# Recent Developments in Cybersecurity

DEPARTMENT OF LEGISLATIVE SERVICES 2022

# Recent Developments in Cybersecurity

**Department of Legislative Services**
**Office of Policy Analysis**
**Annapolis, Maryland**

**December 2022**

**Contributing Staff**

***Writers***
Hillary J. Cleckler Alcott
Tyler Allard

***Reviewer***
Amy A. Devadas

***Support Staff***
Maria S. Hartlein
Michael S. Raup

**For further information concerning this document contact:**

Library and Information Services
Office of Policy Analysis
Department of Legislative Services
90 State Circle
Annapolis, Maryland 21401

Baltimore Area: 410-946-5400 ● Washington Area: 301-970-5400
Other Areas: 1-800-492-7122, Extension 5400
TTY: 410-946-5401 ● 301-970-5401
TTY users may also use the Maryland Relay Service
to contact the General Assembly.

Email: libr@mlis.state.md.us
Home Page: http://dls.maryland.gov

# DEPARTMENT OF LEGISLATIVE SERVICES

OFFICE OF POLICY ANALYSIS
MARYLAND GENERAL ASSEMBLY

**Victoria L. Gruber**
Executive Director

**Ryan Bishop**
Director

December 2022

The Honorable Bill Ferguson, President of the Senate
The Honorable Adrienne A. Jones, Speaker of the House
Members of the Maryland General Assembly

Dear President Ferguson, Speaker Jones, and Members:

Cybersecurity remains a critical issue for governments at all levels and the private sector. Cyberattacks can have significant financial consequences and can affect a variety of services, including public utilities and healthcare. As technology evolves, so have cybersecurity-related laws and policies. This report is intended to serve as a resource for those deliberating cybersecurity issues. The report focuses on (1) recent legislation and other actions in Maryland to address cybersecurity issues; (2) the function and role of the Maryland Cybersecurity Council; (3) recent actions other states and the federal government have taken to address cybersecurity; and (4) cybersecurity insurance trends in response to the recent increase in cyberattacks.

The report was written by Hillary J. Cleckler Alcott and Tyler Allard. Amy A. Devadas reviewed the report. Maria S. Hartlein and Michael S. Raup provided administrative support.

I trust that this information will be of assistance to you.

Sincerely,

Victoria L. Gruber
Executive Director

Ryan Bishop
Director

VLG:RB/AAD/msr

# Contents

# Recent Developments in Cybersecurity

## Introduction

Cybersecurity has become a high priority for many lawmakers, especially in light of several recent, high profile cybersecurity attacks. These attacks, which can be at the hands of private actors or state-sponsored perpetrators, have the potential to wreak havoc on major supply chains, public utilities, hospitals, schools, national defense, private companies, and every level of government. Because of the increased frequency of these attacks and the operational disruptions and economic loss from these attacks, lawmakers are attempting to catch up with cyberattackers and technology by altering criminal statutes and increasing criminal penalties for these acts, establishing new entities or tasking existing entities with monitoring cybersecurity and developing and providing advice on best practices, and requiring private entities to meet specified cybersecurity standards and reporting requirements.

This report is intended to serve as a resource for those deliberating cybersecurity issues. It focuses on (1) recent legislation and other actions in Maryland to address cybersecurity issues; (2) the function and role of the Maryland Cybersecurity Council; (3) recent actions other states and the federal government have taken to address cybersecurity; and (4) cybersecurity insurance trends in response to the recent increase in cyberattacks.

## Recent Cybersecurity Attacks

### National Cybersecurity Attacks

The Center for Strategic and International Studies (CSIS), a bipartisan nonprofit policy research organization based in Washington, D.C., keeps a timeline of significant cyber incidents since 2006. CSIS focuses on cyberattacks on government agencies, defense, and high-tech companies, or economic crimes with losses of more than a million dollars. CSIS' list includes 8 significant cyber incidents in July 2022 and 13 significant cyber incidents in July 2021. In 2021, at least 67 individual ransomware attacks affected at least 954 schools and colleges.

In addition, in July 2021, it was revealed that hackers working for the Chinese government compromised more than a dozen U.S. pipeline operators approximately 10 years ago. In some instances, the hackers possessed the ability to damage or disrupt compromised pipelines, although it does not appear that they did. The Joseph R. Biden, Jr. Administration simultaneously announced cybersecurity requirements on the pipeline industry.

Listed below are examples of recent and noteworthy cybersecurity attacks.

- ***LastPass:*** On August 25, 2022, LastPass, a password manager with more than 33 million users, announced that a hacker recently took portions of source code and proprietary technical information. LastPass reported that customer passwords were not compromised.

- ***JBS Foods:*** On May 30, 2021, JBS Foods, the largest meat processing company in the world, determined that it was the target of a cyberattack that disrupted operations in North America and Australia. More specifically, meat processing was halted at all of the company's U.S. plants for a day, threatening to disrupt supply chains and inflate food prices. The FBI attributed the cyberattack to REvil, a Russian-speaking gang. JBS USA confirmed that it paid the equivalent of $11 million in ransom to mitigate any unforeseen issues related to the cyberattack and ensure that no data was exfiltrated.

- ***Colonial Pipeline:*** On May 7, 2021, Colonial Pipeline experienced a ransomware attack, requiring the company to take its pipeline system offline. Colonial Pipeline confirmed that it paid $4.4 million to a gang of hackers. Part of the reason behind the company's decision to pay the ransom was that tens of millions of Americans rely on Colonial Pipeline for fuel, including hospitals, first responders, airports, truck drivers, and the traveling public.

- ***Kaseya:*** On July 2, 2021, hackers attacked Kaseya, whose Virtual System Administrator software platform is typically used by other technology companies to monitor and manage information technology (IT) networks for smaller companies that do not have their own IT departments. Between 800 and 1,500 businesses around the world were affected. REvil is believed to be behind this attack as well. On November 8, 2021, the U.S. Department of Justice (DOJ) announced the arrest and indictment of a Ukrainian national alleged to have deployed REvil's code in the attack against Kaseya.

- ***SolarWinds:*** Beginning in September 2019, a campaign of cyberattacks breached the computing networks at SolarWinds, a Texas-based network management software company. In February 2020, the threat actor injected hidden code into a file that was later included in the company's software updates. SolarWinds released the software updates to its customers not realizing that the updates were compromised. The federal government uses the Orion software to monitor network activity on federal systems. This incident allowed the actor to breach infected agency information systems. Microsoft informed several federal agencies that Microsoft's unclassified systems had been breached and took steps with other industry partners to divert and neutralize the malicious network activity

and the malicious code. Officials from the United States and the United Kingdom attribute the attacks to the Russian Foreign Intelligence Service.

- ***T-Mobile:*** On August 17, 2021, T-Mobile learned that hackers illegally accessed personal data of former, current, and prospective customers. According to reports, a seller was attempting to sell some of the personal information in return for bitcoin. In July 2022, T-Mobile agreed to pay $350 million to settle claims by customers and $150 million to update the company's data protection. The number of customers affected by the breach remains unclear.

## Cybersecurity Attacks in Maryland

While the attacks listed above have been on a national and international scale, Maryland has not been immune from targeted cyberattacks. According to the Maryland Cybersecurity Council, in fiscal 2020, 871 unique entities reported breaches that affected Maryland residents. A description of recent and significant cybersecurity attacks in Maryland is featured below.

- ***Maryland Department of Health:*** In December 2021, a cyberattack caused the Maryland Department of Health (MDH) to take its website offline and halted the department's ability to post COVID-19 statistics. According to MDH, it does not appear that data was compromised.

- ***Greater Baltimore Medical Center:*** In December 2020, the Greater Baltimore Medical Center (GBMC) fell victim to a ransomware attack that caused multiple computer systems and the hospital's computer-operated telephone system to go offline. GBMC did not detect any misuse of data from the attack and was able to work around the disruptions to its systems.

- ***University of Maryland, Baltimore:*** A December 2020 ransomware attack on a file transfer system at the University of Maryland, Baltimore resulted in the online posting of the personal information of staff members and students. The university offered security assistance (*e.g.*, credit monitoring and identity restoration services) to affected individuals.

- ***Baltimore County Public Schools:*** In November 2020, a ransomware attack shut down the Baltimore County Public Schools (BCPS) system. The cyberattack halted classes for a few days for students attending classes online due to the COVID-19 pandemic. The Office of Legislative Audits (OLA) found that the school system's network was not properly secured, and BCPS did not adequately safeguard sensitive personal information within its computer system. In a January 2021 letter to the BCPS community, Superintendent Darryl A. Williams stated that third-party experts confirmed that no data was accessed or stolen, and BCPS has deployed state-of-the-art endpoint detection monitoring to protect

against future threats. According to news reports, as of November 2021, costs associated with the attack total $9.7 million, with approximately $2 million covered by insurance.

