SB 812

Department of Legislative Services

Maryland General Assembly
2022 Session

FISCAL AND POLICY NOTE
Enrolled - Revised

Senate Bill 812 (Senator Hester, *et al.*)

Education, Health, and Environmental Affairs Health and Government Operations

State Government - Cybersecurity - Coordination and Governance

This bill significantly expands and enhances the State's regulatory framework for State and local government cybersecurity. Among other things, the bill (1) codifies and expands the Maryland Cyber Defense Initiative; (2) establishes various assessment and reporting requirements for State agencies and local governments; (3) requires the Department of Information Technology (DoIT) to ensure each agency's compliance with cybersecurity standards under certain circumstances; and (4) requires DoIT to develop a centralization transition strategy and conduct a self-performance and capacity assessment. The Governor must include an appropriation in the annual budget bill in an amount necessary to cover the costs of implementing a required statewide cybersecurity master plan without the need for DoIT to operate a charge-back model for cybersecurity services provided to units of State and local government. For fiscal 2023, funds may be transferred by budget amendment from the Dedicated Purpose Account (DPA) to implement the bill. **The bill takes effect July 1, 2022.**

Fiscal Summary

State Effect: General fund expenditures increase by *at least* $17.3 million in FY 2023 for staff, cybersecurity assessments, software, and operating costs; $10 million is budgeted for the assessments. Future years reflect annualization and ongoing cybersecurity assessments and operating costs. Biennial cybersecurity assessments totaling $10.0 million are covered by DPA in FY 2025 and general fund expenditures in FY 2027 (with State agency expenditures (all funds) increasing correspondingly). General fund expenditures further increase significantly for DoIT and State agencies to implement the cybersecurity strategy and to produce the various required reports; this impact is not shown below. Revenues are not likely affected.

($ in millions)	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027
Revenues	$0	$0	$0	$0	$0
GF Expenditure	17.3	8.2	8.4	8.6	18.7
SF Expenditure	0	0	10.0	0	0
Net Effect	($17.3)	($8.2)	($18.4)	($8.6)	($18.7)

Note:() = decrease; GF = general funds; FF = federal funds; SF = special funds; - = indeterminate increase; (-) = indeterminate decrease

Local Effect: County and Baltimore City expenditures increase, potentially significantly, to obtain cybersecurity assessments and produce the required plans and reports. These costs may be offset to the extent that local governments receive assistance from DoIT, as discussed below. **This bill may impose a mandate on a unit of local government.**

Small Business Effect: Meaningful.

Analysis

Bill Summary: Broadly, the bill:

- expressly excludes the Office of the Attorney General, the Comptroller, the State Treasurer, and the Legislative Branch and the Judicial Branch of State government from DoIT oversight related to information technology (IT);
- codifies various aspects of Executive Order 01.01.2019.07, which established the Maryland Cyber Defense Initiative, the Office of Security Management (OSM), and the Maryland Cybersecurity Coordinating Council (MCCC) in DoIT, and expands and modifies OSM's and MCCC's responsibilities;
- establishes qualifications for the individual appointed as the State Chief Information Security Officer (SCISO);
- requires the Governor to report to the General Assembly by January 31 of each year on specified IT and cybersecurity issues and funding;
- requires DoIT to develop and require basic security requirements that include specified criteria to be included in State contracts;
- clarifies that the IT master plan must include a statewide cybersecurity strategy;
- expands DoIT's responsibilities to include (1) centralizing the management and direction of IT policy within the Executive Branch under the control of DoIT and (2) ensuring the statewide IT master plan allows a State agency to maintain its own IT unit, as specified;
- requires OSM to (1) ensure that each unit of State government completes an external assessment at least every two years and (2) assist each unit to remediate findings, as specified;
- requires specified units within the Office of the Attorney General, Office of the Comptroller, Office of the State Treasurer, and Legislative and Judicial branches to be evaluated by an independent auditor for compliance with specified cybersecurity standards;
- requires each unit of State government, by December 1 of each year, to report to the Governor and General Assembly on specified information related to recently done cybersecurity preparedness assessments, IT equipment, initiatives, and staffing;

