156

H.R. 5186, CISA Leadership Act
Overview: This bill establishes a term limit and specifies the appointment process for the Director of the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security.
Status: 09/07/2021 Referred to the Committee on Homeland Security, and in addition to the Committees on Energy and Commerce, and Oversight and Reform, 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.
Link: https://www.congress.gov/bill/117th-congress/house-bill/5186/

H.R. 5440, Cyber Incident Reporting for Critical Infrastructure Act
Overview: This bill requires reporting and other actions to address cybersecurity incidents, including ransomware attacks.
Status: 09/30/2021 Referred to the House Committee on Homeland Security.
Link: https://www.congress.gov/bill/117th-congress/house-bill/5440

H.R. 5491, Securing Systemically Important Critical Infrastructure Act
Overview: This bill sets out a process to designate elements of critical infrastructure as systemically important. *Critical infrastructure* refers to the machinery, facilities, and information that enable vital functions of governance, public health, and the economy.
Status: 10/06/2021 Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation.
Link: 117th Congress (2021-2022): Securing Systemically Important Critical Infrastructure Act

H.R. 6084, Energy Product Reliability Act
Overview: With the start of a new Congress, summaries from prior Congresses may be delayed or abbreviated.
Status: 12/01/2021 Referred to the Subcommittee on Energy.
Link: HR6084 - 117th Congress (2021-2022): Energy Product Reliability Act

H.R. 6197, Streamline DoD Cyber Recruitment Act
Overview: This bill requires the Department of Defense (DOD) to study the establishment of a designated central program office within DOD to oversee all academic engagement programs focusing on cyber talent across DOD.
Status: 12/08/2021 Referred to the House Committee on Armed Services.
Link: 117th Congress (2021-2022): Streamline DoD Cyber Recruitment Act

H.R. 6416, Banning Surveillance Advertising Act of 2022
Overview: This bill restricts online advertising that targets an individual, internet-connected device, or group of individuals or devices based on personal information. Personal information includes information that is reasonably linkable to an individual or connected device such as internet browsing history or the content of communications.
Status: 01/19/2022 Referred to the Subcommittee on Consumer Protection and Commerce.
Link: 117th Congress (2021-2022): Banning Surveillance Advertising Act of 2022

H.R. 6580, Algorithmic Accountability Act of 2022
Overview: A summary is in progress.
Status: 02/04/2022 Referred to the Subcommittee on Consumer Protection and Commerce.
Link: HR6580 - 117th Congress (2021-2022): Algorithmic Accountability Act of 2022

H.R. 6755, Cooperation Among Police, Tech and Users to Resist Exploitation Act (the CAPTURE Act)
Overview: This bill directs the Government Accountability Office to study and report to Congress on cooperation between social media companies and law enforcement to address illegal content and activity online.
Status: 02/22/2022 Referred to the Subcommittee on Consumer Protection and Commerce.
Link: HR6755 - 117th Congress (2021-2022): CAPTURE Act

H.R. 6786, Digital Services Oversight and Safety Act of 2022
Overview: This bill requires the Federal Trade Commission and the Department of Justice to develop, and make publicly available, an educational program to inform consumers about the resources available when their safety and security has been violated online.
Status: 02/22/2022 Referred to the Subcommittee on Consumer Protection and Commerce.
Link: HR6786 - 117th Congress (2021-2022): Increasing Consumers' Education on Law Enforcement Resources Act

H.R. 7900, National Defense Authorization Act for Fiscal Year 2023
Overview: This bill authorizes Department of Defense (DOD) activities for FY2023 and addresses other issues.
Status: Passed the House. (A version of this was passed in HR 7776 FY23 NDAA)
Link: H.R.7900 - 117th Congress (2021-2022): National Defense Authorization Act for Fiscal Year 2023

H.R. 8152, American Data Privacy and Protection Act (Federal privacy bill):
Overview: This bill establishes requirements for how companies, including nonprofits and common carriers, handle personal data, which includes information that identifies or is reasonably linkable to an individual. Specifically, the bill requires most companies to limit the collection, processing, and transfer of personal data to that which is reasonably necessary to provide a requested product or service and to other specified circumstances. It also generally prohibits companies from transferring individuals' personal data without their affirmative express consent. The bill establishes consumer data protections, including the right to access, correct, and delete personal data. Prior to engaging in targeted advertising, the bill requires companies to provide individuals with a means to opt out of such advertising. The bill also provides additional protections with respect to personal data of individuals under the age of 17. It further prohibits companies from using personal data to discriminate based on specified protected characteristics. Additionally, companies must implement security practices to protect and secure personal data against unauthorized access, and the Federal Trade Commission (FTC) may issue regulations for complying with this requirement. The bill provides for enforcement of these requirements by the FTC and state attorneys general. Beginning four years after the bill's enactment, individuals may, subject to certain notification requirements, bring civil actions for violations of the bill. Finally, the bill preempts state laws that are covered by the provisions of the bill except for certain categories of state laws and specified laws in Illinois and California.
Status: Passed by the House Energy & Commerce, 53 - 2.
Link: H.R.8152 - 117th Congress (2021-2022): American Data Privacy and Protection Act