- ***Baltimore City Government:*** On May 7, 2019, Baltimore City government's computer systems were infected with ransomware that made the systems inaccessible and unavailable for weeks. Government emails were down, payment to city departments could not be made online, and real estate transactions could not be processed. In May 2019, the city's budget office estimated the overall cost of the attack at $18.2 million ($10 million for the system recovery efforts and $8.2 million in lost or delayed revenue).

- ***Maryland Department of Labor:*** In April 2019, hackers illegally accessed the names and Social Security numbers of as many as 78,000 people whose information was stored in two older State databases. Following an investigation by the Maryland Department of Information Technology (DoIT), the State determined that while the information may have been accessed, it was not misused. The Maryland Department of Labor (MDL) contacted the affected individuals, encouraged them to carefully monitor their accounts, and offered them two years of free credit monitoring through an independent service.

- ***Salisbury Police Department:*** On January 9, 2019, the captain of the Salisbury Police Department reported that officers were unable to access the department's computer database. According to the Director of Information Systems for the City of Salisbury, a hacker had locked down important software and was demanding money. The city did not pay the hacker and was able to restore the locked files in the network.

# Maryland

## 2022 Legislation

### Fiscal 2023 Budget and Recent Appropriations

Supplemental Budget No. 4 includes a $100 million general fund appropriation in fiscal 2023 to provide funding to improve State government cybersecurity. The fiscal 2023 budget bill also included a $100 million deficiency appropriation available "to support cybersecurity activities" for fiscal 2022. In fiscal 2021, $10 million was appropriated to the State Reserve Fund's Dedicated Purpose Account for cybersecurity assessments.

### Chapter 242

Chapter 242 of 2022 significantly expands and enhances the State's regulatory framework for State and local government cybersecurity. Chapter 242 codifies and expands the responsibilities of the Maryland Cybersecurity Coordinating Council (MCCC) and the Office of Security Management (OSM) and establishes the State Chief Information Security Officer

(SCISO) as head of OSM. The measure establishes reporting requirements for State agencies and local governments, including reporting of cybersecurity incidents. OSM must ensure that each unit of State government completes an external assessment at least every two years and is required to assist each unit to remediate any findings. Specified units within the Legislative and Judicial branches, the Office of the Attorney General, the Office of the Comptroller, and the Office of the State Treasurer must be evaluated by an independent auditor for compliance with specified cybersecurity standards. Local government entities (not including municipal governments) must consult with the local emergency manager to create or update a cybersecurity preparedness and response plan and complete a cybersecurity preparedness assessment in a manner and frequency established in regulations adopted by DoIT.

In addition, DoIT's responsibilities are expanded to include (1) centralizing the management and direction of IT policy within the Executive Branch under the control of DoIT; (2) ensuring the statewide IT master plan allows a State agency to maintain its own IT unit; (3) developing a statewide cybersecurity strategy; and (4) developing and requiring basic security requirements to be included in State contracts. DoIT is further required to develop a centralization transition strategy and conduct a performance and capacity assessment.

**Chapter 241**

Chapter 241 of 2022 establishes the Cybersecurity Preparedness Unit in the Maryland Department of Emergency Management and the Information Sharing and Analysis Center in DoIT, both of which are tasked with supporting and cooperating with OSM and SCISCO. Chapter 241 also requires local governments (other than municipalities) to, in a manner and frequency established by DoIT, create cybersecurity preparedness plans and complete assessments and report local cybersecurity incidents. Units of local government that use the State-operated broadband network are also required to certify to DoIT their compliance with the established minimum standards in a manner and frequency established by DoIT. OSM must provide guidance to a unit of local government that fails to achieve compliance with the State's cybersecurity standards.

By December 31 of each year, OSM must provide an annual report to the Governor and specified committees of the General Assembly, which includes (1) OSM's activities and accomplishments from the previous 12 months and (2) a compilation and analysis of the data and information contained in cybersecurity reports received from State and local agencies, as specified.

**Chapter 243**

Chapter 243 of 2022 establishes an independent Modernize Maryland Oversight Commission to ensure security of information and advise the Secretary of Information Technology and SCISO on, among other things, appropriate cybersecurity upgrades based on information provided to the commission by certain assessments that are to be completed every two years. In addition to making periodic recommendations on investments in State IT structures, the oversight commission must advise the Secretary on a strategic roadmap with a timeline and budget that will

(1) require the updates and investment of critical IT and cybersecurity systems to be completed by December 31, 2025, and (2) require all updates and investment of IT and cybersecurity to be made by December 31, 2030.

By December 1, 2023, each water and sewer system that serves more than 10,000 users and receives financial assistance from the State must assess its vulnerability to cyber attacks, develop a cybersecurity plan if one is appropriate, and report statutory recommendations to the General Assembly. The Maryland Water Quality Financing Administration may provide financial assistance to a system for the assessment and plan development required by Chapter 243.

Chapter 243 also establishes the Local Cybersecurity Support Fund to support local government cybersecurity preparedness by providing financial assistance to local governments to improve cybersecurity preparedness, as specified, and assist local governments applying for federal cybersecurity preparedness grants. To be eligible to receive assistance from the fund, a local government must provide proof to DoIT that the local government conducted a cybersecurity preparedness assessment in the previous 12 months or, within 12 months, undergo a cybersecurity preparedness assessment, as specified.

### Chapter 231

The Maryland Personal Information Protection Act generally requires businesses to protect their customers' and employees' personal information by implementing and maintaining reasonable security procedures and practices that are appropriate to the nature of the personal information. It also requires businesses to investigate any breach of their security systems and report specified information to the Attorney General and to individuals whose personal information may have been accessed. Chapter 231 of 2022 adopts the National Association of Insurance Commissioners Model 668 – Data Security Model Law, which establishes data security standards for insurance regulators, insurers, and other specified carriers. Chapter 231 also, under certain circumstances, requires a carrier to notify the Maryland Insurance Commissioner that a cybersecurity event has occurred.

## 2021 Legislation

### Chapter 146

Chapter 146 of 2021 targets crimes involving computers by amending § 7-302 of the Criminal Law Article, which addresses crimes involving unauthorized access to computers. More specifically, the Act prohibits a person from knowingly possessing ransomware with the intent to use the ransomware for specified purposes, as described below. The Act further prohibits committing a ransomware offense or other specified acts with the intent to interrupt or impair the functioning of a health care facility or a public school. Finally, the Act alters existing monetary penalties for specified computer-related offenses. Chapter 146 went into effect on October 1, 2021.

### *Chapter 146 Detailed Summary/How It Altered 2020 Law*

**Ransomware:** Chapter 146 defines "ransomware" as a computer or data contaminant, encryption, or lock that (1) is placed or introduced without authorization into a computer, a computer network, or a computer system and (2) restricts access by an authorized person to a computer, computer data, a computer network, or a computer system in a manner that results in the person responsible for the placement or introduction of the contaminant, encryption, or lock demanding payment of money or other consideration to remove the containment, encryption, or lock.

Except for a person who has a *bona fide* scientific, educational, governmental, testing, news, or other similar justification for possessing ransomware, Chapter 146 prohibits a person from knowingly possessing ransomware with the intent to use the ransomware for the purpose of introduction into the computer, computer network, or computer system of another person without the authorization of the other person. Violators are guilty of a misdemeanor, punishable by imprisonment for up to two years and/or a maximum fine of $5,000.

**Computer-related Offenses:** Under § 7-302 of the Criminal Law Article, a person may not intentionally, willfully, and without authorization, access or attempt to access, cause to be accessed, or exceed the person's authorized access to all or part of a computer or a computer network, control language, software, system, service, or database. A person may not intentionally, willfully, and without authorization, copy, attempt to copy, possess, or attempt to possess the contents of all or part of a computer database that was unlawfully accessed. Violators are guilty of a misdemeanor and are subject to imprisonment for up to three years and/or a maximum fine of $1,000. Chapter 146 did not alter these prohibitions or this penalty.

Under this section of law, a person may not commit the prohibited acts described above with the intent to (1) cause the malfunction or interruption of any or all parts of a computer, network, language, software, system, service, or data or (2) alter, damage, or destroy all or any part of data or a program stored, maintained, or produced by a computer, network, software, system, service, or database. A person is also prohibited from intentionally, willfully, and without authorization (1) possessing, identifying, or attempting to identify a valid access code or (2) publicizing or distributing a valid access code to an unauthorized person. If the aggregate amount of the loss is $10,000 or more, a violator is guilty of a felony, punishable by imprisonment for up to 10 years and/or a maximum fine of $10,000. If the aggregate amount of the loss is less than $10,000, a violator is guilty of a misdemeanor, punishable by imprisonment for up to 5 years and/or a maximum fine of $5,000. Chapter 146 did not alter these offenses or penalties.