- requires each unit of State government to report a cybersecurity incident to SCISO, who must then take specified actions;
- requires specified local government entities (but not municipal governments) to, in a manner and frequency established in regulations adopted by DoIT, consult with the local emergency manager to create or update a cybersecurity preparedness and response plan and complete a cybersecurity preparedness assessment;
- requires local government entities to report a cybersecurity incident to specified entities;
- requires each agency in the Executive Branch of State government to certify to OSM, by June 30, 2023, compliance with specified minimum cybersecurity standards, and requires OSM to ensure compliance of an agency's cybersecurity with cybersecurity standards through specified means if the agency has not remediated cybersecurity-related findings by July 1, 2024 (this requirement does not apply if a federal law or regulation forbids OSM from managing a specific system);
- requires DoIT, by December 31, 2022, to complete the implementation of a governance, risk, and compliance (GRC) module across the Executive Branch of State government that meets specified requirements;
- requires OSM, in consultation with MCCC, to prepare, by June 30, 2023, a specified transition strategy toward cybersecurity centralization and report the strategy and related recommendations to specified committees of the General Assembly;
- requires DoIT to hire a contractor to conduct a performance and capacity assessment to evaluate the department's capacity to implement the bill;
- authorizes, for fiscal 2023, the transfer of funds by budget amendment from the DPA to implement the bill; and
- requires the SCISO to establish, by October 1, 2022, guidelines to determine when a cybersecurity incident must be disclosed to the public.

A more detailed description of these changes can be found below.

Maryland Cyber Defense Initiative – Codified and Expanded

Executive Order 01.01.2019.07, which established the Maryland Cyber Defense Initiative, is codified and expanded. The initiative established OSM within DoIT; the position of SCISO to head OSM; and MCCC to advise and assist SCISO and OSM. The bill adopts substantially similar responsibilities for OSM, SCISO, and MCCC as those required by the executive order; however, the bill also expands the responsibilities beyond what is required by the executive order in the following ways:

- SCISO must be appointed by the Governor with the advice and consent of the Senate and meet the education and experience qualifications established by the bill.

- OSM must establish standards to categorize all information collected or maintained by or on behalf of each unit of State government.
- If the SCISO determines that there are security vulnerabilities or deficiencies in any information systems, OSM must determine and direct or take actions necessary to correct or remediate the vulnerabilities or deficiencies, which may include requiring the information system to be disconnected.
- If SCISO determines that there is a cybersecurity threat caused by an entity connected to Network Maryland that introduces a serious risk to entities connected to the network or to the State, OSM must take or direct actions required to mitigate the threat.
- OSM is responsible for coordinating with the Maryland Department of Emergency Management (MDEM) Cyber Preparedness Unit during emergency response efforts.
- OSM is not responsible for IT information installation and maintenance operations normally conducted by a unit of State government, a unit of local government, a local school board, a local school system, or a local health department.
- OSM must develop and maintain IT security policies, standards, and guidance documents, consistent with best practices developed by the National Institute of Standards and Technology (NIST).
- OSM must, to the extent practicable, seek, identify, and inform relevant stakeholders of any available financial assistance provided by the federal government or non-State entities to support the work of the office.
- OSM must provide (1) technical assistance to localities in mitigating and recovering from cybersecurity incidents and (2) provide technical services, advice, and guidance to units of local government to improve cybersecurity preparedness, prevention, response, and recovery practices.
- OSM must coordinate with MDEM to assist specified local government entities with specified cybersecurity preparedness activities.
- OSM may coordinate with MDEM to conduct regional exercises and establish regional assistance groups, as specified.
- By December 31 each year, OSM must provide an annual report to the Governor and specified committees of the General Assembly on its activities and the state of cybersecurity preparedness in Maryland. The report must include specified information. However, the report may not contain information that reveals cybersecurity vulnerabilities and risk in the State.
- The membership of MCCC is expanded and specified representatives of the General Assembly and Judiciary may serve as nonvoting members. Additionally, the responsibilities of MCCC are expanded to include (1) reviewing OSM analyses to develop recommendations, as specified; (2) promoting cybersecurity education and training opportunities, as specified; and (3) utilizing relationships with institutions

