

Md. State Finance and Procurement Code Ann. § 3.5-2A.04

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

Michie's™ Annotated Code of Maryland > State Finance and Procurement (Divs. I — II) > Division I. State Finance. (Titles 1 — 10A) > Title 3.5. Department of Information Technology. (Subts. 1 — 7) > Subtitle 2A. Office of Security Management. (§§ 3.5-2A-01 — 3.5-2A-06)

§ 3.5-2A-04. Office responsibilities — Duties — Regional assistance — Annual reports — Items included.

(a)

(1) The Office is responsible for:

- (i)** the direction, coordination, and implementation of the overall cybersecurity strategy and policy for units of State government; and
- (ii)** supporting and coordinating with the Maryland Department of Emergency Management Cyber Preparedness Unit during emergency response efforts.

(2) The Office is not responsible for the information technology installation and maintenance operations normally conducted by a unit of State government, a unit of local government, a local school board, a local school system, or a local health department.

(b) The Office shall:

- (1)** establish standards to categorize all information collected or maintained by or on behalf of each unit of State government;
- (2)** establish standards to categorize all information systems maintained by or on behalf of each unit of State government;
- (3)** develop guidelines governing the types of information and information systems to be included in each category;
- (4)** establish security requirements for information and information systems in each category;
- (5)** assess the categorization of information and information systems and the associated implementation of the security requirements established under item (4) of this subsection;
- (6)** if the State Chief Information Security Officer determines that there are security vulnerabilities or deficiencies in any information systems, determine and direct or take actions necessary to correct or remediate the vulnerabilities or deficiencies, which may include requiring the information system to be disconnected;
- (7)** if the State Chief Information Security Officer determines that there is a cybersecurity threat caused by an entity connected to the network established under § 3.5-404 of this title

that introduces a serious risk to entities connected to the network or to the State, take or direct actions required to mitigate the threat;

(8) manage security awareness training for all appropriate employees of units of State government;

(9) assist in the development of data management, data governance, and data specification standards to promote standardization and reduce risk;

(10) assist in the development of a digital identity standard and specification applicable to all parties communicating, interacting, or conducting business with or on behalf of a unit of State government;

(11) develop and maintain information technology security policy, standards, and guidance documents, consistent with best practices developed by the National Institute of Standards and Technology;

(12) to the extent practicable, seek, identify, and inform relevant stakeholders of any available financial assistance provided by the federal government or non-State entities to support the work of the Office;

(13) provide technical assistance to localities in mitigating and recovering from cybersecurity incidents; and

(14) provide technical services, advice, and guidance to units of local government to improve cybersecurity preparedness, prevention, response, and recovery practices.

(c) The Office, in coordination with the Maryland Department of Emergency Management, shall:

(1) assist local political subdivisions, including counties, school systems, school boards, and local health departments, in:

(i) the development of cybersecurity preparedness and response plans; and

(ii) implementing best practices and guidance developed by the Department; and

(2) connect local entities to appropriate resources for any other purpose related to cybersecurity preparedness and response.

(d) The Office, in coordination with the Maryland Department of Emergency Management, may:

(1) conduct regional exercises, as necessary, in coordination with the National Guard, local emergency managers, and other State and local entities; and

(2) establish regional assistance groups to deliver or coordinate support services to local political subdivisions, agencies, or regions.

(e)

(1) On or before December 31 each year, the Office shall report to the Governor and, in accordance with § 2-1257 of the State Government Article, the Senate Budget and Taxation Committee, the Senate Education, Health, and Environmental Affairs Committee, the House Appropriations Committee, the House Health and Government Operations Committee, and the Joint Committee on Cybersecurity, Information Technology, and Biotechnology on the activities of the Office and the state of cybersecurity preparedness in Maryland, including:

- (i) the activities and accomplishments of the Office during the previous 12 months at the State and local levels; and
 - (ii) a compilation and analysis of the data from the information contained in the reports received by the Office under § 3.5-405 of this title, including:
 - 1. a summary of the issues identified by the cybersecurity preparedness assessments conducted that year;
 - 2. the status of vulnerability assessments of all units of State government and a timeline for completion and cost to remediate any vulnerabilities exposed;
 - 3. recent audit findings of all units of State government and options to improve findings in future audits, including recommendations for staff, budget, and timing;
 - 4. analysis of the State's expenditure on cybersecurity relative to overall information technology spending for the prior 3 years and recommendations for changes to the budget, including amount, purpose, and timing to improve State and local cybersecurity preparedness;
 - 5. efforts to secure financial support for cyber risk mitigation from federal or other non-State resources;
 - 6. key performance indicators on the cybersecurity strategies in the Department's information technology master plan, including time, budget, and staff required for implementation; and
 - 7. any additional recommendations for improving State and local cybersecurity preparedness.
- (2) A report submitted under this subsection may not contain information that reveals cybersecurity vulnerabilities and risks in the State.

History

2022, ch. 241, § 2; ch. 242, § 2.

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