Under § 7-302, a person may not commit any of these computer-related offenses with the intent to interrupt or impair the functioning of (1) the State government; (2) a natural gas or electric service, device, or system owned, operated, or controlled in the State by a person other than a public service company; or (3) a service provided in the State by a public service company. Chapter 146 prohibits a person from committing a ransomware offense against these entities or

services and adds a "health care facility" and a "public school" to the list of protected entities. A "health care facility" is a facility or office where health or medical care is provided to patients by a health care provider, as specified. "Public school" means the schools in the public elementary and secondary education system of the State.

Prior to Chapter 146, if the aggregate amount of the loss associated with a violation of this prohibition was $50,000 or more, a violator was guilty of a felony, punishable by imprisonment for up to 10 years and/or a maximum fine of $25,000. If the aggregate amount of the loss was less than $50,000, a violator was guilty of a misdemeanor, punishable by imprisonment for up to 5 years and/or a maximum fine of $25,000. Chapter 146 altered the threshold amounts and monetary penalties for these violations. Under the Act, if the aggregate amount of the loss is $10,000 or more, a violator is guilty of a felony, punishable by imprisonment for up to 10 years and/or a maximum fine of $100,000. The Act applies the existing misdemeanor penalty to a violation involving an aggregate loss of less than $10,000.

Section 7-302 prohibits access under a single scheme or a continuing course of conduct may be considered one violation. A defendant may be tried in any county in Maryland where the act was performed or the accessed computer was located. Chapter 146 did not alter these provisions.

Chapter 146 specifies that a person who has suffered a specific and direct injury as a result of any act prohibited under the Act may bring a civil action in a court of competent jurisdiction, and maintaining a civil action is not dependent upon a criminal conviction against the defendant. A court may award actual damages and reasonable attorney's fees and court costs.

**Chapter 683**

Chapter 683 of 2021 codifies the Center for Cybersecurity at the University of Maryland, Baltimore County and requires the Governor to appropriate $3.0 million for the center annually beginning in fiscal 2023. The Act also increases, beginning in fiscal 2023, mandated appropriations by $2.5 million each for the Center for Maryland Advanced Ventures at the University of Maryland and the University of Maryland Center for Economic and Entrepreneurship Development. A portion of the mandated funding is for the development and location of technology companies in Baltimore City and Prince George's County. In addition, for fiscal 2023 through 2027, the Governor must appropriate at least an additional $4.0 million to the University System of Maryland (USM) Office to increase the estimated funding guideline attainment levels of USM institutions as specified.

**Chapter 113**

Chapter 390 of 2013 established the Cybersecurity Investment Incentive Tax Credit (CIITC) Program, which provides a refundable tax credit for investments in qualified cybersecurity companies. The total amount of credits awarded each year is generally limited to the amount

appropriated to the program's reserve fund in that year less administrative costs. The Governor is required to appropriate at least $2.0 million to the reserve fund in each fiscal year.

Chapter 113 of 2021 alters the CIITC by (1) extending the program termination date by two years, through June 30, 2025; (2) expanding the applicability of the program to technology companies, rather than solely cybersecurity companies, and removing "cybersecurity" from the name of the program; (3) establishing certain reporting requirements and an evaluation and recommendation process for determining eligible industry sectors; (4) establishing the objective and goals of the program; and (5) specifying that a qualified investor may not be a founder or current employee of the company receiving the investment if the company has been in active business for more than five years. The Act extends the $2.0 million annual mandated appropriation for two years (fiscal 2024 and 2025).

### Chapter 318

Chapter 318 of 2021 expands the responsibilities of the Secretary of Information Technology to include advising and consulting with the legislative and judicial branches of State government regarding a cybersecurity strategy and, in consultation with the Attorney General, (1) advising and overseeing a consistent cybersecurity strategy for units of State government, including institutions of higher education and (2) developing guidance on consistent cybersecurity strategies for counties, municipal corporations, school systems, and all other political subdivisions of the State. None of the Secretary's new responsibilities may be construed as establishing a mandate for any of these local government entities.

## Recent State Action

### Executive Order – Office for Security Management

In June 2019, Governor Lawrence J. Hogan, Jr. signed Executive Order 01.01.2019.07, which creates the Maryland Cyber Defense Initiative to strengthen the State's ability to manage the effects of a cybersecurity incident. The initiative creates OSM within DoIT and charges the office with responsibility for the direction, coordination, and implementation of an overall cybersecurity strategy for all Executive Branch IT systems. The office is led by SCISO who is appointed by the Governor. The order also established MCCC to assist SCISO and the office in their duties. As discussed above, Chapter 242 codifies and expands the responsibilities of MCCC and OSM and establishes SCISO as head of OSM.

### Information Technology Security Manual

In that same month, DoIT released the State of Maryland Information Technology Security Manual. The manual currently serves as the primary policy for establishing and defining the State's IT security practices and requirements; all State agencies are required to adhere to the manual.

### 2020 Legislation

Chapter 429 of 2020 expands and enhances the cybersecurity protocols that govern the collection, processing, sharing, and disposal of personally identifiable information (PII) by public institutions of higher education in the State beginning on October 1, 2024.

### Audits of State Agency Cybersecurity Discover PII Vulnerabilities

OLA summarized its audit findings related to cybersecurity and PII and reported those findings to the Joint Audit and Evaluation Committee in December 2019. OLA found that, from July 2013 through December 2019, approximately 37.9 million PII records existed in State and local government agencies that were not adequately protected with data security controls. Over that same period, 77 of OLA's audits contained findings related to PII. While DoIT and the State have been improving their protection of PII, a 2020 legislative audit found additional issues. For example, in one instance, PII was not adequately restricted to employees who should have access to it and instead was visible to over 5,000 State employees.

OLA has previously emphasized the financial cost associated with data breaches by citing the Ponemon Institute, an independent research organization focused on data protection, and IBM, one of the largest computer manufacturers in the world. The two organizations annually publish a report on global data breaches and their economic impacts. The 2021 report found that (1) the average total cost of a data breach in the United States is $9.0 million and (2) customer PII has the highest cost per record at $180. These costs include detection of the breach, escalation, notifications, response, and lost business.

## Maryland Cybersecurity Council

### Summary

Chapter 358 of 2015 established the Maryland Cybersecurity Council, staffed by the University of Maryland University College (now called the University of Maryland Global Campus, which is part of USM). The council is required to work with the National Institute of Standards and Technology (NIST), as well as other federal agencies, private-sector businesses, and private cybersecurity experts to address State cybersecurity issues. The council's responsibilities include (1) examining inconsistencies between State and federal cybersecurity laws; (2) assisting private-sector cybersecurity businesses in adopting, adapting, and implementing the NIST cybersecurity framework of standards and practices; and (3) recommending legislative changes to address cybersecurity issues. The council engages in a variety of activities to fulfill its duties, including conducing public outreach and education, informing legislation, and developing and producing materials on cybersecurity issues.

### Membership

The council is chaired by the Attorney General or the Attorney General's designee and currently consists of 57 members representing government, law enforcement, emergency management, defense, the private sector and private industry, higher education, health care, and crime victims.

### Recent Activities

The council engaged in a variety of activities, such as conducting cybersecurity policy events for the General Assembly, educating the public on cybersecurity issues, providing support for the Emergency Number Systems Board, developing a plan for an information sharing and analysis organization within the State, and enhancing the council's repository of cybersecurity resources.

### 2021 Recommendations

In its July 2021 report, the council made five recommendations to add to the recommendations made in its two previous biennial reports. The five recommendations are listed below.

1. ***Recommendation 1:*** That the State consider incentives for businesses to assess their cybersecurity posture and to invest more, if necessary, to create a cybersecurity program consistent with recognized standards and framework. (This recommendation mainly advocates for the availability of an affirmative defense in a tort action related to cybersecurity breach for businesses that adopt specified cybersecurity standards.)

2. ***Recommendation 2:*** That the State consider appropriate legislation to ensure the transparency to consumers of the information held by entities about them and how it is used, the right of consumers to inspect, correct and delete such data, and their right to opt out of the sale of data to third parties. (This recommendation expands application of a previous council recommendation that only applied to Internet Service Providers.)

3. ***Recommendation 3:*** That the State consider legislation to enhance the security of Internet of Things (IoT) devices. IoT is a term used to describe physical objects that use embedded sensors, software, and other technologies to connect with the internet and exchange data with other devices and systems. (This recommendation appears to take a more generalized approach to a 2017 council recommendation.)

4. ***Recommendation 4:*** That there be transparency with the State by critical infrastructure providers about compromises that interfere with operations. (This recommendation refers to mandatory reporting laws regarding cybersecurity attacks against public entities/public utilities.)

5. ***Recommendation 5:*** That the State consider a strategic partnership to a) engage business and industry in identifying gaps in IT/cybersecurity workforce development and in defining training requirements; b) leverage the postsecondary sector and other training and education providers to offer needed training; c) to coordinate upskilling opportunities for the unemployed or underemployed; and d) provide enhanced funding for a variety of pathways to the cybersecurity profession, including apprenticeships and career and technical education. (This recommendation aims to increase the pool of skilled cybersecurity professionals in the State. The recommendation reflects recent efforts in other states and addresses a survey conducted by the Cybersecurity Association of Maryland whose results indicate that businesses in the State encounter widespread challenges in recruiting cybersecurity professionals.)