of higher education to advertise cybersecurity careers and job positions in State or local governments.

To implement the existing and new responsibilities, the bill establishes two new positions (a director of State cybersecurity and a director of local cybersecurity) to oversee and implement the bill's requirements for units of State and local government, as appropriate. DoIT must provide OSM with sufficient staff to implement the bill.

Local Cybersecurity Preparedness Assessments and Incident Reporting

The following requirements do not apply to municipal governments. In a manner and frequency established by DoIT in regulations, each county government, local school system, and local health department must (1) consult with the local emergency manager to create or update a cybersecurity preparedness and response plan and (2) complete a cybersecurity preparedness assessment. The required assessment may, in accordance with the preference of each county government, be performed by DoIT or a vendor authorized by DoIT.

Each local government must report a cybersecurity incident, including an attack on a State system being used by the local government, to the appropriate local emergency manager and the State Security Operations Center within DoIT. SCISO must determine the criteria for when an incident must be reported, the manner in which to report, and the time period within which a report must be made. The State Security Operations Center must immediately notify appropriate agencies of a reported incident.

External Assessments for Units of State Government

OSM must ensure that each unit of State government completes an external assessment at least once every two years (or more often, if required by regulations) and assist each unit to remediate any security vulnerabilities or high-risk configurations identified in the assessment.

Each unit of the Legislative or Judicial Branch, Office of the Attorney General, Office of the Comptroller, or Office of the State Treasurer that provides IT services for another unit of government must (1) be evaluated by an independent auditor to determine compliance with relevant cybersecurity standards recommended by NIST, as specified, and (2) certify compliance with the recommended standards.

Required Certification of Compliance with Minimum Cybersecurity Standards

By June 30, 2023, each agency in the Executive Branch of State government must certify to OSM compliance with State minimum cybersecurity standards established by DoIT. In

general, certification must be reviewed by independent auditors, and any findings must be remediated. For the Department of Public Safety and Correctional Services and any State criminal justice agency, certification must be reviewed by the Office of Legislative Audits, and any findings must be remediated.

If an agency has not remediated any findings pertaining to State cybersecurity standards found by the independent audit by July 1, 2024, OSM must ensure compliance of an agency's cybersecurity through a shared service agreement, administrative privileges, or access to Network Maryland. This requirement does not apply if a federal law or regulation forbids OSM from managing a specific system.

Authority of the Secretary of Information Technology

The Secretary of Information Technology is responsible for centralizing the management and direction of IT and cybersecurity policy in the Executive Branch under DoIT's control. The Secretary must also ensure that the State's IT plan and related policies allow State agencies to maintain their own IT units that provide IT services. The Secretary may review any cybersecurity project for consistency with the State's master plan.

Basic Security Requirements for Specified Contracts

DoIT must require basic security requirements to be included in a contract (1) in which a third-party contractor will have access to and use State telecommunication equipment, systems, or services or (2) for systems or devices that will connect to State telecommunication equipment, systems, or services. The security requirements must be consistent with a widely recognized security standard, as specified.

The bill further requires DoIT, in consultation with MCCC, to study the security and financial implications of executing partnerships with other states to procure IT and cybersecurity products and services, including the implications for political subdivisions of the State.

