

**LLAGNY Education Committee Program**  
***Blockchain: What Information Professionals Need to Know***

**October 15, 2019**

**Anna Irvin, Ph.D. and Janice E. Henderson, Esq.**

## **BACKGROUND**

[\*\*Blockchain and the Legal Profession\*\*](#), ed. by Alex Davies, ARK Group, June 2018

An in-depth look at the impact Blockchain will affect the legal profession, both in terms of how processes will change in the future, and the legal issues that lawyers will have to become aware of in an increasingly digital era.

[\*\*Blockchain Law: ICO Regulation and Other Legal Considerations in the Blockchain Ecosystem\*\*](#), by Dror Futter (PLI Current: The Journal of PLI Press, vol. 2, no. 1 (Winter 2018)

An in-debt discussion and explanation of ICOs (Initial Coin Offerings).

[\*\*Blockchain-Based Innovation in Cross-Border Payments: Public Policy Opportunities and Regulatory Challenges\*\*](#), by Jessie Cheng (PLI Current: The Journal of PLI Press, vol. 2, no. 1 (Winter 2018)

Discussion of cross-border payments and their mechanics over current correspondent banking relationships. The article highlights significant pain points in current transaction models which may be solved by blockchain-based distributed financial technologies.

[\*\*Beyond Bitcoin: Blockchain and Distributed Ledger Technology Industry Applications and Regulatory Concerns\*\*](#), by Lee G. Petro & Katherine E. Armstrong (PLI Current: The Journal of PLI Press, vol. 2, no. 1 (Winter 2018)

Excerpt: This article provides an overview of DLT (distributed ledger technology), a discussion of how the technology is being used to address industry-specific issues, and an analysis of certain regulatory issues presented by the use of DLT, both in the United States and in Europe.

[\*\*How Blockchain Technology Is Transforming the Legal Industry\*\*](#) by Jasmine Ye Han, Daily Labor Report (Bloomberg Law), February 20, 2018

Excerpt: Blockchain technology is now being used to build tools and infrastructure that help lawyers draft contracts, record commercial transactions, and verify legal documents. Two examples of such tools and infrastructure are OpenLaw and Integra Ledger.

[\*\*Blockchain neophyte carves out niche in cryptocurrency litigation\*\*](#) , ABA Journal, February 9, 2019

Excerpt: The world of cryptocurrency soon spilled over into his practice. He learned that the under-regulated industry has tremendous potential for fraud and that investors have suffered real losses. The Coral Springs, Florida-based plaintiffs' attorney, who had mainly concentrated on securities and financial fraud cases, began to carve out a niche representing allegedly defrauded cryptocurrency investors in class-action lawsuits against the largest crypto exchanges and companies that conducted initial coin offerings.

[\*\*3 Lessons From A Crypto Mock Trial\*\*](#) , Law360, February 22, 2019

Excerpt: As blockchain and crypto are poised to permeate the litigation landscape, regardless of practice area, counsel need to take the time to learn as much as they can about blockchain well in advance of the trial or even discovery.

## [4 Risks for Implementing the New Age of Legal Technologies](#) by By Zach Warren, Legaltech News 2.17.19

Artificial intelligence and the blockchain could have a number of novel uses in the legal world. But as IBM's Shawnna Hoffman noted during the ctrl ALT del conference, they need to be used correctly.

## [Lex Mundi White Paper Series Offers Crash Course in Blockchain](#) By Caroline Spiezio, Corporate Counsel Daily, February 6, 2019

A 10-paper series from law firm networking group Lex Mundi aims to introduce in-house counsel to blockchain by answering frequently asked questions.

## [What Does It Say When a Legal Blockchain e-Book Has 1.7M Views?](#) Forbes, January 14, 2019

Introduction: *Blockchain for Lawyers*, a recently-released e-book by Australian legal tech company Legaler drew 1.7M views in two weeks. What does that staggering number say about blockchain, legal technology, and the legal industry? (KnowItALL 1.14.2019)

## [Blockchain Made Big Strides in the Legal Services Market During 2018](#) by Frank Ready, Legaltech News, December 23, 2018 (available on Lexis)

## [Blockchain: Immutable Ledger, But Admissible Evidence?](#) by Neil Gray and Maxwell J. Eichenberger, New York Law Journal, December 14, 2018

This article begins with a brief overview of blockchain technology, then addresses the current evidentiary hurdles blockchain records face, and concludes with considerations for attorneys seeking to enter blockchain receipts (discussed further below) into evidence and businesses implementing blockchain solutions.

## [Blockchain and Algorithms: Antitrust in the Digital Age \(View Recording\)](#), LexisNexis® InfoPro Weekly Update, December 13, 2018

Please join LexisNexis for a webinar with Robin Adelstein and Eliot Turner of Norton Rose Fulbright discussing common antitrust issues that arise as companies consider adopting blockchain and pricing algorithms and how to navigate antitrust risk including...

## [The Latest Blockchain Craze: Trademark Lawsuits](#) by Alexis Kramer, Bloomberg Law Tech & Telecom Law News, November 29, 2018

The blockchain explosion has unleashed a wave of trademark infringement lawsuits against companies that promote cryptocurrency and digital ledger services.

## [Big Law Attorneys Launch Blockchain-Powered In-House Workflow Software](#) by Victoria Hudgins, NJLJ, November 25, 2018

NMBL Technologies and Dragonchain are partnering for new, blockchain-powered workflow and document management tools geared toward in-house that are set to be released next year.

## [Online Advertisers Embrace Blockchain to Fight Fraud](#) by Alexis Kramer, Bloomberg Law Tech & Telecom Law News, January 4, 2019

Brands are eyeing blockchain as a way to fight advertising fraud. The complexity of online advertising and the struggle to track ad spending has allowed fraudsters to avoid being caught, attorneys told Bloomberg Law. But blockchain technology can uncover ad performance discrepancies and let advertisers and publishers know how many clicks an ad is really getting, the attorneys said.

## [Protecting Blockchain Investments in a Patent Troll World](#) by Kelli Spearman, 26 J. Intell. Prop. L. 173, Spring 2019 (available on Westlaw)

Excerpt: The rising popularity of the blockchain has created an intellectual property gold-rush as firms hoping to capitalize on new adaptations race to the patent office to have their “substantial improvements” recorded. This note provides necessary background material regarding intellectual property, particularly patent and copyright law, its underlying policy and implementations, and application to the blockchain.

**[Blockchain and IP Law: A Match made in Crypto Heaven?](#)** by Birgit Clark, Baker McKenzie, WIPO Magazine, February 2018

Introduction: Blockchain and related distributed ledger technologies have been a hot topic recently, with multiple industries exploring their possibilities and new blockchain use cases emerging almost every day. But how might these technologies be used in the context of intellectual property (IP) law and practice?

**[How blockchain can change how we view IP rights](#)** by AWA, Mondaq, November 12 2018

Blockchain has lately risen in popularity with uses such as the cryptocurrency Bitcoin, and new applications are implemented or suggested almost daily. As an emerging technology with the possibility to validate, preserve and track digital data, and to provide a platform for low cost and transparent for transactions on a global scale, it has the possibility to revolutionize sharing of digital assets. So what are the implications for the management of intellectual property?

**[Blockchain and Digital Assets, Investment Adviser Regulation: A Step-by-Step Guide to Compliance and the Law, 3<sup>rd</sup> ed., ch. 64 \(June 2019\)](#)**

A detailed overview of blockchain technology.

## GENERAL - PRACTICE NOTES

**[Blockchain Update Tracker, Practical Law](#)**

This resource provides a road map to Practical Law's Legal Update coverage of blockchain and blockchain-related topics to help counsel track the latest developments for federal and state. The tracker covers distributed ledger technology (DLT), smart contracts, digital assets, including cryptocurrency/virtual currency, regulation of digital coins and tokens, and other blockchain-related matters.

**[Blockchain and Distributed Ledger Laws: State-by-State Adoption, Practical Law](#)**

This Note is a summary of all state legislative introduction and adoption of blockchain ledger laws.

**[Blockchain and Supply Chain Management, Practical Law](#)**

A Practice Note providing an overview of the use of blockchain and smart contracts in the supply chain context including the legal issues, concerns, benefits, and risks associated with its use. It includes information on key distinctions between public and private blockchains and important considerations regarding the use of blockchain consortia.

**[Blockchain Basics for In-House Counsel, Practical Law](#)**

A Practice Note addressing key blockchain issues for in-house counsel's consideration. This Note discusses how blockchain technology works and its most common applications, including serving as the foundation for virtual currencies and smart contracts.

**[Understanding Smart Contract Mechanics, Practical Law](#)**

A Practice Note providing a practical explanation of how blockchain smart contracts work and an examination of issues presented by the application of traditional contract principles to smart contracts. This Note also provides a technical illustration of amendment and termination of smart contracts on the Ethereum blockchain smart contract platform.

[\*\*Application of Distributed Ledger Technology to Financial Services Regulation and Compliance, Practical Law\*\*](#)

A Practice Note examining how blockchain and distributed ledger technology (DLT) can facilitate regulatory compliance in banking and financial services, saving time and expense, and preventing errors. The Note details a test case for the application of DLT to regulatory compliance using the example of CFTC swap data reporting regulations.

[\*\*Security Interests: Bitcoins and Other Cryptocurrency Assets, Practical Law\*\*](#)

A discussion on collateral comprised of bitcoins and other cryptocurrencies and the methods of perfecting a security interest therein under the UCC. This Note also examines other issues relating to cryptocurrency collateral.

[\*\*Understanding the SEC's Digital Asset Framework and Approach to Digital Asset Regulation, Practical Law\*\*](#)

A Practice Note providing a chronology and explanation of recent Securities and Exchange Commission (SEC) activity relating to its approach to regulation of digital assets, including virtual currency (VC) and cryptocurrency, as well as digital tokens issued in offerings such as initial coin offerings (ICOs) and security token offerings (STOs).

[\*\*Virtual Currency Business Regulation \(NY State\), Practical Law\*\*](#)

A Practice note discussing the licensing and regulation of virtual currency businesses under New York State Law.

[\*\*In Focus: Blockchain, Bloomberg Law\*\*](#)

BLAW primer, federal and state legislative and regulatory trackers, legal analysis, Blockchain patent analytics, litigation, news and more.

**CLE PROGRAMS/MATERIALS**

**[PLI CLE Program TechLaw Institute 2019: The Digital Evolution](#)**

PLI presents "TechLaw Institute 2019: The Digital Evolution" where a faculty of leading practitioners will discuss artificial intelligence, blockchain and Bitcoin, disruptive technologies and the shared economy, data breaches, advertising and social media, privacy developments, CCPA and GDPR, and legal ethics concerns in tech. This program will take place in two locations in March: San Francisco (with a Webcast) and New York. (PLI SmartBrief 2.13.19)

**[Blockchain Technology, Smart Code, and Smart Contracts: Issues and Risks, PLI CLE Program, Recorded on: December 11, 2018](#)**

Many people know that bitcoin is based on blockchain technology, but fewer understand how the underlying technology is being applied to a much broader range of commercial and business functions. At 1 p.m. Eastern on Dec. 11, tune in to PLI's One-Hour Briefing and hear from expert faculty as they explore what smart code and smart contracts are and how they are different, how blockchain technology actually works, and more.

**[Corporate Counsel Symposium: Advising Through Partnering, City Bar Center for Continuing Legal Education, New York City Bar, December 7, 2018 \(available on Westlaw\)](#)**

**[COUNSELING YOUR BUSINESS ON BLOCKCHAIN TECHNOLOGY \(POWERPOINT\), 20181207A NYCBAR 96](#)**

**[Blockchain for Lawyers, City Bar Center for Continuing Legal Education, New York City Bar, May 10, 2018 \(available on Westlaw\)](#)**

**[BLOCKCHAIN TECHNOLOGY AND SMART CONTRACTS SIMPLIFIED \(POWERPOINT\), 20180510P NYCBAR 262](#)**

**[Bitcoin and Initial Coin Offerings \(ICOs\): A Primer on Offerings, Trading and Enforcement, City Bar Center for Continuing Legal Education, New York City Bar, January 18, 2018 \(available on Westlaw\)](#)**

## BLOCKCHAIN AND THE U.S. GOVERNMENT

### Wyoming and Vermont hope to attract tech entrepreneurs by passing laws favorable to blockchain, ABA Journal, March 2019

Excerpt: The state's new laws exclude virtual currency from money transmitter rules, define some tokens—means to access a blockchain—as outside of securities regulations and allow for electronic networks to be used in the creation and maintenance of corporate records. The hope is that these rules will lower regulatory hurdles and clear up ambiguity so that blockchain-based businesses and business practices can flourish. [This article appeared in the March 2019 issue of the ABA Journal with the headline "Blockchain LLC: Wyoming and Vermont relax regulations and pass favorable laws relating to blockchain, hoping they can attract tech entrepreneurs."]

### Blockchain White Paper, National Archives and Records Administration (NARA), February 2019 <https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf>

Introduction: The National Archives and Records Administration (NARA) undertook a research project in fiscal year 2018 to understand how blockchain works, to learn how it is being used in the Federal government, and to discuss the potential implications for records management.

### SEC Takes Aim at Digital Tokens and Smart Contracts by Robert A. Schwinger, New York Law Journal, January 18, 2019

In his Blockchain Law column, Robert A. Schwinger discusses a wave of new enforcement actions brought by the SEC targeting blockchain-based digital token ventures under a variety of provisions in the securities laws.

### Crypto Lobbying Doubles as Industry Seeks Washington Friends, Bloomberg Law Tech & Telecom Law News February 8, 2019

Crypto and blockchain-related congressional lobbying took off in 2018 as some of the industry's top players realized they should go to Washington before Washington comes for them.

### Securities on Blockchain, By Reade Ryan and Mayme Donohue, 73 The Business Lawyer 85 (2017-2018)

This article initially provides a high-level description of blockchain technology intended to be accessible to those without a technical background, and illustratively describes an existing blockchain system that already evidences securities issued and being traded. The article then sets forth and analyzes how Article 8 of the Uniform Commercial Code covers blockchain securities as "uncertificated securities." Finally, the article provides guidance to corporate lawyers faced with giving a legal opinion relating to the issuance and sale of securities on a blockchain.

## INTERNATIONAL REGULATORY LANDSCAPE

In 2018, the European Commission proposed to develop a European Blockchain Partnership, triggering the creation of the EU Blockchain Observatory and Forum (<https://www.eublockchainforum.eu/>), which has already published a number of **thematic reports** (<https://www.eublockchainforum.eu/reports> ).

The ISA ELISE Action recently published the following study: "Blockchain for digital government - An assessment of pioneering implementations in public services." The new publication analyses seven blockchain-based services developed in Europe, with an active participation of public authorities from both national and local levels.

The list of analyzed projects includes:

- [Exonum land title registry](#)
- [Blockcerts academic credentials](#)
- [Chromaway property transactions](#)
- [uPort decentralised identity](#)
- [Infrachain governance framework](#)

- [Pension Infrastructure](#)
- [Stadierspas smart vouchers](#)

The European Economic and Social Committee (EESC) is currently working on a report on Blockchain and the single market (<https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/blockchain-and-eu-single-market-what-next-own-initiative-opinion>), due to be finalized in October 2019.

### [\*\*Regulation of Cryptocurrency Around the World\*\*](#), Library of Congress Legal Report (Last Updated: January 22, 2019)

This report surveys the legal and policy landscape surrounding cryptocurrencies around the world. This report covers 130 countries as well as some regional organizations that have issued laws or policies on the subject.

### [\*\*The European Commission aims to develop a common approach on Blockchain technology for the EU in the international arena\*\*](#), European Commission (Last update: February 1, 2019)

Blockchain may bring great improvements for the European industry - from start-ups to large corporates, administrations and citizens. It can enable the provision of more efficient services and the emergence of new ones...

### [\*\*European countries join Blockchain Partnership\*\*](#), European Commission (Last update: February 1, 2019)

On April 10 2018, 21 Member States and Norway agreed to sign a Declaration creating the European Blockchain Partnership (EBP) and cooperate in the establishment of a European Blockchain Services Infrastructure (EBSI) that will support the delivery of cross-border digital public services, with the highest standards of security and privacy. Since then, 5 more Member States have joined the Partnership...

