Md. State Finance and Procurement Code Ann. § 3.5-406

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 4. Telecommunications. (§§ 3.5-401 — 3.5-407)

§ 3.5-406. Annual reports — Items included — Cybersecurity preparedness assessments performed — Cybersecurity incidents.

(a) On or before December 1 each year, each unit of State government shall:

(1) report the results of any cybersecurity preparedness assessments performed in the prior year to the Office of Security Management in accordance with guidelines developed by the Office; and

(2) submit a report to the Governor and the Office of Security Management that includes:

(i) an inventory of all information systems and applications used or maintained by the unit;

(ii) a full data inventory of the unit;

(iii) a list of all cloud or statistical analysis system solutions used by the unit;

(iv) a list of all permanent and transient vendor interconnections that are in place;

(v) the number of unit employees who have received cybersecurity training;

(vi) the total number of unit employees who use the network;

(vii) the number of information technology staff positions, including vacancies;

(viii) the number of noninformation technology staff positions, including vacancies;

(ix) the unit's information technology budget, itemized to include the following categories:

1. services;

2. equipment;

3. applications;

4. personnel;

5. software licensing;

6. development;

7. network projects;

8. maintenance; and

9. cybersecurity;

(x) any major information technology initiatives to modernize the unit's information technology systems or improve customer access to State and local services;

(xi) the unit's plans for future fiscal years to implement the unit's information technology goals;

(xii) compliance with timelines and metrics provided in the Department's master plan; and

(xiii) any other key performance indicators required by the Office of Security Management to track compliance or consistency with the Department's statewide information technology master plan.

(b)

(1) Each unit of State government shall report a cybersecurity incident in accordance with paragraph (2) of this subsection to the State Chief Information Security Officer.

(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.

History

2022, ch. 242, § 2.

End of Document