Required Transition Strategy and Performance and Capacity Assessment

By June 30, 2023, OSM, in consultation with MCCC, must prepare a transition strategy toward cybersecurity centralization, including recommendations for (1) consistent incident response training; (2) implementing security improvement dashboards to inform budgetary appropriations; (3) operations logs transition to the Maryland Security Operations Center; (4) establishing consistent performance accountability metrics for IT and cybersecurity staff; and (5) whether OSM needs additional staff or contractors to carry out its duties.

In addition, the bill requires DoIT to hire a contractor to conduct a performance and capacity assessment to (1) evaluate DoIT's capacity to implement the bill's provisions and (2) recommend additional resources necessary for DoIT to implement the bill's requirements and meet future needs, including additional budget appropriations, additional staff, altered contracting authority, and pay increases for staff. The contractor hired by DoIT to complete the assessment must submit to the Governor and the General Assembly (1) an interim report of its findings and recommendations by December 1, 2023, and (2) a final report by December 1, 2024.

Guidelines for Disclosure of Cybersecurity Incidents

By June 1, 2022, the SCISO must establish guidelines to determine when a cybersecurity incident must be disclosed to the public. By November 1, 2022, the SCISO must submit a report on the guidelines to specified legislative committees.

Current Law:

Department of Information Technology and Cybersecurity

DoIT and the Secretary of Information Technology are responsible for:

- developing and enforcing IT policies, procedures, and standards;
- providing technical assistance, advice, and recommendations to any unit of State government;
- reviewing agency project plans to make information and services available to the public over the Internet;
- developing and maintaining a statewide IT master plan, as specified;
- adopting and enforcing nonvisual access standards to be used in the procurement of IT services, as specified;
- in consultation with the Attorney General, advising and overseeing a consistent cybersecurity strategy for units of State government, as specified;
- advising and consulting with the Legislative and Judicial branches of State government regarding a cybersecurity strategy; and
- in consultation with the Attorney General, developing guidance on consistent cybersecurity strategies for specified local government entities.

For information on recent cyberattacks affecting State agency and local government information systems and recent legislation and gubernatorial action taken to address cybersecurity and IT issues in the State, including the Governor's Cyber Defense Initiative, please see the **Appendix – Cybersecurity**.

Maryland Department of Emergency Management

Chapters 287 and 288 of 2021 established MDEM as a principal department of the Executive Branch of State government and as the successor to the Maryland Emergency Management Agency. MDEM is responsible for coordinating the State response in any major emergency or disaster. This includes supporting local governments as needed or requested and coordinating assistance with the Federal Emergency Management Agency and other federal partners. MDEM manages many of the federal grants that fund a broad range of initiatives leading to enhanced protection from and responses to the full range of natural and man-made disasters that could threaten the State's citizens. Each local government has a Local Emergency Management Director who works with MDEM on behalf of the local government during a major emergency or disaster.

State Expenditures:

Dedicated Purpose Account

DPA is one of four accounts that make up the State Reserve Fund. The fiscal 2023 budget, as enacted, includes $200.0 million in DPA to address cybersecurity issues – $100.0 million as a deficiency appropriation for fiscal 2022 and another $100.0 million for fiscal 2023. Also, DPA has $10.0 million in unexpended funds from fiscal 2021 specifically for cybersecurity assessments; this $10.0 million in funding will expire at the end of fiscal 2025. Although the bill authorizes the use of funding in DPA to implement the bill in fiscal 2023, this analysis *generally* assumes DoIT uses DPA funding for other purposes related to cybersecurity (such as upgrading existing systems). However, DoIT costs for cybersecurity assessments in fiscal 2025 are assumed to be covered with the unspent DPA funding from fiscal 2021. Initial assessments in fiscal 2023 are assumed to be fully covered with general funds appropriated in DoIT's budget specifically for that purpose; nevertheless, any residual costs for those assessments may be offset with DPA funding as necessary.