### [\*\*EU Blockchain Observatory and Forum\*\*](#)

The European Union Blockchain Observatory and Forum aims to accelerate blockchain innovation and the development of the blockchain ecosystem within the EU, and so help cement Europe's position as a global leader in this transformative new technology.

### [\*\*Blockchain Technology and Anti-Money Laundering Regulations under International Law\*\*](#) by Yurika Ishii, The American Society of International Law, ASIL Insights, Vol.23, Issue 1, February 22, 2019

In October 2018, the Financial Action Task Force (FATF), an intergovernmental organization in charge of anti-money laundering (AML) and counter-terrorist financing regulations, announced that it would issue guidelines on virtual asset by June 2019...

## **BLOCKCHAIN AND INFORMATION PROFESSIONALS**

### [\*\*Blockchain Reaction\*\*](#), By Carrie Smith, American Libraries / 3.1.2019

Introduction: How library professionals are approaching blockchain technology and its potential impact.

### [\*\*AALL Blockchain Resource Guide\*\*](#), Created in November 2018 by Debbie Ginsberg, Educational Technology Librarian, Chicago-Kent College of Law

## **BLOCKCHAIN AND FINANCIAL INDUSTRY**

### [\*\*Block to the Future II: Finance, Transformed\*\*](#), By Stephen J. Obie and Harriet Territt , Corporate Counsel, March 4, 2019

Financial institutions were among the first wave of commercial businesses to explore how blockchain technology can be applied to different aspects of financial markets, including syndicated lending, payment systems, and administration of capital markets.

[Why cryptocurrency and blockchain will be banks' next big growth opportunity](#), 36 No. 16 Westlaw Journal Computer & Internet 03, January 11, 2019

Ryan Rafols, the CEO and co-founder of private equity marketplace Newchip, discusses the advantages blockchain technology and cryptocurrency hold for financial institutions.

[Focus on blockchain's risks before the rewards](#) by Kirk Phillips, Financial Management, August 1, 2018

The digital ledger technology carries enormous transformative potential, but finance professionals must adapt their risk management practices to the legal and security concerns that accompany it.

## INDUSTRY AND BUSINESS APPLICATIONS

[Navigating The Risks Of Blockchain Technology In Commercial Real Estate](#) by Pryor Cashman LLP, February 15, 2019

In their latest article for Commercial Observer, Eric Sherman and Marion Harris explain that while significant legal and regulatory uncertainty remains, the promise of blockchain is rapidly gaining traction in the world of commercial real estate. (Mondaq)

[Virtual Currencies and Blockchain in 2018](#), Wolters Kluwer White Paper, Securities Regulation Daily, January 2, 2019

The Business Blockchain is an invitation for technologists to better understand the business potential of the blockchain, and for business minded people to grasp the many facets of blockchain technology. This book teaches you how to think about the blockchain.

[Legal Contract Blockchain Platform Monax Launches Public Beta](#) Silicon Angle / February 15, 2019

Introduction: Monax Industries, a legal digital infrastructure provider, today announced the launch of its distributed ledger blockchain service for legal contract applications into a public beta, making it generally available for production-level commercial use. The service, called the Monax Platform, provides all a business needs to register, assign and track legal "smart contracts" using a tamper-proof digital ledger. (KnowItALL 2.15.2019)

[Legal Operations Leaders Say Blockchain, Artificial Intelligence Still Not Mainstream in Their Companies](#) by Sue Reisinger, Corporate Counsel Daily, February 1, 2019

Those are some of the key findings in the 2019 Consero Legal Operations Survey Report, based on a poll of 85 legal ops executives who attended a recent forum.

[A proposed agreement for a blockchain-enabled medical staff credentialing process](#), 28 No. 06 Westlaw Journal Professional Liability 01, October 18, 2018

J. Mark Waxman and Jennifer Rathburn of Foley & Lardner discuss the possibility of using blockchain technology in the medical staff credentialing process and propose a form of agreement to be used for that purpose. The medical credentialing process, whether for a hospital, a hospital system or a health plan, has emerged as a potential early target...

[What's in a Blockchain? With New Tools, Anyone Can Find Out](#), By Morgen Peck, IEEE Spectrum / 2.22.2019

Services available through Google's BigQuery platform make it easy to search and analyze blockchain transactions.

## AGREEMENTS / CONTRACTS

[Corporate Finance and the Securities Laws \(5<sup>th</sup> ed\)](#), By Charles J. Johnson, Joseph McLaughlin and Eric S. Haueter, Wolters Kluwer, §2.03, The Underwriting Agreement, Sec. N, Purchase and Sale; Closing; Blockchain!; "Green Shoe" Closing.

This title has an example of an underwriting agreement with a blockchain clause.

### [\*\*Are Smart Contracts the Best of Blockchain?\*\*](#) By Joe Liebkind, June 25, 2019

As cryptocurrency gains greater application and adoption, smart contracts effectively enable trade with significantly fewer barriers. Companies are already racing to the space to build straightforward contractual solutions for businesses of all shapes and sizes.

### [\*\*A quick guide to understanding blockchain smart contracts\*\*](#), By Yessi Bello Perez, Hard Fork Basics (2019)

Smart contracts have been deemed potentially revolutionary across a range of industries with some observers going as far as saying that they will replace traditional contracts and lawyers.

## **STATE RESOURCES**

### **California**

#### [\*\*California Government Operations Agency\*\*](#)

The Government Operations Agency will be forming a Blockchain Working Group as part of the implementation of [Government Code Section 11546.9](#).

### **Colorado**

#### [\*\*Colorado hires 'blockchain solution architect'\*\*](#), by Benjamin Freed, May 23, 2019

The Colorado Office of Information Technology has hired its inaugural “blockchain solution architect” to devise ways the state can use the distributed-ledger technology in government.

### **New York**

#### [\*\*Department of Financial Services – Cybersecurity Resource Center\*\*](#)

Contains NYS cybersecurity regulation, FAQs, cybersecurity filing requirements, etc.

## STATES WITH BLOCKCHAIN LAWS

[Vermont](#) became the first state to address blockchain in legislation in 2015, when it directed the attorney general, Department of Financial Regulation, and secretary of state to report to the General Assembly on opportunities and risks of creating a presumption of validity for electronic facts and records that employ blockchain technology. Then, in 2016, the Vermont General Assembly created the evidentiary standards to determine the authenticity of records using blockchain technology within the state's rules of evidence.

In 2017, four states—Arizona, Delaware, Illinois and Nevada—enacted or adopted blockchain legislation. Arizona enacted two bills. The first, [H.B. 2417](#), established guidelines for electronic signatures and records using blockchain technology. In the second bill, [H.B. 2216](#), the Legislature made it unlawful to require a person to use or be subject to electronic firearm tracking technology, including blockchain and distributed ledger systems. Delaware enacted [S.B. 69](#), providing statutory authority for corporations formed in Delaware to use blockchain to create and maintain corporate records, including the corporation's stock ledger.

Following the formation of the [Illinois Blockchain Initiative](#)—a consortium of Illinois state and county agencies including the departments of Commerce and Economic Opportunity, Insurance, Financial and Professional Regulation, Innovation and Technology, and the Cooks County Recorder of Deeds—the Illinois General Assembly adopted a [joint resolution](#). The resolution created the Illinois Legislative Blockchain and Distributed Ledger Task Force to study how and if the state, county and municipal governments can benefit from a blockchain-based system for recordkeeping and service delivery.

Nevada enacted [legislation](#) recognizing blockchain technology as a type of electronic record for the purposes of the Uniform Electronic Transactions Act and prohibited local governments from taxing or imposing restrictions on the use of blockchain.

# Blockchain 2019 Legislation

7/23/2019

Blockchain is a distributed ledger technology that records and shares every transaction that occurs in the network of users.

One example of how blockchain works is in a sales transaction using distributed ledger technology and a digital currency as payment in the transaction. In this example, the buyer initiates the purchase, known as the block, which contains transaction data such as the date, time and payment amount. Both the buyer and seller can see the block of transaction data, so both parties can confirm that the payment was sent and received. Each transaction's block is created in a shared online accounting ledger that can involve multiple buyers and sellers within a network. As new transactions occur between the buyer and seller, each data block is recorded and forms the chain that documents the transaction history.

Blockchains can be permissionless, also called public, which are typically open for anyone to view and participate. Or, blockchains can be permissioned, which limit the participation to a single administrator or a specific group of participants.

Digital currencies are only one way to use blockchain. Other evolving applications can include online voting, medical records, insurance policies, property and real estate records, copyrights and licenses and supply chain tracking. They can also include smart contracts, where payouts between the contracted parties are embedded in the blockchain and automatically execute when contractual conditions have been met.

Twenty-eight states have introduced legislation relating to blockchain in 2019. Twenty-seven bills and resolutions have been enacted or adopted.

State	Bill Number	Bill Summary
Alabama	None	
Alaska	None	
Arizona	<a href="#">HB 2747</a> <i>Signed by governor 5/31/19, Chapter 263</i>	Appropriates \$2.5 million from the state web portal fund established by §18-421, Arizona Revised Statutes, in fiscal year 2019-2020 to the Arizona commerce authority to distribute to applied research centers and institutes located in this state that specialize in blockchain, wearable technology and automated mobility.
Arkansas	<a href="#">HB 1944</a> <i>Signed by governor 4/16/19, Act 1061</i>	Defines blockchain distributed ledger technology, blockchain technology, and smart contract; provides that a signature, record, or contract that is secured through blockchain technology is considered to be in electronic form; provides that a smart contract shall be considered a commercial contract.
California	<a href="#">SB 373</a> <i>Passed Senate 5/6/19</i>	Existing law requires the state registrar, local registrar, or county recorder, upon request and payment of the required fee, to supply to an applicant a certified copy of the record of a birth, fetal death, death, marriage, or marriage dissolution registered with the official. Existing law authorizes the state registrar, a local registrar, or a county recorder to furnish a certified copy of a birth, death, or marriage record to an

State	Bill Number	Bill Summary
		<p>authorized person and defines the term “authorized person” for these purposes. Existing law requires certain types of applicants for a certified record to execute a statement sworn under penalty of perjury that the person is an authorized person who is allowed to receive the certified record. Existing law requires certified copies of birth, death, and marriage records be printed on chemically sensitized security paper with specified features, including, among others, watermarks, fluorescent fibers, and intaglio print. This bill authorizes a county, until Jan. 1, 2022, to issue certified copies of marriage records by means of blockchain technology, as defined, and would exempt those records from the required physical properties and features in the provisions described above.</p>
Colorado	<a href="#">HB 1247</a> <i>Signed by governor</i> <i>5/30/19, Chapter 375</i>	<p>The bill directs the commissioner of agriculture to convene an advisory group to study the potential applications for blockchain technology in agricultural operations and to report to the General Assembly in 2020 with its findings and recommendations for legislation, if any. The advisory group is subject to repeal July 1, 2020.</p>
Colorado	<a href="#">SB 184</a> <i>Postponed indefinitely</i> <i>3/21/19</i>	<p>The bill directs the Colorado Water Institute at Colorado State University to study the potential uses of blockchain technology to manage a database of water rights; facilitate the establishment or operation of water markets or water banks, and for any other useful purpose in the administration of the institute's powers and duties; and report the results to the General Assembly.</p>
Connecticut	<a href="#">HB 5417</a> <i>Passed House</i> <i>5/22/19</i>	<p>Establishes a task force to study on blockchain technology for use in managing elector registration, including for the purpose of reducing duplicate registrations within the ledger upon which elector information is stored.</p>
Connecticut	<a href="#">HB 6062</a> <i>Failed Joint Favorable</i> <i>deadline 4/3/19</i>	<p>Establishes a task force to study the use of blockchain technology, or other similar technology, for the purpose of casting votes at an election by means of the internet.</p>
Connecticut	<a href="#">HB 7310</a> <i>Failed Joint Favorable</i> <i>deadline 3/19/19</i>	<p>Authorizes the use of smart contracts in commerce in the state.</p>
Connecticut	<a href="#">SB 1032</a>	<p>This bill requires the Office of Policy and Management (OPM) secretary to develop a plan to incorporate blockchain technology to make a state administrative function more efficient by Oct. 1, 2020, and in consultation with the Department of Administrative Service's</p>

State	Bill Number	Bill Summary
Connecticut	<a href="#"><u>SB 1033</u></a> <i>Failed Joint Favorable deadline 3/19/19</i>	Prohibits the use of noncompete agreements in the blockchain technology industry.
Delaware	<a href="#"><u>SB 89</u></a> <i>Signed by governor 6/19/19, Chapter 46</i>	This bill continues the practice of amending periodically the Delaware Revised Uniform Limited Partnership Act (the “Act”) to keep it current and to maintain its national preeminence. Section 1. This section amends §17-101 of the Act in several respects. New definitions are added for “document” and “electronic transmission,” which terms appear in new §17-113 among other places in the Act. Section 4. This section amends §§17-104(d) and 17-104(e) of the Act to include references to protected series and registered series, as appropriate, and §Section 17-104(g) to conform with the addition of the defined term “electronic transmission” in §17-101. Section 7. This section adds new §17-113 of the Act, which establishes non-exclusive, safe harbor methods to reduce certain acts or transactions to a written or electronic document and to sign and deliver a document manually or electronically. The terminology in §17-113(a) is based on analogous provisions in existing §§17-302(e) and 17-405(d) of the Act, the Delaware Uniform Electronic Transactions Act (“UETA”), and the Model Business Corporation Act, with modifications. Section 17-113(a) permits limited partnership transactions (such as entering into agreements of merger not filed with the secretary of state) to be documented, signed and delivered through “DocuSign” and similar electronic means. The §17-113(a) safe harbor provisions apply solely for purposes of determining whether an act or transaction has been documented, and whether a document has been signed and delivered, in accordance with the Act and the partnership agreement. Section 17-113(a) does not preempt any statute of frauds or other law that might require actions be documented, or that documents be signed and delivered, in a specified manner. Section 17-113(a) clarifies how its provisions operate in connection with a transaction conducted pursuant to UETA. To the extent UETA does not apply to a transaction (under §12A-103 of UETA) because the transaction is governed by the Act, the parties to the transaction can satisfy the Act by complying with §17-113(a). Section 17-113(b) addresses certain actions and documents that are not governed by §17-113(a). There is no presumption that these excluded items are prohibited from being effected by electronic or other means, but §17-113 may not be relied on as a basis for documenting an act or transaction, or signing or delivering a document,

State	Bill Number	Bill Summary
		<p>if the exclusions set forth in §17-113(b) apply. Certain of these excluded items are governed by separate provisions that facilitate the use of electronic media, including documents filed with the secretary of state (governed by §17-206(a)). Section 17-113(b) permits partnership agreement provisions that restrict the use of §17-113(a), but those restrictions must be expressly stated. A provision merely specifying that an act or transaction will be documented in writing, or that a document will be signed or delivered manually, will not prohibit the application of §17-113(a). Section 17-113(c) addresses the interaction between the provisions of the Act and the Electronic Signatures in Global and National Commerce Act (the “E-Sign Act”). Section 17-113(c) evidences an intent to allow the Act to govern the documentation of actions, and the signature and delivery of documents, to the fullest extent the Act is not preempted by the E-Sign Act. Sections 23 and 24. These sections amend §17-302(e) and §17-405(d) of the Act to conform with the addition of the defined term “electronic transmission” in §17-101.</p>
Delaware	<a href="#">SB 90</a>	<p><i>Signed by governor 6/19/19, Chapter 47</i></p> <p>This bill continues the practice of amending periodically the Delaware Revised Uniform Partnership Act (the “Act”) to keep it current and to maintain its national preeminence. Section 1. This section amends §15-101 of the Act to include definitions for “document” and “electronic transmission.” These terms appear in new §15-124 among other places in the Act. “Electronic transmission” previously was defined in §15-407(d) of the Act, and the new definition provides specific statutory authority for Delaware partnerships to use networks of electronic databases (examples of which are described currently as “distributed ledgers” or a “blockchain”) for “electronic transmissions.” Section 4. This section adds new §15-124 of the Act, which establishes non-exclusive, safe harbor methods to reduce certain acts or transactions to a written or electronic document and to sign and deliver a document manually or electronically. The terminology in §15-124(a) is based on analogous provisions in existing §15-407(d) of the Act, the Delaware Uniform Electronic Transactions Act (“UETA”), and the Model Business Corporation Act, with modifications. Section 15-124(a) permits partnership transactions (such as entering into agreements of merger not filed with the secretary of state) to be documented, signed and delivered through “DocuSign” and similar electronic means. The §15-124(a) safe harbor provisions apply solely for purposes of determining whether an act or transaction has been documented, and whether a document has been signed and delivered, in accordance with the Act and the partnership agreement. Section 15-124(a) does not preempt any statute of frauds or other law that might require actions be documented, or that documents be signed and delivered, in a specified manner. Section 15-124(a) clarifies how its provisions operate in</p>

