Office of
The Governor

No. 25 FY 20/21
DATE January 13, 2021

AN ORDER ESTABLISHING THE STATE OF MAINE CYBERSECURITY ADVISORY COUNCIL

WHEREAS, information systems, networks and critical infrastructure around the country are threatened by increasing and ever more sophisticated cyber threats and attacks;

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

WHEREAS, the continuous and efficient operation of State Government information systems is both vital and necessary to the mission of providing government services in Maine, and the responsibility for the security of these systems is overseen by the Chief Information Officer;

WHEREAS, the advancing complexity and increasing incidence of cyber threats and attacks demands heightened levels of coordination, information sharing, emergency response capabilities among federal, state, and local government entities to protect the State's computer networks and critical infrastructure systems from such threats; and

WHEREAS, strengthening the State of Maine's information systems, networks, and critical infrastructure against a broad range of cybersecurity risks will improve the State's preparation and response capabilities and better prepare the State to leverage federal cybersecurity resources that may become available;

NOW, THEREFORE, I, Janet T. Mills, Governor of the State of Maine, pursuant to *Me. Const. Art V, Pt 1, §1 and §12*, do hereby Order the following.

I. ESTABLISHMENT AND PURPOSE

The State of Maine Cybersecurity Advisory Council ("Council") is hereby established. The purpose of the Council is to strengthen the security and resiliency of the State's information

technology infrastructure to protect against cybersecurity risks and ensure an effective cybersecurity communication chain to the Governor's Office. To that end, the Council shall:

A. Formalize strategic cybersecurity partnerships at the federal and state level to synchronize defenses and cybersecurity planning strategies, as well as strengthen communication and coordination of information-sharing efforts;
B. Regularly examine threats and vulnerabilities of State information assets;
C. Support the development of statewide policies and procedures that bolster and align the State's cybersecurity framework and governance structure with national best practices, including those developed by the National Institute of Standards and Technology;
D. Develop and sustain the State's capability to identify, mitigate, and detect cybersecurity risks, as well as respond to and recover from cybersecurity- related incidents;
E. Participate in activities coordinated by the Chief Information Officer to understand better and address security incidents and critical cyber security threats to the State, including proven cyber defense measures for government services, critical infrastructure, vulnerability identification, and prioritization strategies and operational response and mitigation tools;
F. Provide recommendations focused on narrowing the cybersecurity workforce gap and developing a talent pipeline in fields involving cybersecurity;
G. Provide advice and recommendations for opportunities to align and integrate cybersecurity strategies within the State's overall strategic planning efforts;
H. Work collaboratively with the Homeland Security Advisory Council, as established in Title 37-B MRSA § 708, to identify cyber threats and align emergency and cyber response and recovery operations; and
I. Present recommendations to the Governor and Cabinet as needed.

All State agencies shall fully cooperate with this Executive Order and are instructed to comply with the following requirements:

A. Ensure compliance with the State's information security policies and procedures to provide optimal cybersecurity for State information assets in their custody;
B. Any State-owned devices, or devices on the State of Maine network that handle Executive Branch information assets are subject to approval by the Office of Information Technology (OIT);
C. OIT will partner with agencies and departments of the Executive Branch to deliver appropriate Security Awareness Training content customized for individual agencies and departments;
D. All personnel and any other individual with access to State information assets must complete the targeted biannual OIT Security Awareness Training; and
E. Review their processes for the collection and/or storage of sensitive personally identifiable information and determine if their agency is adequately resourced to manage its cybersecurity risks.

II. MEMBERSHIP

The Council shall consist of persons appointed by the Governor, with recommendations from the Chief Information Officer, including designees from the Departments of Administrative and Financial Services, Defense, Veterans and Emergency Management,

and Public Safety; the Chief Information Officer; the Chief Information Security Officer; as well as a designee of the Maine National Guard, the University of Maine System and the Office of the Governor. The Chief Information Officer may solicit participation from additional relevant federal, state, and local government representatives, business and industry representatives, and legislative staff, as necessary and appropriate. Members shall not receive compensation for their services.

III. MEETINGS

The Chief Information Officer shall serve as Chair. The Council shall meet at the call of the Chair. The Council shall issue an annual report and recommendations to the Governor. Meetings of the Council are not public proceedings for purposes of Title 1, chapter 13.

IV. OTHER

This order repeals and supersedes *Executive Orders 2014-0003* and *2016-006*.

V. EFFECTIVE DATE

The effective date of this Order is January 13, 2021.

Janet T. Mills
Governor