The State of Maryland

Executive Department

EXECUTIVE ORDER
01.01.2019.07

Maryland Cyber Defense Initiative

WHEREAS, The State of Maryland ("State") is susceptible to a wide range of threats and hazards, including cyberattacks on the Executive Branch of State government ("State Government");

WHEREAS, The State stores and processes a large volume of sensitive data and has a responsibility to its citizens and other data owners to protect the confidentiality, availability, and integrity of this data;

WHEREAS, There is an increase in the volume and technical capabilities of malicious actors seeking to negatively impact the confidentiality, integrity, and availability of State systems and data;

WHEREAS, The State must maximize the security of the State's information technology ("IT") environment to limit potential negative impacts to the confidentiality, integrity, and availability of State data and systems;

WHEREAS, The Department of Information Technology has the authority to set policy and provide guidance and oversight for the security of all State IT systems in accordance with Title 3a, Subtitle 3, of the State Finance and Procurement Article of the Code of Maryland;

WHEREAS, A unified, statewide cybersecurity program is necessary to ensure that State Government agencies are managing systems and data in a consistent, secure manner; and

WHEREAS, It is necessary for State Government to maintain and constantly improve and adapt plans to combat these threats and hazards, and to implement such plans effectively;

NOW, THEREFORE, I, LAWRENCE J. HOGAN, JR., GOVERNOR OF THE STATE OF MARYLAND, BY VIRTUE OF THE POWER INVESTED IN ME BY THE CONSTITUTION AND THE LAWS OF MARYLAND, DECLARE THE FOLLOWING, EFFECTIVE IMMEDIATELY:

A. There is a Maryland Cyber Defense Initiative to strengthen the State's ability to manage the consequences of a cybersecurity incident.

B. State Chief Information Security Officer.

1. There is a State Chief Information Security Officer ("SCISO").

2. The SCISO shall be appointed by, and serve at the pleasure of, the Governor.

3. The SCISO shall report to, and be supervised by, the Secretary of Information Technology and serve as the Department of Information Technology ("DoIT") chief information security officer.

4. The SCISO shall provide cybersecurity advice, recommendations, and consultation to the Governor when requested.

C. Office of Security Management.

1. There is an Office of Security Management within DoIT that is managed and supervised by the SCISO.

2. The Office is responsible for the direction, coordination, and implementation of the overall cybersecurity strategy and policy for the Executive Branch of State government ("State Government"), including, but not limited to:

i. Standards to categorize all information and information systems collected or maintained by or on behalf of each unit of State Government;

ii. Guidelines governing the types of information and information systems to be included in each category;

iii. Security requirements (i.e., management, operational, and technical controls) for information and information systems in each category;

iv. Assessing the categorization of systems and data, and the associated implementation of information security requirements;

v. Determining whether a system should be allowed to continue to operate or be connected to the network created pursuant to § 3A-404 of the State Finance and Procurement Article of the Code of Maryland if the SCISO concludes that there are security vulnerabilities or deficiencies in the implementation of information security requirements;

vi. Management of security awareness training for all appropriate employees of State Government;

vii. Assisting in the development of data management, data governance, and data specification standards to promote standardization and reduce risk; and

viii. Assisting in the development of a digital identity standard and specification applicable to all parties communicating, interacting, or conducting business with or on behalf of State Government.

D. Maryland Cybersecurity Coordinating Council.

1. There is a Maryland Cybersecurity Coordinating Council ("MCCC").

2. The MCCC shall provide advice and recommendations to the SCISO about:

i. The strategy and implementation of cybersecurity initiatives and recommendations; and

ii. Building and sustaining the State's capability to identify, mitigate, and detect cybersecurity risk, and respond to and recover from cybersecurity-related incidents.

3. Each of the following State officials, or a senior staff member designated by each official, shall be a member of the MCCC:

i. The Director of the Governor's Office of Homeland Security;

ii. The Secretary of Budget and Management;

iii. The Secretary of General Services;

iv. The Secretary of Human Services;

v. The Secretary of Public Safety and Correctional Services;

vi. The Secretary of Health;

vii. The Adjutant General;

viii. The Director of the Maryland Emergency Management Agency;

ix. The Superintendent of State Police; and

x. The Secretary of Transportation.

4. The Chair of the MCCC is the SCISO.

5. The MCCC shall meet at least quarterly upon request of the Chair.

6. The MCCC may consult with outside experts, including but not limited to experts in the private sector, government agencies, and institutions of higher education.

GIVEN Under My Hand and the Great Seal of the State of Maryland, in the City of Annapolis, this 18h day of June, 2019.

Lawrence J. Hogan, Jr.
Governor

ATTEST:

John C. Wobensmith
Secretary of State