State	Bill Number	Bill Summary
		<p>connection with a transaction conducted pursuant to UETA. To the extent UETA does not apply to a transaction (under Section 12A-103 of UETA) because the transaction is governed by the Act, the parties to the transaction can satisfy the Act by complying with §15-124(a). Section 15-124(b) addresses certain actions and documents that are not governed by §15-124(a). There is no presumption that these excluded items are prohibited from being effected by electronic or other means, but §15-124 may not be relied on as a basis for documenting an act or transaction, or signing or delivering a document, if the exclusions set forth in §15-124(b) apply. Certain of these excluded items are governed by separate provisions that facilitate the use of electronic media, including documents filed with the secretary of state (governed by §15-105(c)). Section 15-124(b) permits partnership agreement provisions that restrict the use of §15-124(a), but those restrictions must be expressly stated. A provision merely specifying that an act or transaction will be documented in writing, or that a document will be signed or delivered manually, will not prohibit the application of §15-124(a). Section 15-124(c) addresses the interaction between the provisions of the Act and the Electronic Signatures in Global and National Commerce Act (the “E-Sign Act”). Section 15-124(c) evidences an intent to allow the Act to govern the documentation of actions, and the signature and delivery of documents, to the fullest extent the Act is not preempted by the E-Sign Act. Section 5. This section amends §§15-403(c) of the Act to provide specific statutory authority for Delaware partnerships to use networks of electronic databases (examples of which are described currently as “distributed ledgers” or a “blockchain”) for the creation and maintenance of partnership records. Section 6. This section amends §15-407(d) of the Act to conform with the addition of the defined term “electronic transmission” in §15-101.</p>
Delaware	<p><a href="#"><u>SB 91</u></a>  <i>Signed by</i>  <i>governor</i>  <i>6/19/19, Chapter</i>  <i>48</i></p>	<p>This bill continues the practice of amending periodically the Delaware Limited Liability Company Act (the “Act”) to keep it current and to maintain its national preeminence. Section 1. This section amends §18-101 of the Act to include definitions for “document” and “electronic transmission,” and to amend the definitions of “manager” and “member.” The terms “document” and “electronic transmission” appear in new §18-113 among other places in the Act. The changes to the definition of “manager” confirm that the term includes a manager of the limited liability company generally and a manager associated with a series of the limited liability company, and the changes to the definition of “member” confirm that the term includes a member of the limited liability company generally and a member associated with a series of the limited liability company. Section 3. This section amends §18-104(g) to conform with the addition of the defined term “electronic</p>

State	Bill Number	Bill Summary
		<p>transmission” in §18-101. Section 4. This section adds new §18-113 of the Act, which establishes non-exclusive, safe harbor methods to reduce certain acts or transactions to a written or electronic document and to sign and deliver a document manually or electronically. The terminology in §18-113(a) is based on analogous provisions in existing §§18-302(d) and 18-404(d) of the Act, the Delaware Uniform Electronic Transactions Act (“UETA”), and the Model Business Corporation Act, with modifications. Section 18-113(a) permits limited liability company transactions (such as entering into agreements of merger not filed with the secretary of state) to be documented, signed and delivered through “DocuSign” and similar electronic means. The §18-113(a) safe harbor provisions apply solely for purposes of determining whether an act or transaction has been documented, and whether a document has been signed and delivered, in accordance with the Act and the limited liability company agreement. Section 18-113(a) does not preempt any statute of frauds or other law that might require actions be documented, or that documents be signed and delivered, in a specified manner. Section 18-113(a) clarifies how its provisions operate in connection with a transaction conducted pursuant to UETA. To the extent UETA does not apply to a transaction (under §12A-103 of UETA) because the transaction is governed by the Act, the parties to the transaction can satisfy the Act by complying with §18-113(a). Section 18-113(b) addresses certain actions and documents that are not governed by §18-113(a). There is no presumption that these excluded items are prohibited from being effected by electronic or other means, but §18-113 may not be relied on as a basis for documenting an act or transaction, or signing or delivering a document, if the exclusions set forth in §18-113(b) apply. Certain of these excluded items are governed by separate provisions that facilitate the use of electronic media, including documents filed with the secretary of state (governed by §18-206(a)). Section 18-113(b) permits limited liability company agreement provisions that restrict the use of §18-113(a), but those restrictions must be expressly stated. A provision merely specifying that an act or transaction will be documented in writing, or that a document will be signed or delivered manually, will not prohibit the application of §18-113(a). Section 18-113(c) addresses the interaction between the provisions of the Act and the Electronic Signatures in Global and National Commerce Act (the “E-Sign Act”). Section 18-113(c) evidences an intent to allow the Act to govern the documentation of actions, and the signature and delivery of documents, to the fullest extent the Act is not preempted by the E-Sign Act. Section 5. This section amends §18-206(b) of the Act to clarify that the certificate of formation or certificate of registered series, as applicable, shall be amended, corrected or restated upon the filing of a certificate of</p>

State	Bill Number	Bill Summary
		amendment (or judicial decree of amendment), certificate of correction, corrected certificate or restated certificate, and to confirm that a certificate of registered series is canceled upon a certificate of conversion of such registered series to protected series becoming effective. Section 6. This section amends §18-210 of the Act to provide that a plan of division may provide for contractual appraisal rights and that contractual appraisal rights may be made available in connection with any merger or consolidation in which a registered series is a constituent party, any division of the limited liability company, any conversion of a protected series to a registered series of the limited liability company, and any conversion of a registered series to a protected series of the limited liability company. Sections 14 and 15. These sections amend §§18-302(d) and 18-404(d) of the Act to conform with the addition of the defined term “electronic transmission” in §18-101.
District of Columbia	None	
Florida	<a href="#"><u>HB 735</u></a> <i>Laid on table</i> 5/1/19	Establishes Florida Blockchain Task Force in Department of Financial Services (DFS); provides for membership and duties of task force; requires task force to submit report to governor and Legislature and make presentations; requires DFS to provide support staff and other assistance to task force; provides for termination of task force.
Florida	<a href="#"><u>HB 1393</u></a> <i>Signed by governor</i> 6/25/19, <i>Chapter 140</i>	Requires the Division of Treasury to maintain certain warrants rather than turning them over to the Division of Accounting and Auditing; provides requirements for a combination license as funeral director and embalmer; revises the requirements for a funeral establishment and the requirements and responsibilities of a funeral director in charge; requires preneed licensees, under certain circumstances, to provide certain persons with a written notice of intent to distribute funds under the preneed contract; establishes the Florida Blockchain Task Force within the department, etc.
Florida	<a href="#"><u>SB 1024</u></a> <i>Signed by governor</i> 5/23/19	Establishes the Florida Blockchain Task Force within the Department of Financial Services; requires the task force to develop a specified master plan; specifies duties and procedures of the task force, etc.
Georgia	None	
Guam	Not available	
Hawaii	None	

State	Bill Number	Bill Summary
Idaho	None	
Illinois	<a href="#">HB 2540</a> <i>Signed by Governor</i> <i>Signed 8/9/19, Pub. Act 101-0259</i>	Creates the Blockchain Business Development Act. Provides that the secretary of state shall recommend legislation, including uniform laws, necessary to support the possible use of blockchain technology for public records; provides for the blockchain banking study.
Illinois	<a href="#">HB 3575</a> <i>Signed by Governor</i> <i>8/23/19, Pub. Act 101-0514</i>	Creates the Blockchain Technology Act. Provides for the permitted uses of blockchain technology in transactions and proceedings. Provides limitations to the use of blockchain technology. Prohibits units of local government from implementing specified restrictions on the use of blockchain technology. Defines terms.
Illinois	<a href="#">HB 3577</a>	Creates the Blockchain Technology Act. Contains only a short title provision.
Indiana	None	
Iowa	<a href="#">SF 137</a>	Relates to electronic transactions by permitting the use of distributed ledger technology and smart contracts.
Kansas	<a href="#">HB 2039</a> <i>Signed by governor</i> <i>4/18/19, Chapter 47</i>	The bill creates and amends law related to limited liability companies (LLCs) in the Kansas Revised Limited Liability Company Act (RLLCA), Business Entity Standard Treatment Act (BEST Act), and other statutes, as follows. Requires an LLC to maintain a current record identifying the name and last known business, residence, or mailing address of each member and manager, and to allow the use of electronic networks or databases, including distributed electronic networks or databases, to maintain records. Throughout the bill, provisions are added allowing the use of electronic networks or databases, including distributed electronic networks or databases, for certain electronic transmissions.
Kansas	<a href="#">HB 2105</a> <i>Passed House</i> <i>2/21/19</i>	Creates and amends law related to limited liability companies (LLCs) in the Kansas Revised Limited Liability Company Act (RLLCA), Business Entity Standard Treatment Act (BEST Act), and other statutes, as follows. Requires an LLC to maintain a current record identifying the name and last known business, residence, or mailing address of each member and manager, and to allow the use of electronic networks or databases, including distributed electronic networks or databases, to maintain records. Throughout the bill, adds provisions allowing the use of electronic networks or databases, including distributed electronic networks or databases, for certain electronic transmissions.

State	Bill Number	Bill Summary
Kentucky	<a href="#">HR 171</a> <i>Adopted 3/14/19</i>	Urges a comprehensive study of and subsequent plan to deal with the growing blockchain technology.
Louisiana	None	
Maine	<a href="#">LD 909</a>	Directs the commissioner of Economic and Community Development to establish a blockchain technology working group.
Maryland	<a href="#">SB 136</a> <i>Signed by governor 4/30/19, Chapter 288</i>	Authorizes certain records of a corporation to be maintained by means of any information storage device, method, or electronic network or database, including a distributed electronic network or database, under certain circumstances; requires a corporation to convert a record maintained in a certain manner into a clearly legible written form on the request of any person entitled to inspect the records; authorizes certain communications, consents, and requests to be made by means of a certain electronic transmission; etc.
Massachusetts	<a href="#">HB 3763</a>	Notwithstanding any general or special law to the contrary, the state secretary shall, pursuant to this act, establish a pilot program to provide for convenient voting for military personnel, their families and civilians stationed or working abroad who are allowed to register and vote under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), P.L. 99-410. The pilot program shall provide for the use of smart phones to improve voter engagement and the convenience and security of voting. The state secretary shall provide for a pilot program for integration with the state voters registration system, by a metrically secure authentication, electronic ballot delivery to smart phones, an intuitive voting experience that requires no voter training, the secure return of voted ballots in the redundant, immutable storage of ballots on a block chain infrastructure and an easy way to tabulate and consolidate the results. The pilot program shall include: (i) independent security evaluation and post-election audits; (ii) block chain infrastructure; (iii) the ability to spoil ballot, whereby a second ballot could be issued to a voter and only the voter's last ballot would be counted; and (iv) automatic preparation of tabulatable ballots that can provide for automatically printed ballots, which can be inserted directly into a ballot tabulating machine. The state secretary shall partner with a company that has demonstrated security and capacity to deliver the requirements of the pilot program.
Massachusetts	<a href="#">SB 200</a>	Establishes a special commission to investigate and study the emerging technologies of blockchain and cryptocurrencies.

State	Bill Number	Bill Summary
Michigan	<a href="#">HB 4103</a>	Chapter XXIVA of the Code (Credit Cards) currently defines financial transaction device as one of several specifically listed cards or an instrument or other means of access to a credit, deposit or proprietary account. This bill adds to this definition the use of cryptocurrency or distributed ledger technology to access an account.
Michigan	<a href="#">HB 4106</a>	Generally, a person is prohibited from falsely making, altering, forging or counterfeiting various specified kinds of records or documents, such as wills or insurance policies, with the intent to injure or defraud another person. This bill adds that this prohibition applies to a person who violates it by altering a record made utilizing distributed ledger technology.
Minnesota	None	
Mississippi	None	
Missouri	<a href="#">HB 1109</a>	This bill relates to certificate tokens, which are defined as a representation of shares that are stored in an electronic format and contains information entered into a blockchain or other secure, auditable database, linked to or associated with the certificate token, and able to be transmitted electronically to the issuing corporation, the person to whom the certificate token was issued, and any transferee. The bill requires each certificate to state on its face the name of the person to whom it is issued. Each certificate token must state the data address to which the token was issued. This bill allows the articles of incorporation or bylaws of a corporation to specify that all or a portion of the shares of the corporation may be represented by share certificates in the form of certificate tokens. The electronic message, command or transaction that transmits the certificate tokens to the data address to which a certificate token was issued shall be authorized at the time of issuance by the network signatures of two officers. For the purposes of Chapter 351, RSMo, regarding General and Business Corporations, any reference to share certificate, share, stock or share of stock shall be construed to include a certificate token. Any reference to a requirement to print information on a share certificate shall be construed to be satisfied if the information satisfies the requirements under this bill. Any reference to certificated shares or words of similar import shall be construed to include shares represented by certificate tokens, and any reference to the delivery or deposit of these shares to the corporation shall be construed to refer to any method of granting control of the tokens to the corporation. Any reference to a certificate being duly endorsed shall be construed to mean that the transaction authorizing transfer of control of the certificate token was signed by the lawful

State	Bill Number	Bill Summary
		holder of the token with the network signature corresponding to the lawful holder's data address.
Montana	None	
Nebraska	<a href="#">LB 9</a>	Prohibits cities, counties and villages from taxing or regulating distributed ledger technology.
Nebraska	<a href="#">LR 164</a>	The purpose of this interim study is to examine the need to update the insurance laws of Nebraska in response to technology advancement and innovation, also known as insurtech, in the insurance industry. The interim study shall include, but not be limited to, a review of the interaction of insurance regulation and artificial intelligence, blockchain, autonomous vehicles, and the Internet of things. In order to carry out the purposes of this interim study, the committee should seek the assistance of the Department of Insurance and should consider the input of interested parties, as the committee deems necessary and appropriate.
Nevada	<a href="#">AB 533</a>	Revises provisions relating to cannabis. Creates the Cannabis Advisory Commission to, among others, study the feasibility of the use of emerging technologies, including, without limitation, blockchain and systems that use a single source of truth, as a means of collecting data or efficiently and effectively handling transactions electronically to reduce or eliminate the handling of cash.
Nevada	<a href="#">SB 162</a>	Relates to electronic transactions; includes a public blockchain as a type of electronic record for the purposes of the Uniform Electronic Transactions Act; provides that a person who uses a public blockchain to secure information does not relinquish any right of ownership related to that information; requires a governmental agency to accept a certified copy of a record in electronic form under certain circumstances; authorizes the secretary of state to adopt regulations specifying attributes required for a certified copy of a record in electronic form; prohibits a local government from taxing or imposing restrictions upon the use of a public blockchain; and provides other matters properly relating thereto.
Nevada	<a href="#">SB 163</a>	Relates to business entities; revises the definition of "electronic transmission" as it relates to certain communications of certain business entities to include the use of a blockchain or public blockchain; authorizes certain business entities to store certain records on a blockchain or public blockchain; revises provisions authorizing the secretary of state to adopt regulations to define certain terms to allow certain business entities to carry out their powers and duties

State	Bill Number	Bill Summary
		using the most recent technology available to include the use of blockchains or public blockchains; and provides other matters properly relating thereto.
Nevada	<a href="#">SB 488</a>	Relates to technology; creates the Emerging Technologies Task Force within the Department of Business and Industry; prescribes the membership of the Task Force; sets forth the powers and duties of the Task Force; authorizes the director of the Department of Business and Industry to create an Opportunity Center for Emerging Technology Businesses as part of the Office of Business Finance and Planning; and provides other matters properly relating thereto.
New Hampshire	None	
New Jersey	<a href="#">SB 2297</a>	Establishes New Jersey Blockchain Initiative Task Force.
<i>Signed by Governor 8/8/19, P.L.2019, c.213</i>		
New Jersey	<a href="#">AB 3768</a> <a href="#">SB 2462</a>	Permits corporations to use blockchain technology for certain recordkeeping requirements.
New Jersey	<a href="#">AB 5240</a>	This bill requires the state of New Jersey to review and approve a viable blockchain-based, digital payment platform to provide payment services to legal and licensed businesses in this state that do not have access to traditional financial services and are forced to operate in cash-only or cash-heavy environments. The purpose of the payment platform is to provide a safe, secure, and compliant system that does not exclude these businesses from participating in digital commerce. The bill requires the payment platform to provide businesses with access to cashless transactions and to secure revenue on a one-to-one basis of virtual currency to U.S. dollars. A business shall only have access to the payment platform with approval from the state. The payment platform shall provide the ability to manage and process all business expenditures and allow all transactions to be recorded on an immutable blockchain ledger. The payment platform shall facilitate regulatory compliance, provide for audits by the state, and allow for payment of sales tax to local municipalities.
New Mexico	None	
New York	<a href="#">AB 1351</a> <a href="#">SB 6036</a>	Directs the state board of elections to study and evaluate the use of blockchain technology to protect voter records and election results.

