3A V.S.A. § 3-83

Current through Act Nos. 104 and M-21 of the 2023 Adjourned Session of the 2023-2024 Vermont General Assembly

Vermont Statutes Annotated > TITLE 3A Executive Orders (Chs. 1 — 33) > Chapter 3. Executive (§§ 3-1 — 3-97)

Executive Order No. 3-83 (No. 18-17) [Governor's Cybersecurity Advisory Team]

WHEREAS, increasingly sophisticated cyber attacks aimed at breaching and damaging essential computer networks, infrastructure, and operations in Vermont represent major security risks and increase the State's vulnerability to adverse economic impacts, life-threatening institutional disruption, critical infrastructure damage, privacy violations and identify theft; and

WHEREAS, the advancing complexity and incidence of these cyber attacks demands heightened levels of coordination, information sharing, preparation and emergency response capabilities among State government and federal agencies, local governments, tribal governments, utilities, private companies, academic institutions, and other entities in order to protect computer networks and critical infrastructure systems from damage or unauthorized access; and

WHEREAS, Vermont State government agencies protect the State's computer networks and investigate criminal attacks on State computer networks and critical infrastructure systems under current State law.

NOW THEREFORE, BE IT RESOLVED, that I, Philip B. Scott, by virtue of the authority vested in me as Governor, do hereby create the Governor's Cybersecurity Advisory Team, as follows:

I. Composition and Appointments.

The Cybersecurity Advisory Team shall consist of not more than 10 members to be appointed by the Governor from inside and outside of State government. The State members shall include the State's Chief Information Security Officer, the State Chief Information Officer, the Governor's Homeland Security Advisor or designee, a representative from the Vermont National Guard, the Attorney General or designee, and a representative from Vermont Emergency Management. Non-State members may include leaders from the utilities sector, higher education, health care and business. The Cybersecurity Advisory Team may, in its discretion, establish inter-agency working groups to support its mission, drawing membership from any agency or department of State government. The Cybersecurity Advisory Team may also, in its discretion, consult with private sector professionals and those from other states, the federal government and municipalities for information and advice on issues related to the Team's charge as set forth herein.

The Cybersecurity Advisory Team shall receive administrative and staff support from the Secretary of Digital Services and legal support from the Governor's Counsel and the Department of Public Safety.

II. Cybersecurity Advisory Team Charge and Process.

The Cybersecurity Advisory Team will be advisory to the Governor on the State's Cybersecurity posture. The Cybersecurity Advisory Team shall meet at the call of the Chair, but not less frequently than quarterly, beginning October 15, 2017. The focus of the Cybersecurity Advisory Team shall be to:

A. Develop a strategic plan for protecting State of Vermont public sector and private sector information and systems;

B. Formally evaluate statewide Cybersecurity readiness and develop best practices for policies and procedures to strengthen administrative, technical and physical Cybersecurity safeguards as a resource for State government, Vermont businesses and the public;

C. Build strong relationships and lines of communications among the State government, federal government, and the private sector designed to ensure resilience of electronic information systems;

D. Build strong partnerships with local universities and colleges in order to leverage Cybersecurity resources; and

E. Identify and advise on opportunities to:

1. Ensure Vermont promotes, attracts and retains a highly-skilled Cybersecurity workforce;

2. Raise citizen awareness through outreach and public service announcements;

3. Provide technical capabilities, training, and advice to local government and the private sector;

4. Provide expertise to the State Legislature regarding statutory language that could further protect critical assets, infrastructure, services and personally identifiable information;

5. Advise on strategic, operational and budgetary impacts to the State; and

6. Engage State and federal partners in assessing and managing risk.

III. Effective Date.

This Executive Order shall take effect upon execution.

Dated October 10, 2017