## Recent Legislative Activity in Other States

According to the National Conference of State Legislatures (NCSL), at least 40 states and Puerto Rico considered more than 250 bills or resolutions dealing with cybersecurity in 2022. According to NCSL, the most common enactments (1) require government agencies to implement cybersecurity training, establish and implement formal security policies and practices, provide mandatory training to employees, and report cybersecurity incidents; (2) provide funding for cybersecurity programs and practices in state and local government; (3) mandate election-related security practices; and (4) establish or enhance cybersecurity workforce training and education programs. Listed below are some of the more notable state actions in recent years regarding data privacy and recent New York legislation concerning cybersecurity requirements for financial services entities.

### California

***California Consumer Privacy Act and California Privacy Rights Act:*** In 2018, California became the first state to enact a comprehensive data privacy law, the California Consumer Privacy Act (CCPA), which broadly established rights for Californians to inspect and correct how companies use and share their personal data (such as which information is shared or sold to digital advertisers, etc.). CCPA went into effect on January 1, 2020, and applies to for-profit companies that operate in California and meet specified criteria.

The California Privacy Rights Act (CPRA) passed in November 2020 as a ballot initiative and takes effect January 1, 2023. CPRA amends CCPA by altering the scope of covered businesses, granting consumers more control over their personal information, requiring covered business to meet specified annual compliance and audit requirements, and establishing a new enforcement agency. Though CCPA and CPRA refer to "reasonable" precautions and procedures, the Acts do not define "reasonable" precautions or procedures for the protection of consumers' information.

However, the California Attorney General has previously highlighted certain security measures that could constitute a baseline of "reasonable" security practices.

- ***Applicable Businesses:*** CPRA increases the minimum customer base for businesses subject to the data privacy laws. However, CPRA expands application to businesses that derive at least 50% of their annual revenue from *sharing* consumers' personal information (CCPA established similar annual revenue criteria for the *selling* of personal information). CPRA also refines provisions on the application of the statute to commonly branded businesses that control or are controlled by an applicable business. Finally, CPRA extends application to joint ventures or partnerships in which each business has at least a 40% interest.

- ***Contractors and Service Providers:*** CPRA requires "contractors" to whom a business discloses personal information to provide the same level of privacy protection as the covered business itself. Covered entities must adopt contractual clauses and other supply chain security safeguards to ensure that such third-party contractors comply with applicable requirements. CPRA amends the definition of a "service provider" to mirror the definition of a contractor under the Act; CPRA generally imposes the same obligations and on contractors and service providers.

- ***Expanded Consumer Rights:*** CPRA expands on the data privacy rights contained in CCPA. Among the expanded consumer rights under CPRA are (1) the right to correct inaccurate personal information; (2) the right to opt out of the *sharing* of personal information by a business to a third party (CCPA applied this to third-party *sales*); and (3) the right to opt out of and access information about automated decision making.

- ***Sensitive Personal Information:*** While CCPA and CPRA both apply to personal information, CPRA lists a set of data considered to be "sensitive personal information" and imposes specific requirements and restrictions on the treatment of sensitive personal information, such as a consumer's right to limit the use or disclosure of their sensitive personal information. Examples of sensitive personal information include Social Security numbers, account login information, and private communications (*e.g.*, emails, texts, etc.). Information that is "publicly available" is not sensitive personal information or personal information.

- ***Expanded Business Obligations:*** Businesses have obligations that correspond to the expanded consumer rights under CPRA, many of which apply to notice requirements and procedures to allow consumers to exercise their rights under the Act. CPRA also requires companies that own, license, or maintain personal information from consumers to implement reasonable security procedures and practices to protect that information. CPRA limits the processing of personal information to that which is reasonably necessary and proportionate to the purposes for which the information was collected or compatible to

those purposes; information may not be further processed in an incompatible manner. CPRA requires businesses to inform consumers of the length of time they plan to retain their personal information and prohibits businesses from retaining personal information longer than is "reasonably necessary." Covered businesses must communicate consumer requests to delete personal information to service providers, contractors, and third parties.

- ***Audits and Risk Assessments:*** Businesses must conduct annual cybersecurity audits and submit regulatory filings regarding risk assessments with the newly established California Privacy Protection Agency (CPPA) if processing consumer personal information poses a significant risk to consumers' privacy. Created by CPRA, the agency has a $10 million annual budget and is the first state agency in the United States dedicated solely to privacy protection.

- ***Private Cause of Action and Administrative Fines:*** CPRA provides for a private cause of action and statutory damages against companies that fail to reasonably protect a consumer's log-in information. CCPA previously authorized this cause of action with respect to "personal information," as defined in statute.

  As established under CCPA, violators also face administrative fines of $2,500 for each violation and $7,500 for each intentional violation. CPRA applies the $7,500 fine to violations involving the personal information of minors. CPRA also repeals the ability under CCPA for violators to avoid administrative fines by curing a violation within 30 days after being notified of noncompliance. However, CPRA authorizes CPPA to consider an alleged violator's lack of intent to commit a violation or the company's voluntary efforts to remedy the alleged violation when deciding not to investigate a complaint or opting to provide a business with a time period to cure the alleged violation.

**California Age-Appropriate Design Code Act**

On September 15, 2022, California Governor Gavin C. Newsom signed into law the California Age-Appropriate Design Code Act. Effective July 1, 2024, the Act expands privacy requirements for businesses that provide online services, products, or features that are known to be accessed by or, as determined by specified factors, are "likely to be accessed" by individuals younger than age 18. The Act is modeled on legislation from the United Kingdom and goes beyond the provisions of the federal Children's Online Privacy Protection Act.

Among other things and with specified exceptions, covered businesses (1) may not engage in specified data practices (*e.g.*, profiling a child by default or collecting, selling, sharing, or retaining a child's personal information unless necessary to provide the online product, service, or feature); (2) must comply with various transparency requirements; and (3) must complete data-related assessments and review those assessments every two years. The California Attorney General is the sole enforcement authority for the Act. The Attorney General may seek injunctions against violators, and violators are subject to civil penalties of $2,500 per child for a

negligent violation and $7,500 per child for an intentional violation. The Attorney General is required to provide written notice prior to initiating an action against a substantially compliant business and must give the business 90 days to cure violations and avoid penalties. The Act does not establish a private cause of action. Finally, the Act establishes the California Children's Data Protection Working Group, which is required to solicit input from stakeholders and submit reports to the legislature with recommendations on best practices for implementation of the Act.

### Virginia

Virginia followed California to become the second state to enact a comprehensive data privacy law. Virginia's Consumer Data Protection Act (VCDPA) (which is similar to California's CPRA and also takes effect January 1, 2023) affirmatively requires covered entities to "[e]stablish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data." VCDPA applies to persons conducting business in Virginia, or producing products or services targeted to Virginia residents that either (1) control or process the personal data of at least 100,000 consumers during a calendar year or (2) control or process the personal data of at least 25,000 consumers and derives at least 50% of its gross revenue from the sale of personal data. Specified entities are not subject to the Act, including nonprofit organizations, higher education institutions, and entities governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

VCDPA broadly defines "personal data" as "any information that is linked or reasonably linkable to an identified or identifiable natural person," but excludes publicly-available information and de-identified data. The Act also has a separate "sensitive data" category that is defined as (1) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (2) genetic or biometric data; (3) personal data collected from a child; or (4) precise geolocation data. Consumer (or parental) consent is required to process sensitive data.

Similar to California's statute, VCDPA offers the following rights to consumers: the right to confirm whether or not a controller is processing the consumer's personal data and to access that personal data; the right to correct inaccurate personal data; the right to delete personal data provided by or obtained about the consumer; the right to obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and readily usable format; and the right to opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

Under VCDPA, covered entities must undertake a "data protection assessment" when engaging in data processing related to targeted advertising, the sale of personal data, the processing of personal data for profiling purposes that presents specified reasonably foreseeable risks, the processing of sensitive data, or personal data processing that poses a heightened risk of harm to a consumer. The required assessments must incorporate a cost-benefit analysis that addresses factors

related to data security, risk mitigation, and consumer expectations, and the company may have to provide such data protection assessments to the Virginia Attorney General. Similar to California, covered entities must include data protection clauses in contracts with third parties that process personal data on behalf of the covered company.

The Virginia Attorney General may impose penalties of up to $7,500 per violation; entities can avoid enforcement and penalties if they cure an alleged violation within 30 days and commit in writing to refrain from committing further violations. Unlike California's statute, the Virginia law does not include a private right of action for consumers affected by a data breach.

**Colorado**

In July 2021, Colorado enacted the Colorado Privacy Act (CPA), becoming the next state to enact a comprehensive data privacy law that is akin to California and Virginia's recent laws (as described above).