State	Bill Number	Bill Summary
	<i>Passed Senate 6/18/19</i>	
New York	<a href="#"><u>AB 1371</u></a>	Relates to establishing a task force to study and report on the potential implementation of blockchain technology in state record keeping, information storage and service delivery.
New York	<a href="#"><u>AB 1398</u></a> <a href="#"><u>SB 6037</u></a> <i>Passed Senate 6/17/19</i>	Relates to the development and creation of distributed ledger technology, which is a mathematically secured, chronological, and decentralized consensus ledger or database, whether maintained via internet interaction, peer-to-peer network, or otherwise used to authenticate, record, share and synchronize transactions in their respective electronic ledgers or databases, and business entities that develop distributed ledger technology.
New York	<a href="#"><u>AB 1683</u></a> <a href="#"><u>SB 4142</u></a> <i>Passed Senate 4/9/19</i>	Relates to allowing signatures, records and contracts secured through blockchain technology to be considered in an electronic form and to be an electronic record and signature; allows smart contracts to exist in commerce.
New York	<a href="#"><u>AB 2239</u></a> <a href="#"><u>SB 5060</u></a>	Establishes the office of financial resilience to develop and implement new programs and initiatives for the purpose of supporting local economies and promoting resilient financial models.
North Carolina	None	
North Dakota	<a href="#"><u>HB 1043</u></a> <i>Failed to pass House 1/11/19</i>	Relates to the exemption of an open blockchain token from specified securities transactions and dealings; relates to the definitions of an open blockchain token and virtual currency and excluding an open blockchain token and virtual currency from specified money transmission requirements.
North Dakota	<a href="#"><u>HB 1045</u></a> <i>Signed by governor 4/24/19, Chapter 94</i>	Relates to electronic transaction definitions, blockchain technology and smart contracts, number of shareholders and series limited liability companies; relates to electronic transactions, filing of an annual report by corporations engaged in farming or ranching, Business Corporation Act definitions, knowledge and notice, share certificates, corporate voting list and voting trusts.
North Dakota	<a href="#"><u>HB 1048</u></a> <i>Signed by governor 3/20/19, Chapter 469</i>	Relates to the use of distributed ledger technologies; requires the Department of Information Technologies to research and develop the use of distributed ledger enabled platform technologies, such as blockchains, for computer-controlled programs, data transfer and storage, and program regulation to protect against falsification, improve internal data security, and identify external hacking threats.

State	Bill Number	Bill Summary
North Dakota	<a href="#">HB 1049</a> <i>Failed to pass House 1/9/19</i>	Relates to signatures secured through distributed ledger technology.
North Dakota	<a href="#">HCR. 3002</a> <i>Failed to pass House 2/8/19</i>	Requests the legislative management to study the potential benefits of distributed ledger technology and blockchain for state government.
North Dakota	<a href="#">HCR 3004</a> <i>Adopted 3/28/19, Chapter 539</i>	Requests the legislative management to study the potential benefit value of blockchain technology implementation and utilization in state government administration and affairs.
N. Mariana Islands	Not available	
Ohio	<a href="#">HB 220</a>	Enacts §9.16 of the Revised Code to allow a governmental entity to utilize distributed ledger technology, including blockchain technology.
Oklahoma	<a href="#">SB 700</a> <i>Signed by governor 4/25/19, Chapter 177</i>	Relates to electronic records; relates to the Uniform Electronics Transactions Act; modifies certain definitions.
Oklahoma	<a href="#">SB 847</a>	Relates to corporations; defines terms; clarifies number of shareholders in corporation records; requires certain written statement upon certain transfers; requires corporations to prepare certain list for notice; provides contents of list; states effect of certain shareholder information; states effect of certain shareholder information when certain information does not correspond; provides certain method of determination; authorizes the formation of a voting trust; provides method of formation.
Oregon	<a href="#">HB 2179</a>	Establishes the Task Force on Blockchain Applications and Legislation. Directs the task force to study and evaluate status and development of blockchain technology, investigate potential uses for blockchain technology for economic development and business transactions and make recommendations for any changes necessary in state statutes that can promote adopting, using and developing blockchain technologies.
Oregon	<a href="#">HB 2487</a>	Directs the Oregon Department of Administrative Services to study and make recommendations regarding the use of blockchain technology by state agencies to administer public services. Requires the department to submit report on findings by Jan. 1, 2021.

State	Bill Number	Bill Summary
Pennsylvania	None	
Puerto Rico	None	
Rhode Island	<a href="#">HB 5683</a>	Enables the use of electronic networks and databases for corporate records.
South Carolina	<a href="#">SB 4351</a>	Enacts the South Carolina Blockchain Industry Empowerment Act of 2019 in order to establish this state as an incubator for tech industries seeking to develop innovation by using blockchain technology; adds §33-6-245 so as to further provide for the construction of terms relating to stock and certificate tokens; amends §33-6-250, relating to the form and content of corporate stock certificates, so as to authorize corporations to issue certificate tokens in lieu of stock certificates; adds chapter 47 to title 34 so as to provide that a person who develops, sells or facilitates the exchange of an open blockchain token is not subject to specified securities and money transmission laws, and to provide specified verification authority to the secretary of state and banking commissioner. Adds chapter 49 to title 34 so as to create the financial technology sandbox for the testing of financial products and services in South Carolina; authorizes limited waivers of specified provisions of law under certain conditions; establishes standards and procedures for sandbox applications, operations and supervision; authorizes reciprocity agreements with other regulators; requires criminal history background checks; requires the creation of financial technology innovation accounts to be used for special purposes; requires a consumer protection bond; and specifies standards for the suspension and revocation of a sandbox authorization. Adds chapter 51 to title 34 so as to specify that digital assets are property within the uniform commercial code, authorizes security interests in digital assets, establishes an opt-in framework for banks to provide custodial services for digital asset property as custodians, specifies standards and procedures for custodial services, clarifies the jurisdiction of South Carolina courts relating to digital assets, authorizes a supervision fee, and provides for other related provisions to digital assets; amends §35-11-105, relating to definitions under the South Carolina anti-money laundering act, so as to define the term "virtual currency"; and amends §35-11-110, relating to matters and transactions to which the anti-money laundering act does not apply, so as to provide that the act does not apply to buying, selling, issuing, or taking custody of payment instruments or stored value in the form of virtual currency or receiving virtual currency for transmission to a location within or outside the united states by any means.
South Carolina	<a href="#">SB 738</a>	Enacts the "South Carolina Blockchain Industry Empowerment Act of 2019", to establish this state as an incubator for technology industries

State	Bill Number	Bill Summary
		<p>seeking to develop innovation by using blockchain technology; amends article 2, chapter 6, title 33 of the 1976 code, relating to the issuance of shares for corporations, partnerships, and associations, by adding §33-6-245, to provide for the construction of terms relating to stock and certificate tokens; amends §33-6-250 of the 1976 code, relating to the form and content of corporate stock certificates, to authorize corporations to issue certificate tokens in lieu of stock certificates; amends title 34 of the 1976 code, relating to banking, financial institutions, and money, by adding chapter 47, to provide that a person who develops, sells, or facilitates the exchange of an open blockchain token is not subject to specified securities and money transmission laws, and to provide specified verification authority to the secretary of state and banking commissioner; amends title 34 of the 1976 code, relating to banking, financial institutions, and money, by adding chapter 49, to create the financial technology sandbox for the testing of financial products and services in South Carolina, to authorize limited waivers of specified provisions of law under certain conditions, to establish standards and procedures for sandbox applications, operations, and supervision, to authorize reciprocity agreements with other regulators, to require criminal history background checks, to require the creation of financial technology innovation accounts to be used for special purposes, to require a consumer protection bond, and to specify standards for the suspension and revocation of a sandbox authorization; amends title 34 of the 1976 code, relating to banking, financial institutions, and money, by adding chapter 51, to specify that digital assets are property within the uniform commercial code, to authorize security interests in digital assets, to establish an opt-in framework for banks to provide custodial services for digital asset property as custodians, to specify standards and procedures for custodial services, to clarify the jurisdiction of South Carolina courts relating to digital assets, to authorize a supervision fee, and to provide for other related provisions for digital assets; amends §35-11-110 of the 1976 code, relating to the applicability of the anti-money laundering act, to provide that the anti-money laundering act does not apply to the buying, selling, issuing, or taking custody of payment instruments or stored value in the form of virtual currency or receiving virtual currency for transmission to a location within or outside the United States by any means; and to define necessary terms.</p>
South Dakota	<a href="#">HB 1196</a>	<p>Provides a definition of blockchain technology for certain purposes.</p> <p><i>Signed by governor 3/7/19, Chapter 207</i></p>
Tennessee	None	

State	Bill Number	Bill Summary
Texas	<a href="#">HB 3608</a>	Relates to business entities; includes a distributed electronic network or database employing blockchain or distributed ledger technology in definitions.
Texas	<a href="#">HB 4214</a>	Creates programs and requirements for state agencies and local governments to assess cybersecurity risks. Requires each state agency and local government would be required to consider using next-generation technologies, including cryptocurrency, blockchain technology, and artificial intelligence.
Texas	<a href="#">HB 4517</a>	Establishes the Texas blockchain working group.
Utah	<a href="#">HJR 19</a>	This resolution directs a legislative study of blockchain technology. This resolution: recognizes the potential benefits and applications of blockchain technology; and directs the Business and Labor Interim Committee to study and make legislative recommendations regarding the potential benefits and value of blockchain technology, including potential uses in state government.
Utah	<a href="#">SB 213</a>	This bill enacts provisions related to blockchain technology. This bill: defines and clarifies terms related to blockchain technology; exempts a person who facilitates the creation, exchange, or sale of certain blockchain technology-related products from Title 7, Chapter 25, Money Transmitter Act; and makes technical changes.
Vermont	None	
Virginia	<a href="#">HB 1900</a>	Establishes the Health Care Provider Credentials Data Solution Fund for the purpose of soliciting proofs of concept to establish or improve a system for the storage and accessing of health care provider credentials data, utilizing blockchain or a similar technology, to be maintained by the Department of Health Professions. The Fund authorizes the secretary of Health to disburse matching funds on at least a one-to-one basis to any person who demonstrates such proof of concept.
Virginia	<a href="#">HB 2415</a>	Creates a rebuttable presumption that a business record electronically registered on a blockchain is a self-authenticating document for certain facts. The bill provides that such presumption does not extend to the truthfulness, validity, or legal status of the contents of the fact or record.
Virginia	<a href="#">HB 2588</a>	Directs the commissioner of elections to establish and supervise a pilot program by which an active duty member of a uniformed service who has been deployed overseas and is a registered voter of a county or city

State	Bill Number	Bill Summary
		<p>participating in such pilot program may return his voted military-overseas ballot by electronic means. The commissioner is required to promulgate standards and develop procedures for the secure transmission and return, storage, and processing of voted military-overseas ballots, including security measures, methods for verifying and authenticating a voter's identity, and encryption methods for the voted ballots. To the fullest extent practicable, these standards and procedures are required to incorporate the use of blockchain technology, defined in the bill as technology using distributed databases and ledgers protected against revision by publicly verifiable open-source cryptographic algorithms and protected from data loss by distributed records sharing. The bill requires counties and cities participating in the pilot program to participate in a security review after each election. In each year of the pilot program, the bill requires the commissioner to conduct a security assessment and update the security measures for the pilot program. The bill also requires that voters eligible to return their military-overseas ballots by electronic means through the pilot program be permitted to sign the statement of voter and any other documents related to absentee voting using the digital signature associated with their respective Common Access Cards issued by the U.S. Department of Defense. The pilot program is in effect for elections held on and after Jan. 1, 2020. The bill requires the commissioner to submit a report on or before Dec. 1, 2024, on the outcomes of the pilot program and to include a recommendation as to whether to implement the electronic return of voted military-overseas ballots on a permanent, statewide basis. The bill has an expiration date of Dec. 31, 2024.</p>
Virginia	<a href="#"><u>HJR. 677</u></a> <i>To Conference Committee</i> 2/21/19	<p>Establishes a 21-member joint subcommittee to identify blockchain technology research and economic development opportunities with the goal of creating a statewide, comprehensive and coordinated strategy relating to blockchain technology. In conducting its study, the joint subcommittee shall analyze and consider (i) economic development opportunities in the commonwealth available through the utilization of blockchain technology; (ii) different types of blockchain technology and the feasibility of economic development for each type; (iii) the creation of a statewide, comprehensive, coordinated strategy to encourage commercial activity in the blockchain technology sector; (iv) opportunities for deployment of blockchain technology in state government; and (v) strategies to incentivize the development of blockchain companies in the commonwealth. The joint subcommittee shall submit its report to the governor and the 2020 and 2021 regular sessions of the General Assembly.</p>

State	Bill Number	Bill Summary
U.S. Virgin Islands	Not available	
Washington	<a href="#"><u>SB 5638</u></a> <i>Signed by governor</i> <i>4/26/19, Chapter 153</i>	Provides that an electronic record may not be denied legal effect or enforceability solely because it is generated or stored using distributed ledger technology.
West Virginia	None	
Wisconsin	None	
Wyoming	<a href="#"><u>HB 1</u></a> <i>Signed by governor with line item vetoes</i> <i>2/26/19, Chapter 80</i>	Changes the membership of the Blockchain Task Force.
Wyoming	<a href="#"><u>HB 70</u></a> <i>Signed by Governor</i> <i>2/26/19, Chapter 94</i>	Relates to the secretary of state; authorizes the secretary of state to develop and implement a blockchain commercial filing system; authorizes a report; makes an appropriation.
Wyoming	<a href="#"><u>HB 62</u></a> <i>Signed by Governor</i> <i>2/28/19, Chapter 170</i>	The legislature took up multiple measures in 2019 to encourage development of blockchain technology for business purposes in the state. House Bill 62 adopted the Wyoming Utility Token Act.
Wyoming	<a href="#"><u>HB 74</u></a> <i>Signed by governor</i> <i>2/26/19, Chapter 92</i>	Relates to banking; makes legislative findings; creates special purpose depository banks as a new financial institution; provides that special purpose depository banks shall be corporations; requires that depositors be business entities; specifies compliance with applicable federal laws; establishes procedures for the incorporation, chartering and operation of special purpose depository bank.
Wyoming	<a href="#"><u>HB 185</u></a> <i>Signed by governor</i> <i>2/26/19, Chapter 93</i>	Relates to corporate shares and distributions; authorizes corporations to issue certificate tokens in lieu of stock certificates as specified; makes conforming amendments.

