HB 1130

Department of Legislative Services

Maryland General Assembly
2022 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 1130 (Delegate Pendergrass)
Health and Government Operations

Health Occupations - Prohibition on Expiration of Licenses, Certificates, Permits, and Registrations

This emergency bill prohibits the licenses, certificates, permits, and registrations issued by health occupations boards before December 4, 2021 (the date the Maryland Department of Health (MDH) experienced a cybersecurity attack) from expiring and requires such credentials to remain effective until the Department of Information Technology (DoIT) restores the systems and servers of the health occupations boards that were impacted by the cybersecurity attack. DoIT must notify the Department of Legislative Services within five days after restoring all the affected systems and servers.

Fiscal Summary

State Effect: The bill is not anticipated to materially affect State operations and finances, as discussed below.

Local Effect: The bill does not directly affect local government operations or finances.

Small Business Effect: Minimal.

Analysis

Current Law: Twenty health occupations boards share responsibility for regulating various health professions in Maryland. The boards are responsible for the examination, licensure, certification, or registration; regulation; and discipline of more than 388,000 health care providers. Additionally, the boards set standards of practice and continuing education requirements. The boards charged with regulating health care professionals are generally funded through various fees, including license fees and registration fees. Most

boards regulate 5,000 or fewer active licensees, registrants, and certificate holders; however, this number ranges from about 500 (for the Board of Podiatric Medical Examiners) to about 240,000 (for the Board of Nursing).

In 2021, MDH was the victim of a cybersecurity attack that caused disruptions to some of its operations. For more information on cybersecurity incidents in the State and nation, please see the **Appendix – Cybersecurity.**

State Fiscal Effect: The bill's prohibition on the expiration of licenses, certificates, permits, and registrations issued by health occupations boards prior to December 4, 2021, is not anticipated to materially affect board operations or finances. Several health occupations boards advise that they have been able to promptly process initial and renewal applications for licenses and certifications despite the cybersecurity attack, and there is currently no significant backlog of applications. It is unclear if these boards may continue to *renew* licenses under the bill or if renewals must cease until all system and servers are restored. To the extent that it takes several more months to restore MDH's systems and servers and credentials remain active, renewal fee revenues that would have been collected in fiscal 2023 may instead be collected in fiscal 2024.

Additional Information

Prior Introductions: None.

Designated Cross File: None.

Information Source(s): Maryland Department of Health; Department of Information Technology; Department of Legislative Services

Fiscal Note History: First Reader - March 1, 2022
fnu2/jc

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.