Department of Information Technology

To handle the substantial additional responsibilities required by the bill and because the bill requires DoIT to provide OSM with sufficient resources and staff to implement the bill, DoIT requires an estimated 40 additional staff. Additionally, DoIT incurs additional one-time contractual costs to conduct a performance and capacity assessment and annual contractual costs to license vulnerability assessment software and to implement a GRC module across all State agencies.

Therefore, general fund expenditures by DoIT increase by $17.3 million in fiscal 2023, which accounts for a 90-day delay from the bill's July 1, 2022, effective date. This estimate

reflects the cost of hiring 40 full-time staff, including cyber policy and strategy planners, cyber defense incident responders, and vulnerability assessment analysts to handle the significant expansion of responsibilities for OSM, including providing significant levels of assistance to local governments. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses. It also includes $10 million for cybersecurity assessments (which are discussed in greater detail below), an assumed $200,000 for the performance and capacity assessment, $1 million for vulnerability assessment software, and $1 million to implement the GRC module.

Positions	40.0
Salaries and Fringe Benefits	$4,790,260
Cybersecurity Assessments	10,000,000
Vulnerability Assessment Software	1,000,000
GRC Module Costs	1,000,000
Assessment Contractor	200,000
Operating Expenses	293,720
Total FY 2023 DoIT Expenditures	**$17,283,980**

Future year expenditures reflect annualization and full salaries with annual increases and employee turnover, annual increases in ongoing operating expenses, and ongoing licensing costs for the vulnerability assessment and GRC software.

DoIT may experience significant additional costs in future fiscal years to implement the statewide cybersecurity strategy, and to the extent that DoIT is required to ensure compliance of an agency's cybersecurity with cybersecurity standards through a shared service agreement, administrative privileges, or access to Network Maryland; however, any such impact cannot be reliably estimated at this time. If DoIT assumes responsibility for a State agency's cybersecurity, expenditures for that agency decrease accordingly.

The bill requires State agencies to receive "external assessments" at least once every two years. Although not expressly clear, the Department of Legislative Services (DLS) believes that the requirement refers to the more common cybersecurity preparedness assessments. DoIT advises that, on average, cybersecurity assessments cost between $75,000 and $100,000 per IT system, and the State has approximately 125 different systems spanning all Executive Branch agencies. As such, the total cost of conducting the assessments for all State agencies is approximately $10.0 million every two years beginning in fiscal 2023.

As noted above in the discussion concerning DPA, general funds are budgeted to cover the cost of assessments in fiscal 2023 and the unspent $10.0 million in DPA funding (from fiscal 2021) is assumed to cover the subsequent assessments in fiscal 2025; otherwise, that DPA funding will expire at the end of fiscal 2025. While some portion of DPA funding

included in the fiscal 2023 budget could likewise be used for assessments in fiscal 2027; this analysis assumes that the other DPA funding is instead used for broader purposes related to cybersecurity. As such, general funds are needed to cover the cost of assessments in that year because the bill requires implementation of a cybersecurity strategy by DoIT without the need to operate the "charge-back" model that DoIT generally uses to provide services to State agencies.

Independent Audits

The bill requires each unit of the Legislative or Judicial Branch, Office of the Attorney General, Office of the Comptroller, or Office of the State Treasurer that provides IT services for another unit of government to (1) be evaluated by an independent auditor to determine compliance with relevant cybersecurity standards recommended by NIST, as specified, and (2) certify compliance with the recommended standards.

Generally, (1) DLS and the Office of Legislative Audits within the Legislative Branch each have their own internal IT units and (2) the Judiciary primarily uses an internal IT system known as the Maryland Electronic Courts case management system. Thus, it is unclear at this time whether either branch of government would require audits to be conducted. To the extent that any audits are necessary, general fund expenditures increase accordingly.

Similarly, DLS is not aware that the Office of the Attorney General, the Comptroller's Office, or the Treasurer's Office provide IT services to any other unit. However, to the extent that any audits are required for these agencies, general fund expenditures increase accordingly. Any such costs are unknown and not included in this estimate.