*Heather Morton is a program principal in Fiscal Affairs. She covers financial services, alcohol production and sales, telecommunications and medical malpractice issues for NCSL.*

# Cybersecurity Legislation 2019

9/16/2019

State legislatures continue to advance policy proposals to address cyber threats directed at governments and private businesses. As threats continue to evolve and expand and as the pace of new technologies accelerates, legislatures are making cybersecurity measures a higher priority.

**2019 Introductions:** At least 43 states and Puerto Rico introduced or considered close to 300 bills or resolutions that deal significantly with cybersecurity. Thirty-one states enacted cybersecurity-related legislation in 2019 (the status of enacted bills are highlighted in bold). Some of the key areas of legislative activity include:

- Requiring government agencies or businesses to implement training or specific types of security policies and practices
- Creating task forces or commissions
- restructuring government for improved security
- studying the use of blockchain for cybersecurity
- providing for the security of utilities and critical infrastructure
- exempting cybersecurity operations information from public records laws
- addressing the security of connected devices
- regulating cybersecurity within the insurance industry
- Providing funding for improved security measures (note: this page does not list all cybersecurity appropriations bills; rather, it focuses on those that include specific mandates or projects to be funded)
- addressing cybersecurity threats to elections (see NCSL's Elections data base for other types of [elections security](#)-related legislation).

See additional [resources](#) for information on related topics such as security breach legislation, privacy and other issues.

NOTE: Please check individual legislative websites for the most current status, summaries and versions of bill text.

## 2019 Cybersecurity Legislation

### Alabama

AL H 101

Status: Failed-adjourned

Relates to insurance; requires insurers and other entities licensed by the Department of Insurance to develop, implement, and maintain an information security program; provides for reporting to the Commissioner of Insurance, including the reporting of cybersecurity events; provides that information provided to the commissioner pursuant to this act would be confidential and privileged under certain conditions; provides for civil penalties under certain conditions.

**AL S 54**

**Status: Enacted, Chap. 98**

Relates to insurance; requires insurers and other entities licensed by the Department of Insurance to develop, implement, and maintain an information security program; provides for reporting to the Commissioner of

Insurance, including the reporting of cybersecurity events; provides that information provided to the commissioner pursuant to this act would be confidential and privileged under certain conditions; provides for civil penalties under certain conditions.

AL S 109

Status: Failed

Relates to elections; provides that tampering with, hacking, or otherwise manipulating an electronic voting machine or misusing a voting machine is a Class B felony; makes certain enumerated actions relating to voter fraud, whereby a voter takes an unlawful action when voting by absentee ballot, a Class A misdemeanor.

## Arkansas

**AR H 1128**

**Status: Enacted, Act 149**

Amends the law concerning the authority of the Governor to order the militia into service, authorizes the use of the militia to address cybersecurity threats and cybersecurity vulnerabilities.

**AR H 1500**

**Status: Enacted, Act 599**

Provides for the security of the plans of emergency service agencies, prevents, investigates, or responds to incidents of terrorism and mass destruction, provides for the security of investigative files and documents, amends the Homeland Security Information Act.

**AR S 632**

**Status: Enacted, Act 1085**

Enacts the Cyber Initiative Act, authorizes the Economic Development Commission to support a cyber alliance in order to reduce cyber risks and encourage economic development.

## Arizona

**AZ H 2177**

**Status: Enacted, Chap. 45**

Revises provisions relating to the Regulatory Sandbox Program, revises certain definitions, relates to temporary testing of an innovation without otherwise being licensed, revises provisions relating to the application process and requirements, provides for financial products and services, requires the employment of cybersecurity measures to avoid breaches.

**AZ H 2489**

Status: Failed - Adjourned

Relates to election procedures oversight committee.

**AZ S 1470**

Status: Failed - Adjourned

Relates to automatic voter registration, relates to database, relates to agencies.

## California

**CA A 74**

**Status: Enacted, Chap. 23**

Makes appropriations for the support of state government for the upcoming fiscal year, including appropriating funds to establish and operate the office of elections cybersecurity. Provides that activities performed by the

office shall be designed so as to minimize overlap and in coordination with statewide cybersecurity efforts performed by the California Cybersecurity Integration Center.

#### CA A 190

Status: Pending

Makes appropriations for the support of state government for the 2019-20 fiscal year, including appropriating funds to establish and operate the office of elections cybersecurity. Provides that activities performed by the office shall be designed so as to minimize overlap and in coordination with statewide cybersecurity efforts performed by the California Cybersecurity Integration Center.

#### CA A 814

**Status: Enacted, Chap. 16**

Clarifies that, for purposes of the prohibition against unlawfully accessing a computer system, a computer system includes devices or systems that are located within, connected to, or integrated with, a motor vehicle.

#### CA A 1043

**Status: Enacted, Chap. 46**

Authorizes the expenditure of campaign funds to pay for, or reimburse the state for, the installation and monitoring of hardware, software, and services related to the cybersecurity of the electronic devices of a candidate, elected officer, or campaign worker. Requires a candidate or elected officer to report any expenditure of campaign funds for these purposes to the Fair Political Practices Commission in the candidate or officer's campaign statements.

#### CA A 1044

**Status: Enacted, Chap. 106**

Authorizes the Secretary of State to require an applicant to take a training course regarding data security as a condition for the receipt of voter registration information if that course is made available to the applicant at no cost to the applicant. Clarifies that required reports by elections officers may include information about the identity of, and contact information for, the elections official who is responsible for conducting elections in the jurisdiction.

#### CA A 1242

Status: Pending

Requires each state agency to submit a summary of actual and project costs, information security costs, and to comply with the policies and procedures issued by the Office of Information Security. Defines state agency for these purposes to mean every state office, officer, department, division, bureau, board, and commission, except for the California State University.

#### CA A 1376

Status: Pending

Requires the Department of Veterans Affairs to collaborate with specified state agencies to establish a veterans' preference to be applied to employment opportunities within the field of cybersecurity that require a security clearance.

#### CA A 1469

Status: Pending

Requires the Bureau of Household Goods and Services, in consultation with stake holders, to conduct a review of its accepted trade standards for good and workmanlike repair to determine whether additional regulations need to be adopted concerning privacy and security implications of connected devices.

#### CA A 1566

Status: Pending

Establishes the California Cyber Range Pilot Project, under the administration of the California Cybersecurity Institute, to test the overall feasibility of the pilot project through a yearlong, multiphased effort. Requires the

pilot project to produce a scalable model for a permanent California Cyber Range Program.

#### CA S 73

Status: Pending

Makes appropriations for the support of state government for the upcoming fiscal year, including appropriating funds to establish and operate the office of elections cybersecurity. Provides that activities performed by the office shall be designed so as to minimize overlap and in coordination with statewide cybersecurity efforts performed by the California Cybersecurity Integration Center.

#### CA S 239

Status: Pending

Requires the prosecution for a felony violation of crimes relating to computer services and systems, as specified, to be commenced within three years after discovery of the commission of the offense, or within three years after the completion of the offense, whichever date is later.

#### CA SR 54

Status: Adopted

Proclaims the month of October 2019, and every October thereafter, to be National Cybersecurity Awareness Month in the state.

## Connecticut

#### CT H 5417

Status: Failed - Adjourned

Establishes a task force to study the use of blockchain technology to manage elector information.

#### CT H 5989

Status: Failed

Offers protection to certain business data holders in the event of a data breach.

#### CT H 7321

Status: Failed - Adjourned

Requires the Secretary of the State to appoint an individual to serve in the office of the Secretary of the State in a cyber security role, limits, in certain situations, the type of information provided when voter registration records are provided, requires that each voting tabulator has a certain number of memory cards programmed for use with such tabulator, provides for security analysis of such memory cards by the University of State.

#### CT H 7424

**Status: Enacted, Chap. 117**

Concerns the state budget for the upcoming biennium, makes appropriations therefor, implements provisions of the budget. Enacts the "Insurance Data Security Law."

#### CT S 709

Status: Failed - Adjourned

Creates a division of cyber security within the Department of Emergency Services and Public Protection.

#### CT S 811

Status: Failed - Adjourned

Increases penalties for computer crimes against financial institutions and their customers.

#### CT S 903

Status: Failed - Adjourned

Revises the standards governing insurance data and information security, notices following cybersecurity events, and investigations of cybersecurity events.

## **Delaware**

### **DE H 174**

#### **Status: Enacted, Chap. 176**

Enacts the Insurance Data Security Act. Establishes standards for data security for Title 18 licensees and standards for the investigation of and notification to the Commissioner of a cybersecurity event affecting Title 18 licensees.

### **DE S 153**

#### **Status: Enacted, Chap. 185**

Relates to information technology ("IT") recommendations of the Government Efficiency and Accountability Review ("GEAR") Board established by Governor Carney's Executive Order Four; modernizes Chapter 90C of Title 29 of the Delaware Code and authorizes the establishment of a shared it services model for state agencies. Sets forth state information security requirements.

## **Florida**

### **FL H 327**

#### **Status: Enacted, Chap. 2019-37**

Relates to public meetings, exempts from public meetings requirements certain exempt information concerning information technology systems held by specified utilities, provides for future legislative review and repeal of the exemption, provides a statement of public necessity.

### **FL H 735**

#### **Status: Failed**

Relates to blockchain technology, establishes the Blockchain Working Group in the Department of Management Services, provides for membership and duties of the Working Group, requires the Working Group to submit a report to the Governor and the Legislature and make presentations, requires the Department to provide support staff and other assistance.

### **FL H 1393**

#### **Status: Enacted, Chap. 140**

Establishes a Florida Blockchain Task Force to study the ways in which state, county, and municipal governments can benefit from a transition to a blockchain-based system for recordkeeping, security, and service delivery. Provides that the Task Force will develop and submit recommendations concerning the potential for blockchain-based systems to promote government efficiencies, better services for citizens, economic development, and safer cyber-secure interaction between government and the public.

### **FL H 2249**

#### **Status: Failed**

Relates to the appropriations project titled Volusia County Schools Cyber Security Program, provides an appropriation.

### **FL H 2383**

#### **Status: Failed**

Relates to the Appropriations Project titled Saint Petersburg College - Public Safety and Cybersecurity, provides an appropriation.

### **FL H 3147**

Status: Failed

Relates to the Appropriations Project titled University of West State Cybersecurity Support, provides an appropriation.

#### FL H 5001

**Status: Enacted, Chap. 115**

Makes appropriations, including funds to county supervisors of elections for cybersecurity initiatives.

#### FL H 5301

**Status: Enacted, Chap. 32**

Relates to information technology reorganization. Requires a state chief information security officer, who must have experience and expertise in security and risk management for communications and information technology resources, be designated..Creates the Florida Cybersecurity Task Force.

#### FL H 7047

**Status: Enacted, 2019-32**

Relates to a review under the Open Government Sunset Review Act, provides a public records exemption for information received by the Department of Legal Affairs pursuant to a notification of a security breach or during the course of an investigation of such breach, removes the scheduled repeal of the exemption.

#### FL PCB 6047

Status: Failed-adjourned

Relates to a review under the Open Government Sunset Review Act; amending s. 501.171, F.S., which provides a public records exemption for information received by the Department of Legal Affairs pursuant to a notification of a security breach or during the course of an investigation of such breach; removing the scheduled repeal of the exemption.

#### FL PCB 6089

Status: Failed - adjourned

Relates to information technology reorganization, transfers all powers, duties, functions, records, offices, personnel, associated administrative support positions, property, Status: Pending issues and existing contracts, administrative authority, certain administrative rules, trust funds and unexpended balances of appropriations, allocations, and other funds of the Agency for State Technology to the Department of Management Services by a type two transfer.

#### FL S 450

Status: Failed

Relates to public meetings, provides an exemption from public meeting requirements for portions of a meeting at which certain exempt records related to the security of the technology, processes, or practices of certain utilities and the security of existing or proposed information technology systems or industrial control systems of certain utilities are discussed or may otherwise be revealed, provides for future legislative review and repeal of the exemption.

#### FL S 1024

**Status: Enacted, Chap. 52**

Establishes the State Blockchain Task Force to explore and develop a master plan for fostering the expansion of the blockchain industry in the state, to recommend policies and state investments to help make this state a leader in blockchain technology, and to issue a report, requires the study to include if and how state, county, and municipal governments can benefit from a transition to a blockchain based system for recordkeeping, data security, financial transactions, and service delivery.

#### FL S 1570

Status: Failed

Relates to information technology reorganization.

## FL S 2500

### **Status: Enacted, Chap. 115**

Makes appropriations, including funds to county supervisors of elections for cybersecurity initiatives.

## FL S 7008

### Status: Failed

Relates to a review under the Open Government Sunset Review Act, which provides a public records exemption for information received by the Department of Legal Affairs pursuant to a notification of a security breach or during the course of an investigation of such breach, removes the scheduled repeal of the exemption.

## FL SPB 7008

### Status: Failed-adjourned

Provides a public records exemption for information received by the Department of Legal Affairs pursuant to a notification of a security breach or during the course of an investigation of such breach.

## Georgia

### GA H 30

### **Status: Enacted, Chap. 3**

Appropriates funds to the Georgia Cyber Innovation and Training Center to enhance cybersecurity technology for private and public industries through unique education, training, research, and practical applications.

### GA H 31

### **Status: Enacted, Chap. 3**

Appropriates funds for cybersecurity training and cybersedurity initiatives in schools.

## GA H 641

### Status: Pending - Carryover

Relates to general provisions regarding the Georgia Bureau of Investigation, so as to grant the Georgia Bureau of Investigation Powers and duties to identify and investigate violations of Article 6 of Chapter 9 of Title 16 of the Official Code of Georgia Annotated, the Georgia Computer Systems Protection Act, and other computer crimes, provides for subpoena power by the bureau for such investigations, provides for related matters, repeals conflicting laws.

## GA S 21

### Status: Pending - Carryover

Relates to competencies and core curriculum, requires each local board of education to prescribe mandatory instruction concerning cybersecurity in every year in every grade from kindergarten through grade 12, provides for a definition, requires the State Board of Education to prescribe a minimum course of study in cybersecurity, provides for duties of the State School Superintendent.

### GA SR 228

### **Status: Adopted**

Recognizes 2019 as Cybersecurity Career Awareness Year in Georgia.

## GA E.O. 182

Reconstitutes the Government Systems Cybersecurity Review Board. All Executive Branch agencies shall ensure that employees complete at least one form of cybersecurity training within ninety (90) days of this Executive Order. An employee's failure to comply with this Order shall result in formal disciplinary action, up to and including termination.

## Hawaii

HI H 1553

Status: Pending--Carryover

Establishes the Hawaii State Fusion Center to, among other things, Integrate information technology, cybersecurity, and cybercrime prevention, and cyber and analytic capabilities, and improve situational awareness related to critical infrastructure or key resources protection of lifelines.

## Iowa

IA D 1175

Status: Pending - Carryover

Relates to Secretary of State, elections technical bill.

IA H 39

Status: Pending - Carryover

Relates to student data collection by the Department of Education, school districts, and accredited nonpublic schools.

**IA H 692**

**Status: Enacted**

Relates to the conduct of state and local elections, providing penalties, and including effective date elections provisions, provides for penalties for using voter registration information, including resale or redistribution of the voter registration list without written permission of the state registrar, for purposes other than those permitted.

IA HSB 49

Status: Pending - Carryover

Relates to the administration of elections, provides penalties, includes effective date provisions.

IA S 204

Status: Pending - Carryover

Provides for an affirmative defense to certain claims relating to personal information security breach protection.

IA S 575

Status: Pending - Carryover

Relates to the conduct of state and local elections, provides penalties, includes effective date provisions.

IA SSB 1078

Status: Pending - Carryover

Relates to the administration of elections.