H.R. 8215, VOICE Act of 2022
Overview: This bill requires the Department of Veterans Affairs to establish a program to promote digital citizenship and media literacy among veterans by awarding grants to eligible entities, which include civil society organizations and congressionally chartered veterans service organizations.
Status: 07/19/2022 Ordered to be Reported by the Yeas and Nays: 17 - 13.
Link: H.R.8215 - 117th Congress (2021-2022): VOICE Act of 2022

H.R. 8279, Building Cyber Resilience After SolarWinds Act of 2022
Overview: This bill requires evaluations of the impact of the SolarWinds cyber incident and the activities of the Cyber Safety Review Board.
Status: 07/01/2022 Referred to the Committee on Oversight and Reform, and in addition to the Committee on 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.
Link: https://www.congress.gov/bill/117th-congress/house-bill/8279

H.R. 8367, Intelligence Authorization Act for Fiscal Year 2023
Overview: With the start of a new Congress, summaries from prior Congresses may be delayed or abbreviated.

Status: 10/31/2022 Placed on the Union Calendar, Calendar No. 392.
Link: H.R.8367 - 117th Congress (2021-2022): Intelligence Authorization Act for Fiscal Year 2023

H.R. 8403, Proactive Cyber Initiatives Act of 2022

Overview: This bill addresses proactive cybersecurity initiatives. Specifically, each department or agency must (1) conduct regular penetration testing on the information systems of such department or agency; and (2) provide to the Cybersecurity and Infrastructure Security Agency (CISA) and the Office of Management and Budget a report on the results of such testing, including identifying any risks discovered and describing how cybersecurity may be improved.
Status: 07/15/2022 Referred to the Committee on Oversight and Reform, and in addition to the Committee on Armed Services, 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.
Link: https://www.congress.gov/bill/117th-congress/house-bill/8403

H.R. 8803, IGNITE HBCU, TCU, and MSI Excellence Act

Overview: To provide for the long-term improvement of minority-serving institutions, and for other purposes, including strengthening "the safety and security of the campus of such entity by improving or utilizing design elements, principles, and technology . . . ."
Status: 09/13/2022 Referred to the House Committee on Education and Labor
Link: H.R.8803 - 117th Congress (2021-2022): IGNITE HBCU, TCU, and MSI Excellence Act

H.R. 8806, Healthcare Cybersecurity Act of 2022

Overview: This bill requires the Cybersecurity and Infrastructure Security Agency (CISA) to undertake activities to improve the cybersecurity of the health care and public health sector.
Status: 09/14/2022 Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation.
Link: https://www.congress.gov/bill/117th-congress/house-bill/8806

H.R. 8950, Digital Commodities Consumer Protection Act of 2022

Overview: This bill grants exclusive jurisdiction to the Commodity Futures Trading Commission over activity involving digital commodities as specified by the bill.
Status: 10/28/2022 Referred to the Subcommittee on Commodity Exchanges, Energy, and Credit.
Link: https://www.congress.gov/bill/117th-congress/house-bill/8950

H.R. 9228, Ensuring Cybersecurity at the NIH Act of 2022

Overview: With the start of a new Congress, summaries from prior Congresses may be delayed or abbreviated.
Status: 10/25/2022 Referred to the House Committee on Energy and Commerce.
Link: https://www.congress.gov/bill/117th-congress/house-bill/9228

H.R. 9229, Department of Health and Human Services Cybersecurity Coordination Act

Overview: A summary is in progress.
Status: 10/26/2022 Referred to the Subcommittee on Health.
Link: https://www.congress.gov/bill/117th-congress/house-bill/9229

H.R. 9234, Critical Electric Infrastructure Cybersecurity Incident Reporting Act
Overview: To direct the Secretary of Energy to promulgate regulations to facilitate the timely submission of notifications regarding cybersecurity incidents and potential cybersecurity incidents with respect to critical electric infrastructure, and for other purposes.
Status: 10/25/2022 Referred to the House Committee on Energy and Commerce.
Link: https://www.congress.gov/bill/117th-congress/house-bill/9234

H.R. 9259, Cybersecurity Skills Integration Act
Overview: This bill requires the Department of Education to establish a pilot program in order to award grants to partnerships between postsecondary educational institutions and employers in critical infrastructure sectors for cybersecurity education programs.
Status: 10/31/2022 Referred to the House Committee on Education and Labor.
Link: https://www.congress.gov/bill/117th-congress/house-bill/9259

H.R. 9262, To make improvements to cybersecurity acquisition policies of the Department of Defense, and for other purposes.
Overview: This bill requires the Defense Acquisition University of the Department of Defense (DOD) to develop training curricula related to software acquisitions and cybersecurity software or hardware acquisitions and offer the training to applicable DOD contracting officers and individuals with specified acquisition positions. Additionally, DOD must submit to Congress a plan to streamline approval processes related to information assurance and cybersecurity for software acquisitions.
Status: 11/03/2022 Referred to the House Committee on Armed Services.
Link: H.R.9262 - 117th Congress (2021-2022): To make improvements to cybersecurity acquisition policies of the Department of Defense, and for other purposes.