Local Fiscal Effect: Local expenditures increase, potentially significantly, beginning in fiscal 2023 as county governments, local school systems, and local health departments (1) develop, update, and implement cybersecurity preparedness and response plans and (2) conduct annual cybersecurity preparedness assessments.

The total cost for each affected local government cannot be reliably estimated at this time, as it primarily depends on (1) the requirements established by DoIT under the bill for local governments; (2) how many IT systems must be assessed for each local government; and (3) the complexity of the systems being assessed. Specifically, private-sector costs for cybersecurity assessments range significantly depending on the type of assessment being done and the size and complexity of the IT system being assessed; costs can range from between $15,000 (for basic assessments and systems) and $100,000 (for more complicated assessments and systems). As noted above, costs for the high-quality assessments used by DoIT generally range from $75,000 to $100,000 per system.

Local government costs for plan implementation and cybersecurity assessments may be offset to the extent that they receive assistance from DoIT in the manner required by the bill; however, any such offset cannot be reliably estimated without actual experience under the bill.

Small Business Effect: Small businesses that offer cybersecurity preparedness assessments are likely to experience a significant increase in business under the bill.

Additional Information

Prior Introductions: None.

Designated Cross File: HB 1346 (Delegate P. Young, *et al.*) - Health and Government Operations.

Information Source(s): Department of Information Technology; Maryland Department of Emergency Management; Maryland Longitudinal Data Systems Center; Maryland Department of Agriculture; Department of Commerce; Department of Natural Resources; Maryland Department of Planning; Maryland Department of the Environment; Department of General Services; Maryland Higher Education Commission; Maryland Department of Disabilities; Judiciary (Administrative Office of the Courts); Military Department; Department of State Police; Maryland Department of Aging; Office of the Public Defender; State Prosecutor's Office; Department of Public Safety and Correctional Services; Maryland Department of Transportation; Department of Veterans Affairs; Maryland Association of Counties; Maryland Municipal League; Maryland Association of County Health Officers; Charles, Frederick, Montgomery, and Somerset counties; Department of Legislative Services

Fiscal Note History: First Reader - February 20, 2022
km/mcr Third Reader - April 11, 2022
Revised - Amendment(s) - April 11, 2022
Enrolled - May 9, 2022
Revised - Amendment(s) - May 9, 2022
Revised - Budget Information - May 10, 2022

Analysis by: Richard L. Duncan

Direct Inquiries to:
(410) 946-5510
(301) 970-5510

Appendix – Cybersecurity

Cybersecurity Issues in the Nation and State

In recent years, cybersecurity and privacy issues have received significant attention from the general public and policymakers as a result of the many ransomware attacks, data breaches, and other cyberattacks that have taken place in the nation and the State. Globally, from 2019 through 2021, the Center for Strategic and International Studies identified over 300 cyberattacks and data breaches (many of which involved the United States) involving (1) government agencies; (2) defense and high-tech companies; or (3) economic crimes with losses of more than $1 million.

Maryland governmental entities have often been the victim of significant cyberattacks in recent years. For example:

- in 2019, (1) Baltimore City government's computer systems were infected with ransomware that made the systems inaccessible and unavailable for weeks and (2) the Maryland Department of Labor's licensing database was breached; the personal identifiable information (PII) of as many as 78,000 licensees may have been accessed by the hackers;
- in November 2020, Baltimore County Public Schools' information technology (IT) systems were made unusable by a ransomware attack; and
- in 2021, (1) multiple southern Maryland towns lost computer access after a third-party vendor was the victim of a ransomware attack and (2) the Maryland Department of Health was the victim of a cyberattack, resulting in the delay of pandemic data and other information.

Additionally, in November 2021, the Virginia Legislature was the victim of a ransomware attack.