IA SSB 1241

Status: Pending - Carryover

Relates to the conduct of state and local elections, provides penalties.

## Illinois

IL H 2829

Status: Pending

Creates the Financial Institution Cybersecurity Act, provides that persons and entities operating under the authority of the Secretary of Financial and Professional Regulation under the Banking Act, the

Insurance Code, the Savings Bank Act, the Credit Union Act, the Corporate Fiduciary Act, and the Residential Mortgage License Act must maintain a cybersecurity program to protect the confidentiality of their information system.

#### IL H 3017

Status: Pending

Creates the Veterans Cyber Academy Pilot Program Act, provides that the Department of Veterans' Affairs shall establish and implement a pilot program to provide veterans residing in the state with access to cyber security training, certification, apprenticeships, and additional resources to enter the cyber security field of work, provides that the pilot program shall run from January 1, 2021 to December 31, 2023, provides specified requirements to the department in implementing the pilot program.

#### IL H 3391

Status: Pending

Creates the Security of Connected Devices Act, requires manufacturers of connected devices to equip the device with security features that are designed to protect the device and any information the device contains from unauthorized access, destruction, use, modification, or disclosure.

#### IL HJR 1

Status: Pending

Extends the sunset date of the operation of the Cybersecurity Task Force, reconstitutes the focus and membership of the Task Force.

#### IL HJR 2

Status: Pending

Creates the Return Illinois To Prosperity Commission to review and evaluate the creation of a State Bank, provides that the mission of a State Bank would include supporting economic development by increasing access to capital for agriculture, businesses, and industry and providing stability to the local financial sector.

#### IL S 240

Status: Pending

Creates the Consumer Credit Reporting Agency Registration and Cybersecurity Program Act, provides for requirements for consumer credit reporting agency registration, contains provisions regarding grounds for revocation and suspension of a registration, provides that by a certain date, a consumer credit reporting agency must have a cybersecurity program documented in writing and designed to protect the confidentiality, integrity and availability of its information systems.

#### IL S 1622

Status: Pending

Amends the Election Code, provides that no voting machine used or purchased by an election authority may be made, manufactured, or assembled outside the United States or constructed with parts made, manufactured, or assembled outside the United States, including, but not limited to, any hardware or software, provides that, in provisions concerning voting machines, precinct tabulation optical scan technology voting systems, and direct recording electronic voting systems,.

#### IL S 1719

Status: Pending

Creates the Keep Internet Devices Safe Act, provides that a digital device is an internet connected device that contains a microphone, provides that no private entity may turn on or enable a digital device's microphone unless the registered owner or person configuring the device is provided certain notices in a consumer agreement, provides that a manufacturer of a digital device that does not cause to be turned on or otherwise use a digital device's microphone is not subject to the restrictions on its

use.

## IL S 1863

**Status: Pending**

Amends the Freedom of Information Act, exempts from disclosure risk and vulnerability assessments, security measures, schedules, certifications, and response policies or plans that are designed to detect, defend against, prevent, or respond to potential cyber attacks upon the State's or an election authority's network systems, or records that the disclosure of which would, in any way, constitute a risk to the proper administration of elections or voter registration.

## Indiana

### IN S 4

**Status: Enacted, Public Law 15**

Provides that a permit for the discharge from a wastewater treatment plant may not be issued unless the application contains a cybersecurity plan. Excludes the cybersecurity plan from public access.

### IN S 558

**Status: Enacted, Public Law 157**

Relates to election security, requires the Secretary of State to refer suspected criminal violations of election law for investigation by the appropriate prosecuting attorney, establishes an administrative enforcement mechanism for enforcement of election laws other than campaign finance laws, requires the statewide voter registration file to employ two factor authentication to restrict access.

### IN S 560

**Status: Enacted, Public Law 278**

Relates to various election law matters, removes provisions relating to candidates for President of the United States filing ballot placement requests with the secretary of state, provides that the election division annual training conference for county election officials must include information on cybersecurity and physical security practices for the statewide voter registration system, voting systems, and polling places.

### IN S 570

**Status: Enacted, Public Law 71**

Relates to election cyber security, includes a definition of VSTOP voting system technical oversight program in the election code, requires the secretary of state to establish proficiency standards for individuals who are authorized to access the statewide voter registration file, requires such individuals to meet the proficiency standards in order to access the file, requires the county election board to deliver voting systems and electronic poll books to precincts and vote centers.

## Kansas

### KS H 2209

**Status: Enacted, Chap. 54**

Concerns insurance, relates to life insurance unfair or deceptive acts or practices, third party administrator license and renewal application fees, purchase of cybersecurity insurance, association health plans, and healthcare benefit coverage, establishes the Unclaimed Life Insurance Benefits Act.

## Kentucky

### KY HR 171

**Status: Adopted**

Urges the Kentucky Cabinet for Economic Development to work with state and federal officials and study the issue of blockchain technology.

**KY S 14**

**Status: Failed - Adjourned**

Provides definitions relating to personal information, provides certain personal information that shall be protected from disclosure by a public agency or third party contractor through redaction or other means, provides a list of covered persons, provides guidelines for contracts between a public agency and a third party contractor.

**KY S 195**

**Status: Failed - Adjourned**

Requires a manufacturer of a connected device offered for sale in Kentucky to equip the device with reasonable security features appropriate to the nature and function of the device and to the information it may collect, contain, or transmit, and designed to protect the device from unauthorized access, destruction, use, modification, or disclosure, defines authentication, connected device, manufacturer, and unauthorized access, destruction, use, modification, of disclosure.

## **Louisiana**

**LA H 74**

**Status: Enacted, Chap. 292**

Creates the crime of trespass against state computers, provides for elements of the crime, provides for criminal penalties.

**LA H 325**

**Status: Failed - Adjourned**

Prohibits the registrar of voters, clerk of court, and Department of State from disclosing specified computer system information.

**LA H 442**

**Status: Failed - Adjourned**

Establishes the State Cyber security and Information Technology Infrastructure Fund, dedicates revenues into the fund.

**LA H 448**

**Status: Failed - Adjourned**

Establishes the State Cyber security and Information Technology Infrastructure Fund, dedicates revenues into the fund.

**LA H 511**

**Status: Failed - Adjourned**

Creates the Louisiana Cybersecurity Talent Initiative Fund for the purpose of funding degree and certificate programs in cybersecurity Fields and the Cybersecurity Education Management Council to advise relative to the fund.

**LA HCR 67**

**Status: Adopted**

Requests Louisiana Economic Development to study cybersecurity issues faced by businesses in compliance with the Cybersecurity Framework Standards promulgated by the National Institute of Standards and Technology.

**LA S 46**

**Status: Enacted, Chap. 292**

Authorizes entities to monitor, share, and receive certain information relative to cyber threats, authorizes certain defensive measures, relates to certain security and information controls, provides for confidentiality of certain information.

**LA SCR 123**

**Status: Adopted**

Creates a task force to develop and plan a tabletop exercise that tests and strengthens the infrastructure required to combat cyber threats.

## **Massachusetts**

**MA H 223**

Status: Pending

Relates to the security of personal financial information.

**MA H 287**

Status: Pending

Protects the privacy and security of biometric information.

**MA H 2690**

Status: Pending

Establishes a task force to study the need for increased cyber security within government agencies.

**MA H 2692**

Status: Pending

Relates to cybersecurity standards in state contracts or procurements.

**MA H 2728**

Status: Pending

Provides that state agencies procuring information technology goods or services give preference to vendors that carry cybersecurity insurance.

**MA HD 3239**

Status: Pending

Updates chapter 93H data security protections to include biometric information.

**MA S 315**

Status: Pending

Relates to cyber security education in schools.

**MA S 1822**

Status: Pending

Relates to cybersecurity insurance preference in state contracts.

**MA S 1887**

Status: Pending

Establishes a Cybersecurity Control and Review Commission.

**MA S 2056**

Status: Pending

Relates to the cybersecurity of the internet connected devices and autonomous vehicles.

## Maryland

### MD H 211

Status: Failed - Adjourned

Prohibits a person from committing a certain prohibited act with the intent to interrupt or impair the functioning of a health care facility, prohibits a person from knowingly possessing certain ransomware with the intent to use that ransomware for a certain purpose, alters and establishes certain penalties, authorizes a victim of a certain offense to bring a civil action for damages against a certain person, provides for the recovery of attorney's fees and court costs in an action brought under the Act.

### MD H 397

**Status: Enacted, Chap. 301**

Requires the Emergency Number Systems Board to establish certain minimum standards, alters the purposes of the 9-1-1 Trust Fund beginning on a certain date, authorizes the use of money collected from a certain 9-1-1 fee to pay certain costs, alters the amount of and method for calculating the 9-1-1 fee and a certain additional charge.

### MD H 711

Status: Failed

Requires an online platform to make reasonable efforts to detect anonymous foreign political communications disseminated through the online platform and prevent the dissemination of anonymous foreign political communications through the online platform, requires an online platform to report certain information to the State Board of Elections within 48 hours after the online platform becomes aware that an anonymous foreign political communication has been disseminated through the online platform.

### MD H 716

Status: Failed - Adjourned

Requires certain units of State government to comply with certain standards and guidelines to ensure that the security of all information systems and applications is managed through a certain framework, requires certain units of State government to undertake activities comprising collection, processing, and sharing of personally identifiable information in good faith and in accordance with a certain provision of the Act.

### MD H 1315

**Status: Enacted, Chap. 455**

Alters the locations of the Cyber Warrior Diversity Program in the state, specifies the amounts and uses of grants provided under the Program, alters the date by which governing entities must notify the State Higher Education Commission regarding enrollment.

### MD S 151

Status: Failed - Adjourned

Prohibits a person from committing a certain prohibited act with the intent to interrupt or impair the functioning of a health care facility, prohibits a person from knowingly possessing certain ransomware with the intent to use that ransomware for a certain purpose, alters and establishes certain penalties, authorizes a victim of a certain offense to bring a civil action for damages against a certain person, provides for the recovery of attorney's fees and court costs in an action brought under the Act.

### MD S 339

**Status: Enacted, Chap. 302**

Requires a certain custodian of records to deny inspection of the part of a 9-1-1 communications record that depicts certain information, subject to a certain exception, requires the Emergency Number Systems Board to establish certain minimum standards, alters the purposes of the 9-1-1 Trust Fund beginning on a certain date, authorizes the use of money collected from a certain 9-1-1 fee to pay certain costs, alters the amount of and method for calculating the 9-1-1 fee and a certain additional charge.

## MD S 384

Status: Failed - Adjourned

Requires the State Board of Elections to adopt regulations that describe best practices for storage and security of voter registration information by certain persons, requires a person who has received a list of registered voters to disclose a breach in the secure storage of the voter registration information to the State Administrator of Elections as soon as possible after becoming aware of the breach.

## MD S 432

**Status: Enacted, Chap. 454**

Alters the locations of the Cyber Warrior Diversity Program in the State, specifies the amounts and uses of certain grants provided under the Program, alters the date by which certain governing entities must notify the state Higher Education Commission regarding certain enrollment, requires the Commission to allocate certain funds to certain entities on a certain basis.

## MD S 581

**Status: Enacted, Chap. 211**

Extends certain benefits under the More Jobs for Marylanders Program to businesses that locate or expand in opportunity zones in the state, alters the calculation the Governor shall use in determining the amount to include in the budget Reserve Fund, alters the information required to be contained in a certain report on the Tax Credit, provides for the heritage structure rehabilitation tax credit, provides for workforce housing projects.

## MD S 726

Status: Failed - Adjourned

Alters a certain definition under the State income tax credit for the purchase of cybersecurity technology or services to repeal a prohibition on a qualified buyer having 50 or more employees, applies the Act to all tax credit certificates issued after June 30, 2019.

## Michigan

### MI H 4348

Status: Pending

Provides executive recommendations for omnibus bill, including funding for improvement of the state's cybersecurity framework.

### MI S 205

Status: Pending

Provides executive recommendations for omnibus bill, including funding for cybersecurity.

## Minnesota

### MN H 14

Status: Pending - Carryover

Relates to elections, transfers and appropriates money for purposes of the Help America Vote Act, improves the administration and security of elections as authorized by federal law, including but not limited to modernizing, securing, and updating the statewide voter registration system and for cybersecurity upgrades as authorized by federal law, improving accessibility, preparing training materials, and training local election officials.

### MN H 17

Status: Pending - Carryover

Appropriates money from the Help America Vote Act account for certain authorized purposes, provides for the purposes of modernizing, securing, and updating the statewide voter registration system and for cybersecurity upgrades as authorized by federal law.

**MN H 102**

Status: Pending - Carryover

Relates to public safety, expands crime of unauthorized computer access to include accessing a computer without penetrating security system.

**MN H 1833**

Status: Pending - Carryover

Modifies and establishes various provisions governing energy policy and finance, strengthens requirements for clean energy and energy conservation in the state, appropriates money, requires reports.

**MN H 1949**

Status: Pending - Carryover

Relates to state government, requires consideration of cloud computing service options in state agency information technology projects, requires technology infrastructure inventories and security risk assessments, requires completion of the consolidation of information technology services and a strategic workplan, requires a consolidation surcharge for certain agencies, mandates reports, defines terms.

**MN H 2087**

Status: Pending - Carryover

Relates to the operation of state government, appropriates money for the legislature, the governor's office, state auditor, attorney general, secretary of state, certain agencies, boards, and councils, changes provisions for administrative law judge salaries, revolving loan fund, cemeteries, and MERF.

**MN H 2524**

Status: Pending - Carryover

Relates to the secretary of state, creates a technology and cybersecurity account, provides for technology and cybersecurity maintenance.

**MN H 2681**

Status: Pending - Carryover

Relates to utilities, provides access rights to energy usage data maintained by utilities.

**MN H 2721**

Status: Pending - Carryover

Relates to state government, establishes a Legislative Commission on Cybersecurity, provides legislative appointments.

**MN H 2743**

Status: Pending - Carryover

Relates to courts, increases certain court related fees, establishes a cyber security fee.

**MN S 241**

Status: Failed

Relates to state government, requires the use of reports produced by the statewide voter registration system, appropriates money from the Help America Vote Act account for certain authorized purposes, including cybersecurity upgrades.

**MN S 1264**

Status: Pending - Carryover

Relates to state government, establishes a Legislative Commission on Cybersecurity, provides legislative appointments.

**MN S 2097**

Status: Pending - Carryover

Relates to state government, requires consideration of cloud computing service options in state agency information technology projects, requires technology infrastructure inventories and security risk assessments, requires completion of the consolidation of information technology services and a strategic workplan, requires a consolidation surcharge for certain agencies, mandates reports.

#### MN S 2726

Status: Pending - Carryover

Relates to the operation of state government, appropriates money for the Legislature, the Governor's office, State Auditor, Attorney General, Secretary of State, certain agencies, boards, and councils, changes provisions for administrative law judge salaries, revolving loan fund, cemeteries, and MERF.

#### MN H 3 a

Status: Failed - Adjourned

Relates to public safety, modifies certain provisions relating to public safety, courts, corrections, sexual offenders, predatory offenders, vehicle operations, and firefighters, provides for a task force and working group, requires reports, provides for criminal penalties, appropriates money for courts, public safety, sentencing guidelines, corrections, human rights, Peace Officer Standards and Training Board, Private Detective Board, Guardian ad Litem Board, and Uniform Laws Commission.

#### MN H 8 a

Status: Failed - Adjourned

Relates to the operation of state government, appropriates money for the legislature, the governor's office, state auditor, attorney general, secretary of state, and certain agencies, boards, councils, and retirement funds, changes provisions in state government operations, makes state payment terminology changes, adds provisions for presidential nomination primary, changes provisions for information technology, military and veterans affairs policy, gambling control board, and racing commission.

#### MN S 10a

**Status: Enacted, Chap. 10**

Appropriates money for government, including funds for enhancements to cybersecurity across state government and for elections cybersecurity upgrades.

### Missouri

#### MO H 917

Status: Failed - Adjourned

Modifies provisions relating to elections.