Under CPA, consumers have a right to opt out of personal data sharing by a covered entity for targeted advertising sale, or profiling; a right to access the consumer's personal data and to confirm that the consumer's personal data is being processed by the covered entity; a right to correct inaccurate personal data; a right to delete personal data; and a right to access the data in a portable format.

Among other requirements, CPA limits the collection and processing of personal data to that which is reasonably necessary and compatible with the purposes that have been disclosed to consumers. Covered entities may not process a consumer's sensitive data without consent. CPA prohibits covered entities from processing data that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment to evaluate security risks, and covered entities must adopt appropriate security measures to protect data from unauthorized access. Similar to the laws passed in California and Virginia, CPA requires covered businesses (controllers) who engage data processors to enter into written contracts meeting specified requirements with the processors. Data processors are also required to assist controllers in meeting their statutory obligations and must provide controllers with audit rights, deletion rights, and the power to object to subcontractors.

CPA does not contain a private right of action for consumers whose data is breached, but violations are enforceable by the Colorado Attorney General and state district attorneys (subject, until 2025, to a 60-day cure period for any alleged violation). A violation constitutes a deceptive trade practice under Colorado law, with civil penalties of up to $20,000 per violation or $50,000 for a violation committed against an elderly person.

CPA builds upon an earlier law enacted in 2018 (the Colorado Protections for Consumer Data Privacy Law) that requires covered entities to implement reasonable safeguards and conduct a prompt, good-faith investigation in the event of a cyber incident to determine the likelihood that personal information had been or would be misused. In response to such a breach or incident, the

covered entity must generally provide notice within 30 days to the affected Colorado residents and, if more than 500 Colorado residents are affected, the Colorado Attorney General. The required notice must be made in writing, by telephone, or provided electronically; however, substitute notice (via email, or public notice through the media, etc.) may be provided (1) if the cost of providing notice will exceed $250,000; (2) more than 250,000 Colorado residents must be notified; or (3) the company does not have sufficient contact information to provide notice. Subject to legitimate law enforcement needs or other measures that are necessary to determine the scope of the breach and restore the integrity of the entity's data system, notice may potentially be provided beyond 30 days.

### Connecticut

The Connecticut Data Privacy Act (CTDPA), which was enacted in 2022 and goes into effect July 1, 2023, is conceptually similar to Virginia and Colorado's laws, as described above. CTDPA applies to persons conducting business in Connecticut, or producing products or services targeted to Connecticut residents, and who during the preceding calendar year either (1) controlled or processed the personal data of 100,000 or more consumers, except for personal data controlled or processed solely for the purpose of completing a payment transaction or (2) derived more than 25% of their gross revenue from the sale of personal data and controlled or processed the personal data of at least 25,000 consumers. There is no annual revenue threshold at which point CTDPA's obligations are imposed.

CTDPA contains exemptions for certain types of entities (including state and local governments, nonprofits, institutions of higher education, certain financial institutions, etc.), as well as certain types of data (including personal data regulated by the Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Family Educational Rights and Privacy Act, the Farm Credit Act, and the Airline Deregulation Act), and contains other health and employment-related data exemptions. Individuals "acting in a commercial or employment context" are not considered consumers under CTDPA, and de-identified or publicly available information is also excluded from CTDPA's requirements.

Similar to other states' laws, consumers have the right to opt out of certain data processing and have rights relating to data access, correction, deletion, and portability. Consumers must consent to the collection and processing of "sensitive data." Among other requirements relating to data transparency and safety, controllers must "establish, implement, and maintain reasonable administrative, technical, and physical security practices to protect the confidentiality, integrity, and accessibility of personal data." Controllers must also conduct a data protection assessment for processing activities that present a "heightened risk of harm to a consumer."

CTDPA does not contain a private right of action. Violations constitute unfair trade practices under Connecticut law and are exclusively enforced by the Attorney General. Prior to January 1, 2025, cure periods must be given to alleged violators; they are discretionary afterwards.

### Utah

The Utah Consumer Privacy Act (UCPA) was signed into law in March 2022 and takes effect December 31, 2023. Narrower in applicability than the other state laws discussed above, UCPA applies to data controllers and processors that conduct business in Utah or produce products or services targeted to Utah residents, have annual revenue of at least $25.0 million, and either (1) control or process the personal data of at least 100,000 consumers annually or (2) derive over 50% of gross revenue from the "sale" of personal data and control or process the personal data of at least 25,000 consumers. Among other things, UCPA specifically excludes "a controller's disclosure of personal data to a third party if the purpose is consistent with a consumer's reasonable expectations" from the definition of "sale."

UCPA exempts certain data (including, for example, protected health information, as well as data regulated by the Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Farm Credit Act, and the Family Educational Rights and Privacy Act), certain entities (*e.g.*, nonprofits, certain financial institutions, institutions of higher education, government entities or third-party contractors acting on their behalf, tribes, and air carriers) and other specified health- and employment-related data. UCPA further exempts information that has been de-identified, aggregated, or which is publicly available. UCPA requires providing consumers with notice and an opportunity to opt out of using "sensitive data," as defined, but does not require affirmative consumer consent to process such data.

Consumers have the right to (1) access and confirm whether their personal data is being processed; (2) delete personal data (but only the personal data they provided to the controller); (3) data portability; and (4) opt out of processing related to targeted advertising or the sale of personal data. Unlike other state laws, the law does not grant consumers the right to correct inaccurate data, or the right to opt out of profiling. Among other requirements relating to safety and transparency, processors must "establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to protect the confidentiality and integrity of personal data"; however, the law does not require data protection assessments or cybersecurity audits.

UCPA does not contain a private right of action. Distinctively, the Division of Consumer Protection within the Utah Department of Commerce must investigate consumer complaints and refer matters to the Utah Attorney General before the Attorney General may initiate enforcement actions. Prior to initiating an enforcement action, the Attorney General will provide notice to alleged violators along with a 30-day cure period. If an alleged violator fails to cure or continues to violate UCPA, the Attorney General may initiate an enforcement action and impose penalties of actual damages and fines up to $7,500 per violation.

### New York

Since March 2017, New York State's Department of Financial Services' (NYDFS) Cybersecurity Regulation, 23 NYCRR 500, has imposed administrative and security requirements

on specified entities that are regulated by NYDFS under the state's banking, insurance, and financial services laws, as well as relevant third parties that have access to covered entities' systems. Under the regulation, a covered entity is subject to the requirements discussed below.

- A covered entity must maintain a cybersecurity program to protect its information systems, as well as maintain a written cybersecurity policy and incident response plan. Both the program and the policy must meet specified requirements and must be based on a risk assessment.

- A covered entity must designate an individual to oversee and implement its cybersecurity program and enforce its cybersecurity policy.

- Covered entities are required to use qualified personnel to manage cybersecurity threats and countermeasures.

- Based on the risk assessment mentioned above, covered entities must limit and periodically review user access privileges to information systems.

- A covered entity must notify NYDFS within 72 hours of a breach or attempted breach of its information systems or information stored on the system, as specified.

- A covered entity must enact data encryption controls and employ multi-factor authentication for inbound communications to its network.

- Covered entities are subject to reporting requirements, including annual certifications of compliance with the regulation.

In 2022, NYDFS issued proposed amendments to the regulation. Among other requirements, the proposed amendments would (1) expand the types of cybersecurity events subject to the 72-hour notification requirement; (2) require covered entities to notify NYDFS within 24 hours of making an "extortion payment" as a result of a cyber incident, and provide written information about the decision to make the payment within 30 days; (3) require covered entities to implement a business continuity and data recovery plan (in addition to an incident response plan); (4) impose additional requirements on "Class A companies" (defined as a covered entity (including its affiliates) that had $20 million in in-state gross annual revenue in each of the last two fiscal years and has averaged over 2,000 employees over the last two fiscal years or more than $1.0 billion in gross annual revenue in each of the last two fiscal years); (5) impose new guidelines for what should be included in a covered entity's written cybersecurity policies (and requiring the policies to be approved by the entity's "senior governing body" at least annually); (6) require enhancements to existing testing and assessment protocols; and (7) require

enhancements relating to multi-factor authentication, privileged account limitations, and cybersecurity training for personnel.

In March 2021, NYDFS issued its first civil penalty under the regulation against a mortgage services company for $1.5 million, for failing to report a breach and failing to conduct necessary risk assessments. Under a settlement reached with NYDFS, the company agreed to submit comprehensive incident response plans, updated risk assessments, as well as other materials to NYDFS that would detail how it will bolster its cybersecurity procedures going forward.

# Federal Actions

## Recent Executive Branch Actions (Executive Orders)

### Presidential Executive Order on Cybersecurity

In May 2021, President Biden signed an executive order designed to improve cybersecurity by "protecting federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur." The executive order requires that all federal information systems should meet or exceed the standards and requirements set forth in and issued pursuant to the order. In addition to safeguarding federal networks, the executive order aims, by setting criteria for federal procurement, to use the federal government's purchasing power to drive markets and thereby make all software more secure. Key components of the executive order are described below.

