

## **Md. Public Safety Code Ann. § 14-104.1**

Current through all legislation from the 2023 Regular Session of the General Assembly.

*Michie's™ Annotated Code of Maryland > Public Safety (Titles 1 — 15) > Title 14. Emergency Management. (Subts. 1 — 13) > Subtitle 1. Maryland Emergency Management Act. (§§ 14-101 — 14-117)*

### **§ 14-104.1. Cyber Preparedness Unit — Responsibilities — Reporting cybersecurity incidents — Administrator positions.**

---

**(a)**

- (1)** In this section the following words have the meanings indicated.
- (2)** “Local government” includes local school systems, local school boards, and local health departments.
- (3)** “Unit” means the Cyber Preparedness Unit.

**(b)**

- (1)** There is a Cyber Preparedness Unit in the Department.
- (2)** In coordination with the State Chief Information Security Officer, the Unit shall:
  - (i)** support local governments in developing a vulnerability assessment and cyber assessment, including providing local governments with the resources and information on best practices to complete the assessments;
  - (ii)** develop and regularly update an online database of cybersecurity training resources for local government personnel, including technical training resources, cybersecurity continuity of operations templates, consequence management plans, and trainings on malware and ransomware detection;
  - (iii)** assist local governments in:
    1. the development of cybersecurity preparedness and response plans;
    2. implementing best practices and guidance developed by the State Chief Information Security Officer; and
    3. identifying and acquiring resources to complete appropriate cybersecurity vulnerability assessments;
  - (iv)** connect local governments to appropriate resources for any other purpose related to cybersecurity preparedness and response;
  - (v)** as necessary and in coordination with the National Guard, local emergency managers, and other State and local entities, conduct regional cybersecurity preparedness exercises; and

(vi) establish regional assistance groups to deliver and coordinate support services to local governments, agencies, or regions.

(3) The Unit shall support the Office of Security Management in the Department of Information Technology during emergency response efforts.

(c)

(1) Each local government shall 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 in the Department of Information Technology and to the Maryland Joint Operations Center in the Department in accordance with paragraph (2) of this subsection.

(2) For the reporting of cybersecurity incidents under paragraph (1) of this subsection, the State Chief Information Security Officer shall determine:

(i) the criteria for determining when an incident must be reported;

(ii) the manner in which to report; and

(iii) the time period within which a report must be made.

(3) The State Security Operations Center shall immediately notify appropriate agencies of a cybersecurity incident reported under this subsection through the State Security Operations Center.

(d)

(1) Five Position Identification Numbers (PINs) shall be created for the purpose of hiring staff to conduct the duties of the Maryland Department of Emergency Management Cybersecurity Preparedness Unit.

(2) For fiscal year 2024 and each fiscal year thereafter, the Governor shall include in the annual budget bill an appropriation of at least:

(i) \$220,335 for 3 PINs for Administrator III positions; and

(ii) \$137,643 for 2 PINs for Administrator II positions.

## History

---

2022, ch. 135, § 5; ch. 241, § 2.

Michie's™ Annotated Code of Maryland  
Copyright © 2024 All rights reserved.