### Mississippi

#### MS H 613

Status: Failed

Exempts certain information technology records from the Mississippi Public Records Act, conforms to the provisions of this Act.

#### MS H 911

Status: Failed

Establishes the insurance data security law, provides the purpose and intent of the act, defines certain terms used in the act, requires insurance licensees in this state to develop, implement and maintain an information security program, requires certain investigation of a cyber security event, requires certain notification of a cyber security event, provides for certain confidentiality, provides exceptions to the act, provides for penalties for violations of the act.

## MS S 2046

### Status: Enacted

Exempts from the Public Records Act certain information technology related information that, if disclosed, could allow unauthorized access to the State's IT assets.

## MS S 2768

### Status: Failed

Authorizes and directs the Mississippi Department of Education to implement a mandatory k-12 computer science curriculum based on the Mississippi College and Career Readiness Standards for computer science which includes instruction in, but not limited to, computational thinking, cyber related, programming, cyber security, data science, robotics, and other computer science and cyber related content.

## MS S 2831

### Status: Enacted

Establishes the Insurance Data Security Law, provides the purpose and intent of the Act, defines certain terms used in the Act, requires insurance licensees in this state to develop, implement and maintain an information security program, requires certain investigation of a cybersecurity event, requires certain notification of a cybersecurity event, provides for certain confidentiality, provides exceptions to the Act, provides for penalties for violations of the Act.

## Montana

### MT D 1858

#### Status: Failed

Revises cybersecurity laws, relates to information technology.

### MT H.B. 2

#### Status: Enacted, Chap. 483

Appropriates money to various state agencies for the upcoming biennium, including funding for next generation antivirus software; cybersecurity staff; cybersecurity student programs; web application firewall; e-mail security gateway; security information and event management; analytics-driven security and continuous monitoring for threats; governance, risk, and compliance software; enterprise risk assessment; digital forensics lab; source code repository; security orchestration, automation and response; and outsourced professional services. Also provides that the State Information Technology Services Division shall report to the legislative finance committee quarterly on the Montana Cybersecurity Enhancement Project.

### MT H 305

#### Status: Enacted, Chap. 184

Revises the definition of state duty for special work by Montana National Guard personnel, provides state duty for special work is limited to existing provisions in preparation for declarations of emergencies and disasters and cyber security operations.

## North Carolina

### NC H 217

#### Status: Enacted, Chap. 200

Makes miscellaneous and technical changes to the statutes relating to the Department of Information Technology, amends various statutes relating to state agency cybersecurity, amends various statutes relating to the Emergency Telephone Service and the 911 Board.

NC H 904

Status: Pending

Amends the identity theft protection act.

NC H 911

Status: Pending

Directs the Department of Information Technology to study and assess the threat of foreign technologies in state owned computer systems.

NC S 542

Status: Pending

Pertains to the cyber security regional training center.

NC S 666

Status: Pending

Appropriates funds for improved cyber security education and robotics education in school districts.

## North Dakota

**ND H 1048**

**Status: Enacted, Chap. 469**

Relates to the use of distributed ledger technologies, requires the Department of Information Technologies to research and develop the use of distributed ledger enabled platform technologies, such as blockchains, for computer controlled programs, data transfer and storage, and program regulation to protect against falsification, improve internal data security, and identify external hacking threats.

**ND HCR 3004**

**Status: Adopted**

Provides for a study of the potential benefits of blockchain technology in state government administration and affairs, including the cost-effectiveness and increased security of utilizing a blockchain technology electronic voting system.

**ND S 2015**

**Status: Enacted, Chap. 40**

Provides an appropriation for defraying the expenses of the various divisions under the supervision of the director of the office of management and budget.

ND S 2110

**Status: Enacted, Chap. 468**

Expands the powers and duties of the Information Technology Department to oversee cybersecurity strategy for all executive branch state agencies, including institutions under the control of the State Board of Higher Education, counties, cities, school districts, or other political subdivisions.

ND S 2209

**Status: Enacted, Chap. 375**

Relates to protection for records related to critical infrastructure and security planning, mitigation, or threats.

ND S 2340

**Status: Enacted, Chap. 370**

Revises provisions relating to the protection and confidentiality of records regarding emergency planning and response.

## **Nebraska**

NE L 351

Status: Pending

Provides for school district levy and bonding authority for cybersecurity and violence prevention.

## **Nevada**

S.B. 21

Status: Failed

Relates to cybersecurity; enacts the Insurance Data Security Law; requires certain licensees with licenses or other authorizations related to the provision and administration of insurance to develop, implement and maintain an information security program that meets certain requirements; establishes requirements for the selection and oversight of third-party service providers by such licensees.

S.B. 123

### **Status: Enacted, Chap. 546**

Enacts provisions governing the security and integrity of elections, including requiring an annual training class on cybersecurity for those who administer elections. Provides that any records of the Secretary of State or county or city clerk relating to the security of an election information system, including records relating to the prevention of a threat or attack on the security of an election information system, are confidential and not public records and may be disclosed only under certain limited circumstances.

## **New Hampshire**

**NH H 25**

### **Status: Enacted, Chap. 146**

Makes appropriations for capital improvements for the biennium and extends certain lapse dates for previous appropriations.

**NH H 329**

### **Status: Enacted, Chap. 54**

Permits a school board to review and adopt a data security plan at a non-public meeting.

NH LSR 570

Status: Pending

Relates to review and adoption of school data security plans.

NH LSR 781

Status: Failed

Establishes the insurance data security law.

NH LSR 923

Status: Pending

Relates to the insurance data security law.

**NH S 194**

### **Status: Enacted, Chap. 309**

Establishes the Insurance Data Security Law, updates and establishes standards for protection of consumers' non public information, requirements for investigation of a breach and notification to the Commissioner and consumers in the event of cyber security breaches relating to consumers' nonpublic information.

## New Jersey

NJ A 730

Status: Pending

Clarifies crime of unlawful access concerning certain password protected communications in electronic storage.

NJ A 1766

Status: Pending

Requires certain persons and business entities to maintain comprehensive information security program.

NJ A 2355

Status: Pending

Concerns debarment of contractors for conviction of certain computer related crimes.

NJ A 3542

Status: Pending

Requires state, county, and municipal employees and certain state contractors to complete cybersecurity awareness training.

NJ A 3546

Status: Pending

Directs Rutgers Discovery Informatics Institute, the Office of Information Technology, and Big Data Alliance to develop an advanced cyber infrastructure strategic plan, appropriates funds.

NJ A 3613

Status: Pending

Revises provisions relating to the State Blockchain Initiative Task Force, requires the Task Force to study whether state, county, and municipal governments can benefit from a transition to a blockchain-based system for recordkeeping and service delivery.

NJ A 3659

Status: Pending

Requires Economic Development Authority to establish program offering low-interest loan to certain financial institutions and personal data businesses to protect business's information technology system from customer personal information disclosure.

NJ A 3922

Status: Pending

Requires state employees to review best cybersecurity practices.

NJ A 3983

Status: Pending

Requires public institutions of higher education to establish plans concerning cyber security and prevention of cyberattacks.

NJ A 4247

Status: Pending

Concerns information security standards and guidelines for State and local government.

NJ A 4854

Status: Pending

Directs New Jersey Cybersecurity and Communications Integration Cell to develop cybersecurity prevention and awareness materials for businesses and to establish electronic mail fraud Internet website.

NJ A 4976

Status: Pending

Directs New Jersey Cyber security and Communications Integration Cell to develop cyber security prevention best practices and awareness materials for consumers in this state.

NJ A 5035

Status: Pending

Requires state election officials to coordinate with relevant federal officials regarding election security.

NJ A 5467

Status: Pending

Creates affirmative defense for certain breaches of security.

NJ AJR 54

Status: Pending

Designates October of each year as Cyber Security Awareness Month.

NJ AJR 86

Status: Pending

Urges Secretary of State to assure Legislature and public that State's electoral system is protected from foreign computer hackers.

NJ AR 194

Status: Pending

Urges Congress to appropriate additional federal funds to upgrade voting equipment and systems to address vulnerabilities to cyber attacks.

NJ S 998

Status: Pending

Requires Economic Development Authority (EDA) to establish program offering low-interest loan to certain financial institutions and personal data businesses to protect business's information technology system from customer personal information disclosure.

NJ S 1249

Status: Pending

Clarifies crime of unlawful access concerning certain password protected communications in electronic storage.

**NJ S 2297**

**Status: Enacted, Chap. 213**

Revises provisions relating to the State Blockchain Initiative Task Force, relates to a study as to whether state, county, and municipal governments can benefit from a transition to a blockchain system for recordkeeping and service delivery, modifies membership of the Task Force.

NJ S 2692

Status: Pending

Requires certain persons and business entities to maintain a comprehensive information security program.

NJ S 3153

Status: Pending

Requires certain businesses to notify data subjects of collection of personally identifiable information and establishes certain security standards.

NJ S 3344

Status: Pending

Requires state election officials to coordinate with relevant federal officials regarding election security.

NJ S 3436

Status: Pending

Directs State Cybersecurity and Communications Integration Cell to develop cybersecurity prevention and awareness materials for businesses and to establish electronic mail fraud internet website.

NJ S 3488

Status: Pending

Directs State Cybersecurity and Communications Integration Cell to develop cybersecurity best practices and awareness materials for consumers in this State.

NJ S 3673

Status: Pending

Directs State Cybersecurity and Communications Integration Cell, Office of Information Technology, and State Big Data Alliance to develop an advanced cyber infrastructure strategic plan.

NJ S 3738

Status: Pending

Requires State employees to receive best cybersecurity practices.

NJ S 3836

Status: Pending

Creates affirmative defense for certain breaches of security.

NJ SJR 22

Status: Pending

Urges Secretary of State to assure Legislature and public that State's electoral system is protected from foreign computer hackers.

NJ SR 113

Status: Pending

Urges Congress to appropriate additional federal funds for election security and voting equipment purposes.

NJ SJR 134

Status: Pending

Designates October of each year as Cyber Security Awareness Month.

## New Mexico

**NM H 7**

**Status: Enacted, Chap. 60**

Relates to higher education, creates centers of excellence at higher education institutions to promote development in the cybersecurity, sustainable agriculture, and renewable energy industries, and bioscience.

## Nevada

NV A 33

Status: Failed

Revises provisions relating to the governance and oversight of information services for state agencies.

## NV S 21

Status: Failed

Relates to cybersecurity, enacts the Insurance Data Security Law, requires certain licensees with licenses or other authorizations related to the provision and administration of insurance to develop, implement and maintain an information security program that meets certain requirements, establishes requirements for the selection and oversight of third-party service providers by such licensees.

## NV S 69

**Status: Enacted, Chap. 392**

Revises provisions relating to emergencies and cybersecurity.

## NV S 123

**Status: Enacted, Chap. 546**

Revises provisions relating to elections.

## NV S 237

Status: Failed

Revises provisions relating to the security of elections.

## NV S 302

**Status: Enacted, Chap. 412**

Revises provisions relating to personal information collected by governmental agencies.

## New York

### NY A 291

Status: Pending

Directs the commissioner of the division of homeland security and emergency services to work with other experts who maintain experience and knowledge in the area of cyber security to develop a cyber security action plan for New York state.

### NY A 465

Status: Pending

Enacts the Personal Information Protection Act, establishes a personal information bill of rights requiring parties having custody of residents personal identifying information to ensure the security thereof, provides for the approval of programs to secure personal identifying information by the office of information security, requires the notification of the division of state police and the subjects of information upon the breach of such information, directs the office of technology services to/.

### NY A 914

Status: Pending

Amends the Penal Law, relates to creating the crime of cyberterrorism and calculating damages caused by computer tampering, provides that cyberterrorism shall be a class B felony.

### NY A 1185

Status: Pending

Amends the Insurance Law, authorizes continuing care retirement communities to adopt a written cybersecurity policy, requires such policies to be self certified and approved by the superintendent.

### NY A 1351

Status: Pending

Directs the state board of elections to study and evaluate the use of blockchain technology to protect voter

records and election results.

**NY A 1729**

Status: Pending

Establishes a commission to study the European Union's general protection data regulation and the current state of cyber security in the state.

**NY A 2124**

Status: Pending

Creates specific computer crimes as well as increasing penalties for crimes committed with the aid of a computer, provides for civil relief in cases of pornography on the internet, and penal sanctions in such cases.

**NY A 2229**

Status: Pending

Requires manufacturers of connected devices to equip such devices with reasonable security features.

**NY A 4884**

Status: Pending

Relates to creating the Modernized Voter Registration Act of New York, modernizes voter registration, promotes access to voting for individuals with disabilities, protects the ability of individuals to exercise the right to vote in elections for local and state office, makes an appropriation therefor.

**NY A 6514**

Status: Pending

Establishes the offenses of phishing in the third degree, phishing in the second degree and phishing in the first degree, relates to the time in which prosecution of such offenses must be commenced.

**NY A 7682**

Status: Pending

Relates to critical utility infrastructure security and responsibility, relates to the protection of critical infrastructure in the state, provides that an electric or gas corporation or municipality shall not share, disclose or otherwise provide access to a customer's electrical or gas consumption data.

**NY A 7913**

Status: Pending

Removes the economic harm requirement from the felony commercial bribery statutes, expands the crime of larceny to include theft of personal identifying information, computer data, computer programs, and services, to adapt to modern technological realities, provides state jurisdiction and county venue over cases involving larceny of personal identifying information, computer data, and computer programs, where the victim is located in the state or the county.

**NY S 229**

Status: Pending

Amends the Penal Law, relates to computer tampering.

**NY S 394**

Status: Pending

Amends the Penal Law, elevates all computer tampering offenses by one degree in severity.

**NY S 2475**

Status: Pending

Relates to computer related crimes.

**NY S 3172**

Status: Pending

Establishes the offenses of phishing in the third degree, phishing in the second degree and phishing in the first degree, relates to the time in which prosecution of such offenses must be commenced.

NY S 3625

Status: Pending

Amends the Insurance Law, promotes competitive property and casualty insurance markets for business to business insurance transactions.

NY S 3973

Status: Pending

Requires manufacturers of connected devices to equip such devices with reasonable security features.

NY S 4012

Status: Pending

Relates to the use of voice recognition features on certain products.

NY S 4273

Status: Pending

Amends the Penal Law, relates to creating the crime of cyberterrorism and calculating damages caused by computer tampering, cyberterrorism shall be a class B felony.

NY S 4444

Status: Pending

Establishes the computer security act, addressing the widespread problem of spyware, makes it illegal for third parties to knowingly and deceptively cause computer software to be copied onto personal computers that changes the computer users settings without permission, prevents users from resetting computers to the original preferences or removing third party software, secretly collects information about internet searches, disables the computers security software or causes related disruptive activities.

NY S 4744

Status: Pending

Establishes a commission to study the European Unions general protection data regulation and the current state of cyber security in the state.

NY S 5222

Status: Pending

Removes the specified amount economic harm requirement from the felony commercial bribery statutes, expands the crime of larceny to include theft of personal identifying information, computer data, computer programs, and services, to adapt to modern technological realities, provides state jurisdiction and county venue over cases involving larceny of personal identifying information, computer data, and computer programs, where the victim is located in the state or the county.

**NY S 5575B**

**Status: Enacted**

Requires businesses have in place reasonable data security for private information, with a more flexible standard for small businesses, without creating new requirements for entities subject to existing or future regulations by any federal or other New York State government entity. Deems failure to provide required reasonable data security to be a violation of section 349 of the General Business Law, permitting the attorney general to bring suit but not any private plaintiff.

NY S 6036

Status: Pending

Directs the state board of elections to study and evaluate the use of blockchain technology to protect voter

records and election results.

NY S 6195

Status: Pending

Relates to critical utility infrastructure security and responsibility, relates to the protection of critical infrastructure in the state, provides that an electric or gas corporation or municipality shall not share, disclose or otherwise provide access to a customer's electrical or gas consumption data.