- ***Contractual Language:*** The order requires the Office of Management and Budget (OMB) to propose updated contractual language (for federal contracts with both IT and operational technology service providers) to ensure that service providers (1) collect and preserve information relevant to cybersecurity events on all information systems over which they have control; (2) share threat and incident information (consistent with applicable privacy laws) with federal agencies; and (3) collaborate with federal agencies in investigations of and responses to cyber incidents on federal information systems. [*Sec. 2(c)*] The executive order further states that it is the policy of the federal government that service providers entering into contracts with agencies must promptly report to federal agencies when they discover a cyber incident involving a software product or service provided to such agencies, or a support system. The executive order directs the Department of Homeland Security (DHS) to recommend mandatory reporting contractual language and requires specified federal officials to develop procedures for prompt sharing of reported incidents.

- ***Best Practices:*** The executive order directs federal agencies to advance toward security best practices, such as secure cloud services and a "Zero Trust Architecture," and mandates the adoption of multifactor authentication and encryption for data at rest and in transit.

- ***Security Standards:*** The executive order requires federal agencies to establish comprehensive baseline security standards for software sold to the federal government and aims to improve the security and integrity of the software supply chain by requiring software companies to maintain greater visibility into their software development processes and making security data publicly available.

- ***Pilot Program:*** The executive order creates a pilot program to establish a consumer product label that can inform consumers about the security of cyber products.

- ***Cyber Safety Review Board:*** The executive order establishes a Cyber Safety Review Board (modeled after the National Transportation Safety Board) comprised of federal officials and private-sector representatives. After significant cyber incidents, the board is to review, assess, and make recommendations regarding threat activity, vulnerabilities, mitigation activities, and agency responses.

- ***Incident Response Procedures:*** The executive order tasks specified federal officials with developing a standard set of operational procedures for responding to cybersecurity incidents across the federal government.

- ***Early Detection of Threats:*** The order directs the federal government to maximize the early detection of cybersecurity vulnerabilities and incidents on federal networks, including by deploying an endpoint detection and response system to support proactive detection of incidents, active cyber hunting, containment and remediation, and incident response.

- ***Tracking Cybersecurity Events:*** The order establishes requirements for logging events and retaining other relevant data within an agency's systems and networks to aid in the investigation and remediation of cyber incidents.

**July 2021 Presidential Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems**

In July 2021, President Biden signed a memorandum designed to safeguard the cybersecurity and resilience of systems supporting "National Critical Functions," defined as "the functions of Government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on national security, economic security, public health or safety, or any combination thereof."

As part of this effort, the Biden Administration has established a voluntary Industrial Control Systems Cybersecurity Initiative that is designed to foster collaboration between the federal government and private industry (including the electricity, natural gas pipeline, water, wastewater, and chemical sectors) and to set baseline cybersecurity goals that are consistent across all critical infrastructure sectors. Under the memorandum, DHS must set cybersecurity performance goals for critical infrastructure, as specified, that will serve as "clear guidance to owners and operators about cybersecurity practices and postures that the American people can trust and should expect for such essential services."

## Recent Federal Agency Regulatory and Enforcement Actions

### Department of Homeland Security (Transportation Security Administration)

Following the ransomware attack on Colonial Pipeline, DHS' Transportation Security Administration (TSA) issued two security directives in 2021 imposing cybersecurity-related requirements on owners and operators of TSA-designated critical pipelines (*i.e.*, pipelines that transport hazardous liquids and natural gas). In July 2022, TSA issued a revised security directive requiring specified owners and operators of pipeline and liquefied natural gas facilities to take action to (1) develop network segmentation policies and controls to ensure that operational technology systems can continue to safely operate in the event that an IT system has been compromised (and vice-versa); (2) create access control measures to secure and prevent unauthorized access to critical cyber systems; (3) build continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect critical cyber system operations; and (4) reduce the risk of exploitation of unpatched systems through the application of security patches and updates in a timely and designated manner. Under the reissued 2022 directive, pipeline owners and operators also must (1) establish and execute an approved cybersecurity implementation plan; (2) develop and maintain a cybersecurity incident response plan; and (3) establish a cybersecurity assessment program. TSA's directive leaves in place previous requirements to report significant cybersecurity incidents to CISA, establish a cybersecurity point of contact, and conduct an annual cybersecurity vulnerability assessment.

Prior to the 2021 directives, TSA's pipeline cybersecurity standards were voluntary. The directives signal the federal government's shift to a more "hands-on" regulatory approach in response to recent cyberattacks and their potential effect on national infrastructure and security.

### Department of Justice

In October 2021, DOJ announced the launch of a Civil Cyber-Fraud Initiative, under which federal government contractors and grant recipients face enforcement under the federal False Claims Act if they endanger U.S. information or systems "by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or

protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches."

In May 2022, DOJ revised its policy regarding charging violations of the Computer Fraud and Abuse Act (CFAA) (discussed below).

### Department of the Treasury

In July 2021, the Treasury Department's Financial Crimes Enforcement Network announced that it will work with banks and other companies to counter money laundering schemes that involve the use of cryptocurrency and to improve efforts to trace ransomware payments. At the same time, the U.S. Department of State announced that it will offer rewards of up to $10 million for information that leads to the identification of entities involved in malicious state-sanctioned cyber activities, such as ransomware against critical infrastructure.

### Securities and Exchange Commission

"Disclosure controls and procedures" typically refers to controls and procedures a company implements to ensure the proper, complete, and timely disclosure of information required to be included in the company's Securities and Exchange Commission (SEC) reports. In 2018, SEC advised that specified rules of the Securities Exchange Act of 1934 require a public company to implement vigorous disclosure controls and procedures for cybersecurity threats and incidents. According to the commission, "it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion." Proper protocols include directors and officers being kept abreast of the company's existing and potential future cybersecurity threats and incidents. As a result of these rules, SEC has begun to pursue enforcement actions against companies for materially misleading statements and omissions relating to cyber incidents and nondisclosure of breaches – and not only for instances of intentional fraud and misconduct, but cases of negligence, as well.

For example, in August 2021, SEC assessed a $1 million penalty against Pearson, a British educational publishing firm, for failing to disclose a cyber breach on a securities filing to SEC. In accepting the company's offer to pay a $1 million fine, SEC noted that Pearson only disclosed the relevant incident after being contacted by a national media outlet, downplayed the incident's scope, overstated the company's capacity to handle the breach, failed to take prompt action to repair its cybersecurity vulnerabilities, and failed to maintain protocols that kept the company's leadership properly informed of the extent of the circumstances surrounding the breach. Due to the company's misleading statements, SEC found the company violated relevant sections of the Securities Act of 1933 and the Securities Exchange Act of 1934. Two weeks later, SEC penalized another eight firms that negligently failed to ensure the security and confidentiality of customer records and failed to protect against unauthorized access to customer records and information. In short, understated or misleading communications about cyber events may form a basis for liability with SEC.

In addition to enforcement by SEC itself, companies could also face class action lawsuits from private investors. For instance, investors filed a securities class actions lawsuit against SolarWinds following the high-profile hack of the company. According to the plaintiffs, SolarWinds made false or misleading statements on its securities filings regarding the company's cybersecurity vulnerabilities and capabilities.

In February 2022, SEC proposed new rules and amendments to enhance cybersecurity preparedness and improve the resilience of investment advisors and investment companies. SEC's proposal would (1) require advisers and funds to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks; (2) require advisers to report significant cybersecurity incidents, including on behalf of a fund or private fund client; (3) require disclosure of cybersecurity risks and incidents to clients, investors, and prospective clients or investors (including a description of any significant fund cybersecurity incidents that occurred during the previous two fiscal years); and (4) require advisers and funds to maintain, make, and retain cybersecurity-related books and records.

Additionally, in March 2022, SEC proposed amendments to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies. SEC proposed to require registrants to disclose information about a material cybersecurity incident within four business days after the registrant determines that it has experienced a material cybersecurity incident. SEC also proposed to require registrants to provide updated disclosure relating to previously disclosed cybersecurity incidents and to require disclosure, to the extent known to management, when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate. In addition, SEC proposed requiring enhanced and standardized disclosure on registrants' cybersecurity risk management, strategy, and governance, including disclosure regarding board member cybersecurity expertise.

### Federal Reserve/Office of the Comptroller of the Currency/Federal Deposit Insurance Corporation

In November 2021, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation issued a final rule requiring a banking organization to notify its primary banking regulatory within 36 hours of a "computer-security incident," which has or is reasonably likely to materially disrupt or degrade its operations or services, or which would pose a threat to U.S. financial stability. The final rule also requires bank service providers, by any reasonable means, "to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for 4 or more hours."