H.R. 9356, RESILIENCE Act of 2022
Overview: To establish a pilot program for State, local, Tribal, and territorial government officials to be trained by the Cybersecurity and Infrastructure Security Agency regarding carrying out security vulnerability or terrorism risk assessments of critical infrastructure facilities, and for other purposes.
Status: 11/22/2022 Referred to the House Committee on Homeland Security.
Link: https://www.congress.gov/bill/117th-congress/house-bill/9356

H.R. 9420 - Cybersecurity Education Task Force Act of 2022
Overview: This bill requires the Office of the National Cyber Director to establish the Cyber Education Task Force. The task force must issue recommendations and guidance for increasing and promoting cybersecurity courses, degrees, and programs in institutions of higher education to improve the diversity of the cybersecurity workforce.
Status: 12/02/2022 Referred to the House Committee on Education and Labor.
Link: https://www.congress.gov/bill/117th-congress/house-bill/9420

S. 70, National Guard Cybersecurity Support Act

Overview: This bill authorizes members of the National Guard to perform, at the request of a state and in connection with training or other duty, cybersecurity operations or missions to protect critical infrastructure.
Status: Senate - 01/27/2021 - Introduced and referred to the Committee on Armed Services.
Link: S.70 - 117th Congress (2021-2022): National Guard Cybersecurity Support Act

S. 161, SECURE Small Business Act

Overview: This bill requires the Small Business Administration (SBA) to help small businesses purchase cybersecurity products and services.
Status: 02/02/2021 - Introduced and referred to the Committee on Small Business and Entrepreneurship.
Link: S.161 - 117th Congress (2021-2022): SECURE Small Business Act | Congress.gov | Library of Congress

S. 745, Accessible, Affordable Internet for All Act

Overview: This bill reauthorizes through FY2026, revises, and establishes grants and activities to promote access to telecommunications services, including broadband internet.
Status: 03/15/2021 Read twice and referred to the Committee on Commerce, Science, and Transportation.
Link: S.745 - 117th Congress (2021-2022): Accessible. Affordable Internet for All Act

S. 808, Cybersecurity Disclosure Act

Overview: This bill directs the Securities and Exchange Commission to issue final rules requiring a registered issuer of securities to disclose in its mandatory annual report or annual proxy statement whether any member of its governing body has expertise or experience in cybersecurity. If no member has such expertise or experience, the issuer must describe what other company cybersecurity aspects were taken into account by the persons responsible for identifying and evaluating nominees for the governing body.
Status: 09/14/2021 Committee on Banking, Housing, and Urban Affairs. Hearings held.
Link: S.808 - 117th Congress (2021-2022): Cybersecurity Disclosure Act of 2021

S. 965, Cyber Shield Act

Overview: This bill requires the Department of Commerce to establish the Cyber Shield Program, a voluntary program to identify and certify covered products. These products are consumer-facing physical objects that meet industry-leading cybersecurity and data security benchmarks and that can (1) connect to the internet; and (2) collect, send, or receive data or control the actions of a physical object or system. Commerce must also establish a Cyber Shield Advisory Committee to recommend (1) the format and content of Cyber Shield labels for covered products; and (2) the process to identify, establish, report on, adopt, maintain, and promote compliance with industry-leading cybersecurity and data security benchmarks to enhance cybersecurity and protect data. On its website, Commerce must make publicly available (1) program information, (2) a database of covered products certified under the program, and (3) contact information for each manufacturer of a covered product certified under the program.

Status: 03/25/2021 - Read twice and referred to the Committee on Commerce, Science and Transportation.
Link: S.965 - 117th Congress (2021-2022): Cyber Shield Act of 2021

S. 1316, Cyber Response and Recovery Act of 2021

Overview: This bill authorizes the Department of Homeland Security (DHS) to declare a significant incident in the event of a breach of a public or private network and establishes a Cyber Response and Recovery Fund. Specifically, DHS may make the declaration upon determining that a specific significant incident has occurred or is likely to occur imminently and that otherwise available resources, other than the fund, are likely insufficient to respond to or mitigate the incident effectively. Upon a declaration, the Cybersecurity and Infrastructure Security Agency must coordinate (1) the response activities of each federal agency; and (2) with other responding entities, including local governments and law enforcement agencies. The fund shall be available for the coordination of such activities and for response and recovery support.
Status: 12/14/2022 Placed on Senate Legislative Calendar under General Orders. Calendar No. 648.
Link: S.1316 - 117th Congress (2021-2022): Cyber Response and Recovery Act of 2021

