Md. Public Safety Code Ann. § 14-104.2

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)

§ 14-104.2. Local Cybersecurity Support Fund — Purpose — Funding — Eligibility for assistance.

(a)

(1) In this section the following words have the meanings indicated.

(2) "Fund" means the Local Cybersecurity Support Fund.

(3) "Local government" includes local school systems, local school boards, and local health departments.

(b)

(1) There is a Local Cybersecurity Support Fund.

(2) The purpose of the Fund is to:

(i) provide financial assistance to local governments to improve cybersecurity preparedness, including:

1. updating current devices and networks with the most up-to-date cybersecurity protections;

2. supporting the purchase of new hardware, software, devices, and firewalls to improve cybersecurity preparedness;

3. recruiting and hiring information technology staff focused on cybersecurity;

4. paying outside vendors for cybersecurity staff training;

5. conducting cybersecurity vulnerability assessments;

6. addressing high-risk cybersecurity vulnerabilities identified by vulnerability assessments;

7. implementing and maintaining integrators and other similar intelligence sharing infrastructure that enable connection with the Information Sharing and Analysis Center in the Department of Information Technology; and

8. supporting the security of local wastewater treatment plants, including bicounty, county, and municipal plants, by acquiring or implementing cybersecurity-related upgrades to the plants; and

(ii) assist local governments applying for federal cybersecurity preparedness grants.

(3) The Secretary shall administer the Fund.

(4)

(i) The Fund is a special, nonlapsing fund that is not subject to § 7-302 of the State Finance and Procurement Article.

(ii) The State Treasurer shall hold the Fund separately, and the Comptroller shall account for the Fund.

(5) The Fund consists of:

(i) money appropriated in the State budget to the Fund;

(ii) interest earnings; and

(iii) any other money from any other source accepted for the benefit of the Fund.

(6) The Fund may be used only:

(i) to provide financial assistance to local governments to improve cybersecurity preparedness, including:

1. updating current devices and networks with the most up-to-date cybersecurity protections;

2. supporting the purchase of new hardware, software, devices, and firewalls to improve cybersecurity preparedness;

3. recruiting and hiring information technology staff focused on cybersecurity;

4. paying outside vendors for cybersecurity staff training;

5. conducting cybersecurity vulnerability assessments;

6. addressing high-risk cybersecurity vulnerabilities identified by vulnerability assessments;

7. implementing or maintaining integrators and other similar intelligence sharing infrastructure that enable connection with the Information Sharing and Analysis Center in the Department of Information Technology; and

8. supporting the security of local wastewater treatment plants, including bicounty, county, and municipal plants, by acquiring or implementing cybersecurity-related upgrades to the plants;

(ii) to assist local governments applying for federal cybersecurity preparedness grants; and

(iii) for administrative expenses associated with providing the assistance described under item (i) of this paragraph.

(7)

(i) The State Treasurer shall invest the money of the Fund in the same manner as other State money may be invested.

(ii) Any interest earnings of the Fund shall be credited to the Fund.

(8) Expenditures from the Fund may be made only in accordance with the State budget.

(c) To be eligible to receive assistance from the Fund, a local government shall:

(1) provide proof to the Department of Information Technology that the local government conducted a cybersecurity preparedness assessment in the previous 12 months; or

(2) within 12 months undergo a cybersecurity preparedness assessment provided by, in accordance with the preference of the local government:

(i) the Department of Information Technology at a cost to the local government that does not exceed the cost to the Department of Information Technology of providing the assessment; or

(ii) a vendor authorized by the Department of Information Technology to complete cybersecurity preparedness assessments.

History

2022, ch. 243, § 1.

End of Document