### Federal Trade Commission

In August 2022, the Federal Trade Commission (FTC) issued an Advance Notice of Proposed Rulemaking (ANPR) on the prevalence of "commercial surveillance and data security practices that harm consumers." The ANPR did not include proposed regulatory language but rather posed 95 questions for public comment relating to commercial surveillance and data security, as well as the costs and benefits of issuing regulations using the agency's rulemaking authority under the FTC Act. (Under the FTC Act, the agency must show that regulated practices are prevalent and unfair or deceptive.) Public comments on the initial phase of the rulemaking are due within 60 days, after which FTC may issue a Notice of Proposed Rulemaking. In the ANPR, commissioners noted that any proposed rulemaking would be a backstop in the end event that the U.S. Congress does not pass federal privacy legislation (discussed further below.)

In May 2022, FTC adopted a policy statement announcing that it will crack down on education technology companies that violate the Children's Online Privacy Protection Act, including requirements against (1) requiring children to provide more information than is reasonably necessary to participate in an activity; (2) using personal information collected from a child for any other commercial purpose including marketing or advertising; and (3) retaining children's personal information for longer than is necessary to fulfill the purpose for which it was collected. Education technology providers must also have procedures to maintain the confidentiality, security, and integrity of children's personal information.

In late 2021, FTC updated its "Safeguard Rule" strengthening the data security safeguards that nonbanking financial institutions (*e.g.*, mortgage brokers, motor vehicle dealers, and payday lenders) must put in place to protect customers' financial information. The updated requirements include limiting who can access consumer data and requiring encryption to secure data. Covered institutions must explain their information sharing practices and must designate a single qualified individual to oversee information security and report to relevant corporate officials.

## Congressional Action

### Cyber Incident Reporting for Critical Infrastructure Act

On March 15, 2022, President Biden signed into law the omnibus Consolidated Appropriations Act of 2022, which included the Cyber Incident Reporting for Critical Infrastructure Act, which requires critical infrastructure entities to report to the federal government cybersecurity incidents and ransom payments. Covered entities will be required to (1) report covered cyber incidents to CISA within 72 hours of reasonably believing that a covered cyber incident has occurred and (2) report any ransom payments within 24 hours, including for situations that might not otherwise trigger the incident reporting requirement. Initial reports must be supplemented as "substantial new or different information becomes available," until the incident has been resolved. The reporting requirements do not apply to entities that are already required to

report "substantially similar information to another federal agency within a substantially similar timeframe," provided the other agency has an agreement and sharing mechanism with CISA. The Act requires CISA to promulgate implementing regulations (*e.g.*, the types of covered entities, what constitutes a covered cyber incident, incident and ransom report content requirements).

CISA may issue a subpoena after making an initial request to covered entities that it believes may have experienced a reportable incident (or made a reportable ransom payment); an entity's failure to comply with a subpoena may result in a civil lawsuit; however, this enforcement mechanism does not apply to state and local governments. Failing to comply with the Act's reporting requirements also denies covered entities the protection from liability that is otherwise afforded to entities for compliance: required reports and voluntarily disclosures are exempt from disclosure under the federal Freedom of Information Act, "as well as any provision of State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records." Covered entities are shielded from litigation that may arise from the submission to CISA of a cyber incident report or ransom payment report (although, not from the underlying incident or payment itself), and information related to such reports are shielded from being used in litigation or before a regulatory body.

Among other provisions, the Act also (1) calls for the creation of a Cyber Incident Reporting Council led by the Secretary of Homeland Security, to harmonize federal incident reporting requirements; (2) provides for the creation of a ransomware vulnerability warning pilot program; and (3) calls for a new task force, chaired by CISA, "to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation."

### American Data Privacy Protection Act

In July 2022, the proposed American Data Privacy Protection Act (ADPPA), H.R. 8152, advanced out of the House Energy and Commerce Committee. As noted by the Congressional Research Service, ADPPA would create a comprehensive federal consumer privacy framework that applies to covered business entities, nonprofits, and common carriers (with certain small and medium-sized businesses exempt from several of the bill's requirements). Among other requirements, covered entities would be prohibited from collecting, using, or transferring covered data beyond what is reasonably necessary and proportionate to provide a service requested by an individual, unless doing so for a specified permissible purpose. Additional protections would apply for sensitive covered data. ADPPA would give consumers various rights over covered data and would require covered entities to disclose the type of data they collect, how and for how long the data is used and retained, and whether the data is made accessible to China, Russia, Iran, or North Korea. Covered entities would be prohibited from using covered data in a discriminatory manner, must conduct algorithm impact assessments, and must adopt reasonable data security practices and procedures (depending on the entity's size and activities).

ADPPA would be enforceable by FTC and state Attorneys General (and state privacy authorities) in civil actions. Beginning two years after the bill's enactment, ADPPA would allow suits in federal court for damages, injunctions, litigation costs, and attorneys' fees; however, individuals would have to inform FTC or a state Attorney General (or a violator) before bringing certain actions.

ADPPA would generally preempt state laws that are "covered by the provisions" of the bill but would not preempt 16 categories of state laws, including generally applicable consumer protection laws as well as data breach notification laws. The bill's potential preemption of state laws has generated some criticism from state stakeholders and may be one of the chief obstacles to the bill's ultimate success in both chambers of Congress.

## Other Notable Federal Legislation and Actions

### Infrastructure Investment and Jobs Act

Also known as the Bipartisan Infrastructure Framework (BIF), the infrastructure bill was enacted in November 2021 and included funding for a $1.0 billion grant program (over four years) for state and local governments to improve their cybersecurity measures. Under the program, qualifying governments will be required to present DHS with comprehensive cybersecurity plans. The Act also includes $550 million in funding for electric grid cybersecurity programs, as well as $140 million ($20 million annually for seven years) for a Cyber Incident Response and Recovery Fund to help entities affected by cyber incidents.

BIF also amended the Internal Revenue Code to require taxpayers to report when they receive or transfer $10,000 or more in digital assets in certain transactions. This revision aligns cryptocurrency transactions with existing requirements for fiat currency transactions above $10,000, which businesses must report to the Internal Revenue Service (IRS), along with the identities of the parties engaged in the transaction. (Ransomware payments are frequently made via cryptocurrency, due to the putative anonymity and nonphysicality of the payment scheme. As such, the Treasury Department had, in 2021, proposed requiring businesses to report cryptocurrency transfers of more than $10,000 to the IRS.) Prior to the enactment of BIF, IRS already required individuals to report capital gains from cryptocurrency transactions on the 1040 Form.

### CHIPS and Science Act

In August 2022, President Biden signed into law the CHIPS and Science Act of 2022, which is designed to bolster a domestic semiconductor industry within the United States, most notably through $52.7 billion in appropriations (over five years) for semiconductor incentives. The Act also appropriates $400 million annually from fiscal 2023 through 2027 for the CHIPS Defense Fund, through which the Department of Defense is meant to facilitate the production of secure

semiconductors related to national security and critical infrastructure applications. The law additionally authorizes approximately $170 billion over five years for research and development initiatives, including to promote research security and develop cybersecurity standards.

### State and Local Government Cybersecurity Act

The State and Local Government Cybersecurity Act of 2021, which President Biden signed into law in June 2022, provides for cybersecurity-related collaboration between DHS and state, local, tribal, and territorial governments, as well as corporations, associations, and the general public.

The Act expands DHS responsibilities through grants and cooperative agreements, including provision of assistance and education related to cyber threat indicators, proactive and defensive measures and cybersecurity technologies, cybersecurity risks and vulnerabilities, incident response and management, analysis, and warnings.

The Act also requires the National Cybersecurity and Communications Integration Center, upon request, to coordinate with entities such as the Multi-State Information Sharing and Analysis Center to engage in specified activities, including to (1) conduct exercises with state, local, tribal, or territorial government entities; (2) provide operational and technical cybersecurity training to such entities; and (3) promote cybersecurity education and awareness.

### Better Cybercrime Metrics Act

In May 2022, President Biden signed into law the Better Cybercrime Metrics Act, which establishes various requirements to improve the collection of data related to cybercrime and cyber-enabled crime. Among other requirements (1) DOJ must enter into an agreement with the National Academy of Sciences to develop a taxonomy for categorizing different types of cybercrime faced by individuals and businesses; (2) DOJ must establish a category in the National Incident-Based Reporting System for collecting cybercrime reports from federal, state, and local officials; (3) DOJ's Bureau of Justice Statistics and the Bureau of the Census must include questions about cybercrime in the annual National Crime Victimization Survey; and (4) the U.S. Government Accountability Office (GAO) must assess the effectiveness of reporting mechanisms for cybercrime and disparities in reporting cybercrime data and other types of crime data.

### National Cybersecurity Preparedness Consortium Act

In May 2022, President Biden signed into law the National Cybersecurity Preparedness Consortium Act of 2021, which allows DHS to work with one or more consortia composed of nonprofit entities to develop, update, and deliver cybersecurity training and education in support of homeland security.