S. 1324, Civilian Cyber Security Reserve Act

Overview: This bill authorizes the Department of Homeland Security and the Department of Defense to each create a temporary Civilian Cyber Security Reserve within their agencies to address U.S. cybersecurity needs with respect to national security. Reserve members must be former federal employees or former military personnel, have cybersecurity expertise, and obtain any necessary security clearances, in addition to any other criteria specified by each agency. Membership in the reserves is contingent on a mutual agreement between the agency and the individual. Reserves may consist of different components, with one component obligated to respond to a call to activation and the other not obligated to do so; each agency may establish penalties for those individuals who fail to respond when required. The Government Accountability Office and each agency must evaluate and report on the reserves, including whether they should be made permanent.
Status: 12/21/2022 Message on Senate action sent to the House.
Link: S.1324 - 117th Congress (2021-2022): Civilian Cyber Security Reserve Act

S. 1350, National Risk Management Act

Overview: This bill requires the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency to identify, assess, and prioritize risks to critical infrastructure and requires the President to deliver to Congress a national critical infrastructure resilience strategy designed to address the risks identified.
Status: 12/15/2022 Placed on Senate Legislative Calendar under General Orders. Calendar No. 652.
Link: S.1350 - 117th Congress (2021-2022): National Risk Management Act of 2021

S. 2134, The Data Protection Act

Overview: The bill would establish the Data Protection Agency, an independent agency to regulate specified high-risk data practices and the collection, processing, and sharing of personal data. This includes the transfer of the powers and duties with respect to specified federal privacy laws from the Federal Trade Commission to the agency.

Status: 06/17/2021 Read twice and referred to the Committee on Commerce, Science, and Transportation.
Link: https://www.congress.gov/bill/117th-congress/senate-bill/2134

S. 2274, Federal Cybersecurity Workforce Expansion Act

Overview: To authorize the Director of the Cybersecurity and Infrastructure Security Agency to establish an apprenticeship program and to establish a pilot program on cybersecurity training for veterans and members of the Armed Forces transitioning to civilian life, and for other purposes.
Status: 7/18/2022 Placed on Senate Legislative Calendar under General Orders. Calendar No. 446.
Link: S.2274 - 117th Congress (2021-2022): Federal Cybersecurity Workforce Expansion Act

S. 2305, Cybersecurity Opportunity Act

Overview: This bill requires the Department of Homeland Security to award grants to specified institutions of higher education for establishing or expanding cybersecurity education programs and opportunities.
Status: Reported out of Committee on Homeland Security and Governmental Affairs (Jan 20, 2022).
Link: S.2305 - 117th Congress (2021-2022): Cybersecurity Opportunity Act | Congress.gov | Library of Congress

S. 2377, Energy Infrastructure Act

Overview: This bill addresses energy infrastructure, clean energy supply chains, carbon capture and storage, ecosystem restoration, and western water infrastructure.
Status: Passed by the Committee on Energy and Natural Resources (July 19, 2021).
Link: S.2377 - 117th Congress (2021-2022): Energy Infrastructure Act | Congress.gov | Library of Congress

S. 2407, Cyber Incident Notification Act

Overview: This bill requires federal agencies and certain entities to report cybersecurity intrusion incidents to the Cybersecurity and Infrastructure Security Agency (CISA) and addresses related issues.
Status: Referred to the Committee on Homeland Security and Governmental Affairs (July 21, 2021).
Link: S.2407 - 117th Congress (2021-2022): Cyber Incident Notification Act of 2021

S. 2439, DHS Industrial Control Systems Capabilities Enhancement Act

Overview: This bill requires the Cybersecurity and Infrastructure Security Agency (CISA) to maintain certain capabilities to identify and address threats to industrial control systems. Specifically, the bill requires CISA's National Cybersecurity and Communications Integration Center to ensure that its activities address the security of both information and operational technology, including industrial control systems.Additionally, CISA must maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes by (1) leading efforts to identify and mitigate cybersecurity threats to industrial control systems; (2) maintaining threat hunting and incident response capabilities to respond to cybersecurity risks and incidents; (3) providing cybersecurity technical assistance to stakeholders; and (4) collecting, coordinating, and providing vulnerability information to the industrial control systems community. CISA shall provide to the homeland security committees a briefing on its industrial control systems capabilities at specified intervals. The Government Accountability Office

must review and report on implementation of the bill's requirements.
Status: 12/13/2022 Placed on Senate Legislative Calendar under General Orders.
Link: S.2439 - 117th Congress (2021-2022): DHS Industrial Control Systems Capabilities Enhancement Act of 2021