Cybersecurity Governance – Generally

In June 2019, the Governor signed Executive Order 01.01.2019.07, which creates the Maryland Cyber Defense Initiative to strengthen the State's ability to manage the effects of a cybersecurity incident. The initiative creates the Office for Security Management within the Department of Information Technology (DoIT) and charges the office with responsibility for the direction, coordination, and implementation of an overall cybersecurity strategy for all Executive Branch IT systems. The office is led by the State chief information security officer (SCISO), who is appointed by the Governor. The order

also established the Maryland Cybersecurity Coordinating Council to assist SCISO and the office in their duties.

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

Recent State Action

During the 2021 legislative session, multiple pieces of legislation were enacted to enhance State cybersecurity and resilience.

- Chapter 218 of 2021 requires the Secretary of Information Technology to consult with the Attorney General to oversee a consistent cybersecurity strategy specifically for the Executive Branch.
- Chapter 683 of 2021 establishes the Center for Cybersecurity at the University of Maryland Baltimore County in order to provide research and support for cybersecurity-related activities.
- Chapter 425 of 2021 expands the list of network-related prohibited acts on a broad array of computer networks in the State. Chapter 425 also prohibits a person from performing acts to impair network functioning, including exceeding authorized network access and distributing valid access codes to unauthorized persons, on public school or health care facility networks.

In July 2021, the Governor announced several new cybersecurity measures that his office will be undertaking, including (1) a new partnership with the National Security Agency; (2) a memorandum of understanding with the University of Maryland Baltimore County to establish the Maryland Institute of Innovative Computing; and (3) an executive order creating a statewide privacy framework to govern the manner in which the State secures the PII of its citizens.

Maryland Cybersecurity Council Study

The Maryland Cybersecurity Council is required to work with the National Institute of Standards and Technology, as well as other federal agencies, private-sector businesses, and private cybersecurity experts to address State cybersecurity issues. Over the 2021 interim, a council workgroup conducted a review and study of the State's cybersecurity governance and resilience. Through the study, the workgroup developed numerous recommendations for the State to improve and enhance its system. The recommendations include codifying the aforementioned executive order that established the Maryland Cyber Defense Initiative

and centralizing State cybersecurity and IT governance within DoIT. The workgroup's final report is expected to be released during the 2022 legislative session.

Cybersecurity Legislation in Other States

The National Conference of State Legislatures advises that 45 states, the District of Columbia, and Puerto Rico introduced or considered over 250 bills or resolutions that dealt significantly with cybersecurity in 2021. Some of the key cybersecurity issues considered included:

- requiring government agencies to implement training or specific types of security policies and practices and improving incident response and preparedness;
- increasing penalties for computer crime or addressing specific crimes, *e.g.*, ransomware;
- regulating cybersecurity within the insurance industry or addressing cybersecurity insurance;
- creating task forces, councils, or commissions to study or advise on cybersecurity issues; and
- supporting programs or incentives for cybersecurity training and education.

Federal Action

On October 8, 2021, President Joseph R. Biden, Jr., signed the K-12 Cybersecurity Act into law in response to cybersecurity attacks directed at schools. Narrow in scope, the law directs the federal Cybersecurity and Infrastructure Security Agency (CISA) to examine cybersecurity-related risks exclusive to K-12 educational settings. The Director of Cybersecurity and Infrastructure Security must conduct a study and make recommendations specific to K-12 related cybersecurity risks.

Additionally, the Infrastructure Investment and Jobs Act was signed into law on November 15, 2021. Related to cybersecurity, the act established a cyber grant program within the Federal Emergency Management Agency that must be managed in consultation with CISA. Through the program, $1 billion will be distributed to state and local governments over four years; however, to receive a grant, states must submit a cybersecurity plan to the Department of Homeland Security, establish a planning committee before grants are received, and match a portion of the funding provided over the grant program. Grant funding may not be used for ransomware attack payments, to supplant other funding, or for any noncyber purpose.