### K-12 Cybersecurity Act

In October 2021, President Biden signed into law the K-12 Cybersecurity Act, which requires CISA to study specific cybersecurity risks facing K-12 educational institutions, including securing school information systems and records and the cybersecurity challenges of remote learning. Following the study, CISA must develop recommendations for voluntary cybersecurity guidelines for K-12 schools and an online training toolkit for school officials.

### Ransomware Act

H.R. 4551, which passed the House of Representatives on July 27, 2022, requires 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.

### Quantum Computing Cybersecurity Preparedness Act

S. 4592/H.R. 7535 are companion bills designed to address the transition of agencies' IT systems to post-quantum cryptography (*i.e.*, encryption strong enough to resist attacks from quantum computers developed in the future). The bills require OMB to submit a report to Congress within one year on strategy, necessary funding, and standards relating to quantum computing and post-quantum cryptography. H.R. 7535 passed the House of Representatives on July 12, 2022.

### Understanding Cybersecurity of Mobile Networks Act

H.R. 2685, which passed the House of Representatives on December 1, 2021, 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 must 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.

### DHS Industrial Control Systems Capabilities Enhancement Act

S.2439/H.R. 1833 are companion bills that direct CISA to (1) lead federal efforts to identify and mitigate cybersecurity threats to industrial control systems (the products and technologies intended for use in the automated control of critical infrastructure processes, including pipelines, water supply, and electric utilities); (2) maintain threat hunting and incident response capabilities; (3) provide technical assistance to public and private-sector entities to help identify and mitigate

vulnerabilities; and (4) collect and disseminate information regarding vulnerabilities to the industrial control systems community. H.R. 1833 passed the House of Representatives on July 20, 2021.

**State and Local Cybersecurity Improvement Act**

H.R. 3138, which passed the House of Representatives on July 20, 2021, requires CISA to establish the State and Local Cybersecurity Grant Program to address cybersecurity risks and threats to state and local information systems. Eligible grant applicants (*i.e.*, states and certain Indian tribes) must submit a cybersecurity plan meeting specified criteria and subject to CISA approval. 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 to the entity's information systems. 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 to state and local information systems. CISA must develop and maintain a resource guide for state, local, tribal, and territorial government officials to assist those officials 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. CISA must also assess the feasibility of implementing a short-term rotational program to assign approved state, local, tribal, and territorial government employees to CISA in cyber workforce positions.

**Computer Fraud and Abuse Act: Van. Buren v. United States**

In June 2021, the U.S. Supreme Court issued its decision in *Van Buren v. United States*, 593 U.S. (2021), the first major case interpreting the federal CFAA. The CFAA prohibits unauthorized access to a computer, and the case explored what constitutes "unauthorized access." There are two ways of violating the statute – "access without authorization" and "exceed[ing] authorized access." The facts of the case presented the Supreme Court with an opportunity to interpret whether "unauthorized access" is more narrowly limited to *technologically* unauthorized activities such as hacking, or more broadly applicable to situations where an individual might technically have access to a computer, and yet nonetheless accesses certain areas for purposes beyond the wishes of a site administrator. Judicial circuits were split on their interpretation of the CFAA.

In a 6-3 decision, the Supreme Court rejected the federal government's broad interpretation of the statute and adopted a narrower reading. According to the court, to violate the CFAA, a person must enter "particular areas of the computer – such as files, folders, or databases – that are off limits to him." Put another way, "…liability under [the statute] stems from a gates-up-or-down inquiry – one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." Under this reading, a person does not violate the statute if he or she was given access to the relevant database. Nonetheless, the Supreme Court did not resolve whether "down gates" may only consist of *bona fide* technological limitations on access, or

whether other types of limits or policies (such as a term of service or contractual clause) may also constitute "gates" that prohibit access.

In May 2022, DOJ announced the revision of its policy regarding charging violations of the CFAA. For the first time, DOJ directed federal prosecutors that good-faith security research should not be charged. The guidance further stated that hypothetical violations that should not be charged under the CFAA include (1) embellishing an online dating profile contrary to the terms of service of the dating website; (2) creating fictional accounts on hiring, housing, or rental websites; (3) using a pseudonym on a social networking site that prohibits them; (4) checking sports scores at work; (5) paying bills at work; or (6) violating an access restriction contained in a term of service. DOJ explained that its policy "focuses the department's resources on cases where a defendant is either not authorized at all to access a computer or was authorized to access one part of a computer…and, despite knowing about that restriction, accessed a part of the computer to which [the] authorized access did not extend, such as other users' emails."

## Insurance

With cyberattacks increasing in frequency and severity in recent years, companies have been taking out cyber insurance policies to offset the costs that are incurred when, in the wake of attacks, the companies' operations go offline, and cyber ransoms are paid. In turn, the increasing frequency and severity of claims – along with the ongoing, uncertain, and evolving nature of the threat posed by cyber criminals – is causing cyber insurance to become more expensive.

According to the National Association of Insurance Commissioners (NAIC), cyber insurance premiums have more than doubled since 2015, totaling $3.2 billion in 2020. The average paid loss for a cyber claim increased in 2020 to $358,000, from $145,000 in 2019; the second quarter of 2021 saw cyber insurance rates increase 56%. However, coverage may still outweigh the cost of being uninsured. According to a 2018 study, 60% of small businesses close within six months of a cyberattack.

Standalone cyber insurance policies arose because traditional insurance policies (*i.e.*, commercial general liability, professional liability, errors and omissions, directors and officers, kidnap and ransom, etc.) typically did not cover cyber risks expressly. Given the uncertainty as to whether damage from cyberattacks would fall under the coverage terms of more traditional plans, some insurers started to modify those policies to explicitly exclude cyber risks from traditional coverage. Standalone cyber policies thus developed to cover losses from data breaches, ransomware attacks, theft of unencrypted assets, insider threats, denial of service attacks, supply chain cyberattacks, phishing scams, exploitation of cloud misconfigurations, cybersecurity litigation, investigations, and business interruption coverage for network downtime, etc. According to one business report, the cost of business interruption and post-incident recovery costs make up more than half of the value of cyber insurance claims.

Cyber insurance typically covers *first-party* losses (*e.g.*, losses the insured party incurs directly from an incident, such as data retrieval and restoration, ransomware payments, breach notification, credit monitoring, public relations fees to handle reputational fallout), and *third-party* losses that arise from liability to others (*e.g.*, litigation, regulatory fines, or indemnification of clients). In general, cyber insurance policies are highly variable and tailored to the covered party. For example, particular policies may not cover the costs of future lost profits, personal injury, or physical property damage related to the incident. If a policy excludes losses arising from "acts of war or terrorism," it could be an open question as to whether the coverage will apply if the cybercriminal was acting with the tacit support of a foreign power such as Russia or China.

A policy's cost is based on a number of risk-related factors, such as the covered entity's size and annual revenue, the type and sensitivity of data handled, and the overall security of the entity's network (*i.e.*, security measures already in place, incident response plans, network preparedness, and employee training). Insurance policies are often reassessed every year, and – especially given the recent increase in risks and payouts – premiums may increase, terms and conditions may be adjusted, and some insurers may reduce future payouts.

Additionally, given the increasing scale of cyber risks and the increased cost of payouts, insurance companies are tightening standards and asking tougher questions during the underwriting process, inquiring about entities' networks, and requiring entities to take proactive and preventive measures before a policy is approved. As such, in addition to the other regulatory efforts that may be pursued at the federal and State level, precautionary measures that are being imposed by insurers as part of the underwriting process may contribute to companies shoring up their networks and thereby raise the overall resiliency and strength of the cybersecurity environment.

### National Association of Insurance Commissioners Insurance Data Security Model Law

In 2017, NAIC adopted an Insurance Data Security Model Law for states to adopt in order to encourage insurers to better protect their consumers' personal information, as well as to establish uniform security standards. The model law requires insurers and other entities that are licensed by state insurance departments to develop and maintain information security programs based on risk assessments and to investigate and inform state insurance commissioners about a cyber incident. (Entities with fewer than 10 employees, or which are compliant with federal HIPAA, are exempt from the model law.) Under the model law, state insurance regulators have the power to investigate compliance with the law and remedy deficiencies. The model law does not create a private cause of action or limit already-existing private causes of action. Notably, a drafting note in the model law states that if any entity is in compliance with the regulations issued by New York's Department of Financial Services (discussed above), the entity would be deemed to be in compliance with the model law.

The U.S. Treasury Department has recommended that states adopt the model law; as of June 2022, 21 states (including Maryland) had adopted the model law, with certain variations in the provisions ultimately adopted among the various states.

## Conclusion

As seen by the recent, noteworthy cyberattacks and the various actions taken at both the State and federal level, cybersecurity is a critical issue for State governments, the federal government, and private businesses. As hackers become more advanced and important information continues to move online, cybersecurity will likely continue to be a topic of discussion. This report is meant to be a guide for such discussions.