## Ohio

OH S 52

Status: Pending

Creates the Civilian Cyber Security Reserve Forces, requires the Secretary of State as a member of the Homeland Security Advisory Council, requires the Secretary to appoint a Chief Information Security Officer, requires the Boards of Elections to audit election results, makes an appropriation.

## Ohio

**OH H 166**

**Status: Enacted, Chap. 10**

Provides funding for cybersecurity initiatives, including for the establishment of a cyber range. The cyber range shall: (1) provide cyber training and education to K-12 students, higher education students, Ohio National Guardsmen, federal employees, and state and local government employees, and (2) provide for emergency preparedness exercises and training.

## Oklahoma

OK H 2146

Status: Pending - Carryover

Creates a credit against income tax for qualified software or cybersecurity employees.

**OK H 2759**

**Status: Enacted, Chap. 483**

Relates to revenue and taxation, provides for certain qualified employers to make application to the Tax Commission, provides for income tax credit, specifies tax credit amount, imposes limitation on taxable years for which tax credit may be claimed, prohibits reduction of tax liability to less than zero, authorizes qualified employers to participate in designated economic incentives.

**OK S 261**

**Status: Enacted, Chap. 163**

Relates to election security, relates to the security of election materials, coercion, and election emergencies, authorizes post election audits for certain purposes, provides procedures, specifies the duties of the Secretary of State Election Board and the Secretary of County Election Board, specifies requirements relating to office space and arrangements for county election boards, prohibits providing false or misleading information to prevent registration or voting.

**OK S 584**

**Status: Enacted, Chap. 331**

Relates to public finance, relates to security risk assessments, establishes requirements for information security audit conducted by certain firm under certain basis, requires Information Services Division to assist in repairing vulnerabilities, provides an exception for certain agencies subject to

certain mandatory cybersecurity standards, requires submission of information security audit findings, modifies requirement for submission of findings within certain time.

#### OK S 746

Status: Pending - Carryover

Relates to income tax credits, establishes tax credits for certain software or cybersecurity employees, provides a specified amount for the credit, imposes a maximum number of taxable years for which the credit may be claimed, prohibits the use of the credit to reduce tax liability below a certain amount, provides for certain qualified employers to make application to the State Tax Commission.

### Oregon

#### OR H 2395

**Status: Enacted, Chap. 193**

Requires person that manufactures, sells or offers to sell connected device to equip connected device with reasonable security features that protect information that connected device collects, contains, stores or transmits from access, destruction, modification, use or disclosure that consumer does not authorize.

#### OR H 3109

Status: Failed

Directs Oregon Business Development Department to study tax incentives for cyber security businesses and to report its findings to interim legislative committees related to economic development.

#### OR H 3233

Status: Failed

Establishes program to improve cyber security of systems used to administer elections by encouraging independent technical experts, in cooperation with state election officials, local government election officials and election service providers, to identify and report election cyber security vulnerabilities.

#### OR S 818

Status: Failed

Establishes program to improve cybersecurity of systems used to administer elections by encouraging independent technical experts, in cooperation with state election officials, local government election officials and election service providers, to identify and report election cybersecurity vulnerabilities.

#### OR SCR 4

Status: Failed

Declares policy of the state concerning cybersecurity risks and need for proactive cybersecurity risk management.

### Pennsylvania

#### PA H 140

Status: Pending

Provides appropriations from the General Fund for the expenses of the Executive, Legislative and Judicial Departments of the Commonwealth, the public debt and the public schools for the fiscal year July 1, 2019, to June 30, 2020, and for the payment of Bills incurred and remaining unpaid at the close of the fiscal year ending June 30, 2019, provides appropriations from special funds and accounts to the Executive and Judicial Departments.

## **PA H 225**

Status: Pending

Amends the act, known as The Administrative Code of 1929, in organization of departmental administrative boards and commissions and of advisory boards and commissions, provides for Cyber security Innovation Commission.

## **PA S 487**

Status: Pending

Amends the act of December 22, 2005, known as the Breach of Personal Information Notification Act, provides for title of act, for definitions and for notification of breach, prohibits employees of the Commonwealth from using nonsecured Internet connections, provides for Commonwealth policy and for entities subject to the Health Insurance Portability and Accountability Act of 1996.

## **PA S 810**

Status: Pending

Relates to boards and offices; provides for information technology; establishes the Office of Information Technology and the Information Technology Fund; provides for administrative and procurement procedures and for the Joint Cybersecurity Oversight Committee; imposes duties on the Office of Information Technology; imposes penalties.

## **Rhode Island**

### **RI H 5480**

Status: Failed--adjourned

Establishes that manufacturers of devices capable of connecting to the Internet equip the devices with reasonable security features.

### **RI H 5987**

Status: Failed--adjourned

Criminalizes accessing the user account of another person without consent for the purpose of viewing or using information maintained on any electronic database, website, or account, with each instance constituting a separate offense.

### **RI S 537**

Status: Failed--adjourned

Establishes that manufacturers of devices capable of connecting to the Internet equip the devices with reasonable security features.

## **South Carolina**

### **SC H 4293**

Status: Pending - Carryover

Establishes the state Election Security Council, provides for the council's composition, duties, powers, and responsibilities, provides that after the effective date of this act, all voting systems used in the state shall utilize a paper based system using paper ballots tabulated by optical scanners as the ballot of record, requires the General Assembly to appropriate the funds necessary to purchase the voting systems required by this section.

### **SC S 374**

Status: Pending - Carryover

Establishes the state Election Security Council, provides for the council's composition, duties, powers, and responsibilities, provides that after the effective date of this act all voting systems used in the state

shall utilize a paper-based system using paper ballots tabulated by optical scanners as the ballot of record, requires the general assembly to appropriate the funds necessary to purchase the voting systems required by this section.

## Texas

### TX H 1

#### **Status Enacted, Chap. 1353**

Provides for appropriations for cybersecurity.

### TX H 350

Status: Failed - Adjourned

Relates to the composition of the cybersecurity council.

### TX H 351

Status: Failed - Adjourned

Relates to emergency management for cyberattacks against this state.

### TX H 904

Status: Failed - Adjourned

Relates to requiring The University of Texas at San Antonio to conduct a study regarding cyber attacks against financial institutions in this state.

### TX H 1421

#### **Status: Enacted, Chap. 1069**

Relates to cybersecurity of voter registration lists and other election-related documents, systems, and technology, provides that the secretary of state shall adopt rules defining classes of protected election data and establishing best practices for identifying and reducing risk to the electronic use, storage, and transmission of election data and the security of election systems.

### TX H 2401

Status: Failed - Adjourned

Relates to the requirement that state agency employees complete cyber security awareness training.

### TX H 2591

Status: Failed - Adjourned

Relates to a cybersecurity monitor for certain electric utilities.

### TX H 2689

Status: Failed - Adjourned

Relates to the designation of a cybersecurity coordinator by each school district.

### TX H 2984

#### **Status: Enacted, Chap. 1149**

Revises provisions relating to the essential knowledge and skills of the technology applications curriculum, establishes the Computer Science Strategic Advisory Committee to increase computer science instruction and participation in public schools.

### TX H 3377

Status: Failed - Adjourned

Relates to a cybersecurity monitor for certain electric utilities.

### TX H 3834

**Status: Enacted, Chap. 1308**

Revises provisions relating to the requirement that certain state and local government employees and state contractors complete a cybersecurity training program certified by the State Cybersecurity Coordinator.

**TX H 4214**

Status: Failed - Adjourned

Relates to matters concerning governmental entities, including cyber security, governmental efficiencies, information resources, and emergency planning.

**TX H 4539**

Status: Failed - Adjourned

Relates to elections.

**TX H 4597**

Status: Failed - Adjourned

Relates to cybersecurity of state agencies.

**TX HR 2180**

Status: Adopted

Appropriates funds for the purpose of providing security vulnerability and penetration testing services and information security assessments to state agencies and institutions of higher education.

**TX S 1**

Status Failed-adjourned.

Provides for appropriations for cybersecurity.

**TX S 9**

Status: Failed - Adjourned

Relates to election integrity, increases criminal penalties, creates a criminal offense, creates civil penalties.

**TX S 64**

**Status: Enacted**

Establishes strategies to incentivize cybersecurity degree programs, provides for the coordination of cybersecurity coursework development, revises provisions relating to information sharing, requires the State Cybersecurity Coordinator to develop best practices for cybersecurity, provides for cybersecurity coordination programs for utilities.

**TX S 820**

**Status: Enacted, Chap. 605**

Requires a school district to develop and maintain a cybersecurity framework.

**TX S 936**

**Status: Enacted, Chap. 610**

Revises provisions relating to the Cybersecurity Monitor Program for electric utilities, requires the Public Utilities Commission to contract with an entity to act as the Commission's Cybersecurity Monitor, authorizes an electric utility, municipally owned utility, or electric cooperative to participate or discontinue participation in the Cybersecurity Monitor Program.

**TX S 1779**

Status: Failed - Adjourned

Relates to security for state agency information and information technologies.

**TX S 1785**

Status: Failed - Adjourned

Relates to the composition of the cybersecurity council.

TX S 1985

Status: Failed - Adjourned

Relates to the regulation of certain health organizations certified by the State Medical Board, provides an administrative penalty.

## Virginia

**VA H 1700**

**Status: Enacted, Chap. 854**

Amends the Budget Bill. provides funding for cybersecurity programs.

**VA H 2178**

**Status: Enacted, Chap. 426**

Relates to the voter registration system, relates to security plans and procedures, relates to remedy security risks, directs the State Board of Elections to promulgate regulations and standards necessary to ensure the security and integrity of the voter registration system and the supporting technologies utilized by the counties and cities to maintain and record registrant information, requires local electoral boards to develop and update annually written plans.

**VA H 2332**

**Status: Enacted, Chap. 399**

Requires the State Corporation Commission to convene a stakeholder group on consumer data protection issues.

**VA H 2519**

Status: Failed

Relates to Virginia Information Technologies Agency, relates to a cybersecurity task force, establishes a cybersecurity task force to assist the Chief Information Officer (CIO) of the Virginia Information Technologies Agency in developing policies, standards, and guidelines applicable to the Commonwealth's executive, legislative, and judicial branches and independent agencies for assessing security risks, determining the appropriate security measures and performing security audits.

**VA H 2534**

Status: Failed

Relates to Virginia Information Technologies Agency, relates to required information security training program for state employees, requires the Chief Information Officer of the Virginia Information Technologies Agency to develop and annually update a curriculum and materials for training all state employees in information security awareness and in proper procedures for detecting, assessing, reporting, and addressing information security threats by November 1, 2019.

**VA H 2787**

Status: Failed

Relates to state voter registration system, relates to security plans and procedures, relates to remedying security risks.

**VA H 2793**

Status: Failed

Relates to cybersecurity, relates to care and disposal of customer records, relates to security for connected devices, requires any business to take all reasonable steps to dispose of, or arrange for the disposal of, customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable.

**VA HJR 628**

**Status: Failed**

Relates to Virginia Freedom of Information Advisory Council, relates to threat of phishing attacks, relates to reporting, directs the Virginia Freedom of Information Advisory Council (FOIA Council) to study the threat of phishing attacks on citizens and public employees whose contact and private information is legally obtained as a result of a Freedom of Information Act (FOIA) request, provides that the study further directs the FOIA Council to examine the current FOIA provisions.

**VA S 966**

**Status: Enacted, Chap. 296**

Relates to electric utility regulation, provides for grid modernization and energy efficiency programs, provides for rate review proceedings and transitional rate periods, provides for energy storage facilities, relates to electric distribution grid transformation projects, and wind and solar generation facilities, relates to coal combustion by product management, relates to undergrounding electrical transmission lines, relates to fuel factor.

**VA S 1233**

**Status: Enacted, Chap. 302**

Relates to the administration of government, prohibits public bodies from using products and services provided by Kaspersky Lab, requires the State Information Technologies Agency to review statewide procedures for implementing such a prohibition and to prepare a report with recommendations for the Governor and General Assembly.

**VA H 5001a**

**Status: Enacted, Chap. 1**

Revises the budget bill; makes appropriations to various state agencies and programs, including cybersecurity programs.

**VA H 5002a**

**Status: Enacted, Chap. 2**

Revises the budget bill; makes appropriations to various state agencies and programs, including cybersecurity programs.

## **Vermont**

**VT H 135**

**Status: Enacted, Chap. 49**

Relates to the authority of the Agency of Digital Services.

**VT H 157**

**Status: Pending - Carryover**

Relates to adopting minimum security standards for connected devices.

**VT S 110**

**Status: Pending - Carryover**

Requires a report concerning the three branches of state government and the management of personally identifiable information. Relates to security of student information.

## **Washington**

**WA H 1109**

**Status: Enacted, Chap. 415**

Makes operating appropriations for the upcoming biennium, including appropriations for the office of cybersecurity.

## WA H 1126

### **Status: Enacted, Chap. 205**

Enables electric utilities to prepare for the distributed energy future, proposes monitoring, control, and metering upgrades that are supported by a business case identifying how those upgrades will be leveraged to provide net benefits for customers, provides for cybersecurity and data privacy practices to the changing distribution system and the internet of things, including an assessment of the costs associated with ensuring customer privacy.

## WA H 1251

### Status: Pending - Carryover

Concerns security breaches of election systems or election data including by foreign entities.

## WA H 1840

### Status: Pending - Carryover

Concerns the removal of payment credentials and other sensitive data from state data networks.

## WA H 2111

### Status: Pending - Carryover

Concerns enhancing cybersecurity by eliminating the return of ballots by fax and email.

## WA S 5153

### Status: Pending - Carryover

Makes 2019-2021 biennium operating appropriations, including for the office of cyber security.

## West Virginia

## WV H 2452

### **Status: Enacted, Act 123**

Creates the West Virginia cybersecurity office, relates to cybersecurity of state government, removes the requirements of the Chief Technology Officer to oversee security of government information, creates the Cybersecurity Office, provides that the Chief Information Security Officer to oversee the Cybersecurity Office, authorizes the Chief Information Security Officer to create a cybersecurity framework, to assist and provide guidance to agencies in cyber risk strategy.

## WV S 314

### Status: Failed - Adjourned

Relates to cybersecurity of state government.

## Puerto Rico

## PR H 92

### Status: Pending - Carryover

Creates the Investigative Cyber Crimes Unit under the Department of Justice which will be in charge of investigating and prosecuting serious and less serious crimes and/or misdemeanors related to the right to privacy, ownership, identity and security in commercial transactions, when committed using electronic means, such as the Internet and the computer.

## PR HR 246

### **Status: Adopted**

Orders the House Committee on Public Security to investigate the feasibility of establishing a forensic laboratory in cybercrimes, similar to that of the Immigration and Customs Enforcement, which provides primary services to state agencies.

**PR HR 367**

Status: Pending - Carryover

Orders the House Committee on Public Safety to assess the feasibility of establishing a forensic laboratory in cyber crimes, similar to that of the Immigration and Customs Enforcement, which provides services exclusively to state agencies.

**PR HR 257**

Status: Pending - Carryover

Orders the House Committees on Finance and Public Security to investigate the information systems of the Department of the Treasury, its maintenance and the reasons for a cyber virus that caused on Monday, January 6 of 2017 the Department of the Treasury to raise about \$20 million, determines if the information from taxpayers and the government hosted on the servers of the Department of the Treasury was affected as a result of this cyber virus.

**PR HR 475**

Status: Pending - Carryover

Orders the House Committee on Public Safety to research the practices and policies of cyber security and of the executive departments and agencies of the Government, with urgency in the Department of the Treasury, the State Department and Department of Public Safety.

**PR SR 158**

**Status: Adopted**

Orders the Senate Committee on Finance of the Senate to study cyber attacks on the electronic systems of the Department of the Treasury and the Municipal Revenues Collection Center; studies the effect of this incident in the fulfilment of the functions of these agencies regarding any information, either from the Government or its taxpayers, that was affected; studies preventive measures to be established to avoid that this continues happening.

*Powered by*

**LexisNexis® State Net®**

*Heather Morton is a program principal in Fiscal Affairs. She covers financial services, alcohol production and sales, telecommunications and medical malpractice issues for NCSL.*