S. 2483, Improving Cybersecurity of Small Organizations Act

Overview: This bill requires the Cybersecurity and Infrastructure Security Agency (CISA) to maintain and promote cybersecurity guidance for use by small organizations.
Specifically, the bill requires CISA to maintain cybersecurity guidance that documents and promotes evidence-based cybersecurity policies and controls for use by small organizations to improve their cybersecurity. This guidance must be publicly available at no cost, and CISA, the Small Business Administration (SBA), and the Department of Commerce must promote the guidance through relevant resources that are regularly used by small organizations. Commerce must report on methods of incentivizing small organizations to improve their cybersecurity, including through the adoption of policies, controls, products, and services that have been demonstrated to reduce cybersecurity risk. Every two years, the SBA must submit and make publicly available specified data on the state of small businesses' cybersecurity.
Status: 12/05/2022 Placed on Senate Legislative Calendar under General Orders. Calendar No. 573.
Link: S.2483 - 117th Congress (2021-2022): Improving Cybersecurity of Small Organizations Act of 2021

S. 2491, Defense of United States Infrastructure Act

Overview: This bill sets out programs and requirements related to critical infrastructure and cybersecurity threats.
Status: 12/19/2022 Placed on Senate Legislative Calendar under General Orders. Calendar No. 670.
Link: S.2491 - 117th Congress (2021-2022): Defense of United States Infrastructure Act of 2021

S. 2540, CISA Technical Corrections and Improvements Act

Overview: This bill makes technical corrections to certain statutes relating to cybersecurity. To make technical corrections to title XXII of the Homeland Security Act of 2002, and for other purposes (including definition of ISACs).
Status: 12/13/2022 Placed on Senate Legislative Calendar under General Orders. Calendar No. 632.
Link: S.2540 - 117th Congress (2021-2022): CISA Technical Corrections and Improvements Act of 2021

S. 2666, Sanction and Stop Ransomware Act

Overview: This bill addresses ransomware threats to national security.
Status: 08/05/2021 Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
Link: https://www.congress.gov/bill/117th-congress/senate-bill/2666/

S. 2699, American Cybersecurity Literacy Act

Overview: This bill requires the National Institute of Standards and Technology to develop and conduct a cybersecurity literacy campaign to increase knowledge and awareness of best practices to reduce cybersecurity risks.
Status: Passed out of Committee on Commerce, Science, and Transportation on 12/17/2021 Placed on Senate Legislative Calendar under General Orders. Calendar No. 221.

Link: S.2699 - 117th Congress (2021-2022): American Cybersecurity Literacy Act | Congress.gov | Library of Congress

S. 2792, National Defense Authorization Act for Fiscal Year 2022
Overview: This bill authorizes Department of Defense (DOD) activities for FY2022 and addresses related issues.
Status: 09/22/2021 An errata sheet on written report No. 117-39 was printed. A related bill, S. 1605, the National Defense Authorization Act, passed both houses and became Public Law No: 117-81 (Dec 27, 2021).
Link: S.2792 - 117th Congress (2021-2022): National Defense Authorization Act for Fiscal Year 2022

S. 3396, Department of Defense Principal Cyber Advisor Empowerment Act
Overview: To improve the position of the Principal Cyber Advisor, and for other purposes.
Status: 12/15/2021 Read twice and referred to the Committee on Armed Services.
Link: S.3396 - 117th Congress (2021-2022): Department of Defense Principal Cyber Advisor Empowerment Act of 2021

S. 3904, Healthcare Cybersecurity Act of 2022
Overview: This bill requires the Department of Health and Human Services (HHS) to undertake activities to improve the cybersecurity of the health care and public health sector.
Status: Passed out of Committee (Oct 18, 2022) and placed on Senate Legislative Calendar under General Orders. Calendar No. 527.
Committee Report: report No. 117-177.
Link: S.3904 - 117th Congress (2021-2022): Healthcare Cybersecurity Act of 2022

S. 4490, Digital Citizenship and Media Literacy
Overview: This bill directs the National Telecommunications and Information Administration to award grants to state and local educational agencies, public libraries, and qualified nonprofit organizations to develop and promote media literacy and digital citizenship education for elementary and secondary school students.
Status: 07/28/2022 Referred to the Committee on Commerce, Science, and Transportation
Link: S.4490 - 117th Congress (2021-2022): Digital Citizenship and Media Literacy Act

S. 4493, Veterans Online Information and Cybersecurity Empowerment Act of 2022
Overview: This bill requires the Department of Veterans Affairs to establish a program to promote digital citizenship and media literacy among veterans by awarding grants to eligible entities, which include civil society organizations and congressionally chartered veterans service organizations.
Status: 06/23/2022 Read twice and referred to the Committee on Veterans' Affairs.
Link: S.4493 - 117th Congress (2021-2022): Veterans Online Information and Cybersecurity Empowerment Act of 2022

S. 4503, Intelligence Authorization Act for Fiscal Year 2023
Overview: With the start of a new Congress, summaries from prior Congresses may be delayed or abbreviated.

Status: 07/20/2022 By Senator Warner from Select Committee on Intelligence filed a written report. Report No. 117-132. Additional views filed.
Link: S.4503 - 117th Congress (2021-2022): Intelligence Authorization Act for Fiscal Year 2023

S. 4528, Improving Digital Identity Act of 2022

Overview: This bill establishes the Improving Digital Identity Task Force to establish a government-wide effort to develop secure methods for governmental agencies to protect the privacy and security of individuals and support reliable, interoperable digital identity verification in the public and private sectors.
Status: 09/28/2022 Committee on Homeland Security and Governmental Affairs. Ordered to be reported with an amendment in the nature of a substitute favorably.
Link: S.4528 - 117th Congress (2021-2022): Improving Digital Identity Act of 2022

S. 4592, Quantum Computing Cybersecurity Preparedness Act

Overview: This bill addresses the migration of executive agencies information technology systems to post-quantum cryptography. Post-quantum cryptography is encryption strong enough to resist attacks from quantum computers developed in the future.
Status: 12/13/2022 Placed on Senate Legislative Calendar under General Orders. Calendar No. 635.
Link: S.4592 - 117th Congress (2021-2022): Quantum Computing Cybersecurity Preparedness Act

S. 4623, AGILE Procurement Act

Overview: This bill addresses federal procurement policy and barriers to entry in federal contracting.
Status: 11/17/2022 Placed on Senate Legislative Calendar under General Orders. Calendar No. 561.
Link: S.4623 - 117th Congress (2021-2022): AGILE Procurement Act of 2022

S. 4629, Federal Data Center Enhancement Act

Overview: This bill modifies requirements relating to data centers of federal agencies and extends the sunset of provisions regarding the federal data center consolidation initiative.
Status: 11/17/2022 Placed on Senate Legislative Calendar under General Orders. Calendar No. 562.
Link: S.4629 - 117th Congress (2021-2022): Federal Data Center Enhancement Act of 2022

S. 4698, Improving Cybersecurity of Credit Unions Act

Overview: With the start of a new Congress, summaries from prior Congresses may be delayed or abbreviated.
Status: 11/15/2022 Committee on Banking, Housing, and Urban Affairs. Hearings held.
Link: S.4698 - 117th Congress (2021-2022): Improving Cybersecurity of Credit Unions Act

S. 4701, Small Business Cybersecurity Act

Overview: With the start of a new Congress, summaries from prior Congresses may be delayed or abbreviated.
Status: Senate - 08/02/2022 Read twice and referred to the Committee on Small Business and Entrepreneurship.
Link: https://www.congress.gov/bill/117th-congress/senate-bill/4701

S. 4913, Securing Open Source Software Act of 2022
Overview: This bill sets forth the duties of the Cybersecurity and Infrastructure Security Agency (CISA) regarding open source software security.
CBO Cost Estimate for S. 4913: https://www.cbo.gov/system/files/2022-11/s4913.pdf
Status: Passed by Senate Homeland Security Committee (Dec 19, 2022).
Link: S.4913 - 117th Congress (2021-2022): Securing Open Source Software Act of 2022

STATE ACTION

State Legislation

Passed into law

State of Connecticut: S. 6: Act Concerning Personal Data Privacy and Online Monitoring
Overview: Connecticut became the fifth state to enact a comprehensive consumer privacy law, following California, Virginia, Colorado, and Utah. The law grants Connecticut consumers new privacy rights and requires data protection obligations for businesses.
Status: Governor signed the bill into law on May 10, 2022. The effective date is January 1, 2023.
Link: Substitute Senate Bill No. 6 - Public Act No. 22-15

State of Utah: S.B. 227, the Consumer Privacy Act
Overview: Utah became the fourth state to enact a comprehensive consumer privacy law, following California, Virginia, and Colorado. The law grants Utah consumers several new rights over the personal data that they previously provided to a business, including the right to: (1) know or confirm processing activity; (2) access personal data; (3) obtain a copy of personal data in a portable & readily usable format; (4) delete personal data; (6) opt out of targeted advertising and sales of personal information; and (7) avoid discrimination as a result of exercising their consumer rights under the new law.
Status: Governor signed the bill into law on March 24, 2022. The effective date is December 31, 2023.
Link: SB0227

State of North Carolina: Public Sector Organizations Prohibited from Paying Ransom in Ransomware Attack
Overview: North Carolina prohibited state and local government organizations from paying ransom in a ransomware attack: CYBERSECURITY/STATE AGENCIES PROHIBITED FROM MAKING RANSOMWARE PAYMENTS, SECTION 38.13.(a) Chapter 143 of the General Statutes is amended by adding a new Article to read:"Article 84. "Various Technology Regulations: *"No State agency or local government entity shall submit payment or otherwise communicate with an entity that has engaged in a cybersecurity incident on an information technology system by encrypting data and then subsequently offering to decrypt that data in exchange for a ransom payment."*
Status: Governor signed into law on November 18, 2021
Link: SL 2021-180 (SB 105)

State of Connecticut: H.B. No. 6077, an Act Incentivizing the Adoption of Cybersecurity Standards for Businesses
Overview: Incentivizes voluntary adoption of cybersecurity best practices, including the CIS Critical Security Controls, by creating a cap against punitive damages in a lawsuit resulting from a data breach.
Status: Governor signed into law on July 6, 2021. Effective date: October 1, 2021. Passed the Senate on June 7, 2021. Passed the House of Representatives on May 20, 2021.

Link: Text of Public Act No. 21-118 (CIS Controls at page 4): Substitute House Bill No. 6607 - Public Act No. 21-119

State of Utah: H.B. 80, the Cybersecurity Affirmative Defense Act
Overview: Incentivizes voluntary adoption of cybersecurity best practices, including the CIS Critical Controls, by creating an affirmative defense against lawsuits resulting from a data breach.
Status: Governor signed into law on March 11, 2021. Effective date: May 5, 2021.
Link: Text of enrolled bill (CIS Controls at page 5): Enrolled Copy HB 80 1 DATA SECURITY AMENDMENTS

Other bills of interest:

State of Massachusetts: H. 4514 & S. 2687, the Massachusetts Information Privacy & Security Act

Overview: This bill combines a consumer data privacy provision with an incentive to voluntarily adopt cyber best practices, like the CIS Critical Security Controls.

Status: A "study order" of the House version of this bill has been reported out of the Joint Health Care Financing Committee and sent to the House Rules Committee, which must act before Dec. 31, 2022. Did not pass.

Link: MA H4514 | 2021-2022 | 192nd General Court | LegiScan

State of New Jersey: S. 1860, Creates affirmative defense for breaches of security.
Overview: This bill would incentivize voluntary adoption of cybersecurity best practices, including the CIS Controls, by creating an affirmative defense against lawsuits resulting from a data breach.

Status: Pending: Senate Economic Growth Committee. Did not pass.

Link: https://legiscan.com/NJ/text/S1860/id/2532935

State of Nevada: S.B. No. 239, An Act Relating to Cybersecurity
Overview: This bill would incentivize voluntary adoption of cybersecurity best practices, including the CIS Critical Security Controls, by creating an affirmative defense against lawsuits resulting from a data breach.
Status: Failed to get a hearing so the bill will not proceed this session. Introduced on March 15, 2021.
Link: SB239 Overview

Executive Orders

Kansas Governor Laura Kelly Signs Executive Order No. 21-25: Establishing the Governor's Cybersecurity Task Force (July 13, 2021):

- Executive Order No. 21-25, establishing the Governor's Cybersecurity Task Force.

Reports

Idaho Governor Brad Little Convenes a Cybersecurity Task Force (August 5, 2021):

- The Task Force will focus on identifying cybersecurity assets, resources, public-private partnerships; promoting improved business, government, and personal cybersecurity procedures; ensure secure, transparent and resilient election infrastructure; and enhancing the educational pipeline for cybersecurity workforce needs.
- Cybersecurity - Idaho Commerce

New York State Department of Financial Services Report on the SolarWinds Cyber Espionage Attack and Institutions' Response (April 2021):

- **Overview:** Following the SolarWinds cyber espionage attack (the "Attack") and the resulting focus on supply chain risk, the New York Department of Financial Services (NYDFS) has issued a report detailing the impact on and responses by its regulated covered entities to the Attack.
- **Article:** https://www.alstonprivacy.com/nydfs-issues-report-on-the-solarwinds-attack-and-covered-entities-responses

NON-GOVERNMENTAL RESOURCES (Reports, White Papers, etc.):

Institute for Security + Technology, Ransomware Task Force: *Blueprint for Ransomware Defense*:

- **Released**: August 2022
- **Overview:** The *Blueprint* curates a subset of the CIS Critical Security Controls that represents essential cyber hygiene for all organizations. This single, authoritative source of best practices is an especially valuable roadmap for small- and medium-sized enterprises to help defend against ransomware.
- **Link**: https://securityandtechnology.org/ransomwaretaskforce/blueprint-for-ransomware-defense/

National Academy of Public Administration: A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation

- **Released:** January 2022
- The report recommends that the Office of the National Cyber Director lead the development of a government-wide strategy for developing the national cybersecurity workforce, in consultation with CISA, the Office of Management and Budget (OMB), and leaders of relevant federal agencies. Moreover, the Panel recommends that the strategy should include four key elements:
    - 1. Encouraging more people to choose a career in the cybersecurity field through outreach and education
    - 2. Enabling education and training to build needed competencies and alternative pathways to cybersecurity careers
    - 3. Overcoming barriers to recruiting talent and matching people to jobs
    - 4. Assessing performance and promoting innovation in workforce development practice
- **Link:** NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf (amazonaws.com)

THE ASPEN INSTITUTE: Commission on Information Disorder Final Report

- **Released**: November 15, 2021
- The report's recommendations fall into 3 categories:
    - **(1) Increasing Transparency and Understanding:** Enhancing access to and inquiry in social media platforms' practices, and more deeply examining the information environment and its interdependencies.
    - **(2) Building Trust:** Exploring the challenges the country faces in building and rebuilding trust in the institutions people count on to support informed public discourse and debate, and the role that access to reliable facts and content plays in those conversations.
    - **(3) Reducing Harms:** Mitigating the worst harms of mis- and disinformation, such as threats to public health and democratic participation, and the targeting of communities through hate speech and extremism.
- **Link**: Commission on Information Disorder Final Report - The Aspen Institute

Institute for Security + Technology Ransomware Task Force Report:

- **Released:** April 2021
- **Overview:** Over 60 experts from industry, government, law enforcement, civil society, and international organizations worked together to produce this comprehensive framework, which breaks down siloed approaches and advocates for a unified, aggressive, comprehensive, public-private anti-ransomware campaign.
- **Link:** Combating Ransomware - A Comprehensive Framework for Action

The Brennan Center for Justice: A Framework for Election Vendor Oversight

- **Released:** November 12, 2019
- **Overview:**
  - More than 80 percent of voting systems in use today are under the purview of three vendors.
  - A successful cyberattack against any of these companies could have devastating consequences for elections in vast swaths of the country.
  - Other systems that are essential for free and fair elections, such as voter registration databases and electronic pollbooks, are also supplied and serviced by private companies. Yet these vendors, unlike those in other sectors that the federal government has designated as critical infrastructure, receive little or no federal review. This leaves American elections vulnerable to attack.
- **Key Action/Aim:**
  - This report proposes a new framework for oversight that includes the following:
    - Independent oversight
    - Issuance of vendor best practices
    - Vendor certification
    - Ongoing review
    - Enforcement of guidelines
- Link to Report

MALWAREBYTES: CYBERCRIME TACTICS AND TECHNIQUES: THE 2019 STATE OF HEALTHCARE

- **Released on:** November 12, 2019
- **Overview:**
  - In this special report on healthcare, Malwarebytes focuses on the top threat categories and families that plagued the medical industry over the last year.
  - The report also highlights the security challenges inherent to organizations, from small private practices to enterprise health maintenance organizations (HMOs), as well as the reasons why hackers look to infiltrate their defenses.
- **Key Action/Aim:**
  - The report aims to educate those in healthcare IT and security to get ahead of the curve with an ounce of prevention before they need a pound of breach remediation.
- **Link** to Report

GLOBAL CYBER ALLIANCE: DNS ECONOMIC VALUE REPORT

- **Released on:** June 12, 2019

- **Overview:**
  - The Global Cyber Alliance reports that by using the Domain Name System (DNS) firewall, which is free to install, can prevent more than 33% of data breaches from occurring.
  - The study identified $10 billion in losses over the past five years that could have been prevented by DNS firewalls. The report goes on to claim that DNS can stop $150-200 billion in cybercrime losses annually.
- **Key Action/Aim:**
  - Side spread adoption of DNS firewalls to prevent losses to easily preventable hacks.
- Link to Report

STANFORD REPORT: SECURING OUR CYBER FUTURE

- **Released on:** June 6, 2019
- **Overview:**
  - As the Special Counsel report stated, "The Russian government interfered in the 2016 presidential election in sweeping and systematic fashion."1 More precisely, Russian President Vladimir Putin, his government, and his proxies deployed multiple strategies and instruments—media, doxing, covert operations, direct contacts with Trump associates, and cyber-attacks on U.S. electoral infrastructure—to influence the outcome of the 2016 U.S.
  - The report combines analysis from experts on cybersecurity, deterrence, Russia, social media companies, and American electoral regulations, as well as diplomacy, democracy and ethics. Gathering together this analyses the report attempts to answer what the Kremlin did, how the US countered it, and what the US should do in the future to prevent future interference.
- **Key Actions/Aims:**
  - Increase the Security of US Election Infrastructure
  - Regulate Online Political Advertising by Foreign Governments and Nationals
  - Confront Efforts at Election Manipulation from Foreign Media Organizations
  - Combat State-Sponsored Disinformation Campaigns from State-aligned Actors
  - Enhance Transparency about Foreign Involvement in U.S. Elections
  - Establish International Norms and Agreements to Prevent Election Interference
  - Deter Foreign Governments from Election Interference
- Link to Report page