

Department of Planning and Budget 2024 Session Fiscal Impact Statement

1. **Bill Number:** SB222

House of Origin Introduced Substitute Engrossed
Second House In Committee Substitute Enrolled

2. **Patron:** McGuire

3. **Committee:** General Laws and Technology

4. **Title:** Commonwealth information security requirements.

5. **Summary:** Requires state public bodies, defined in the bill, to (i) comply with the Commonwealth's security policies and standards, (ii) ensure each of its employees completes information security training, (iii) conduct regular security audits, and (iv) report the results of such audits to the appropriate entity. The bill directs the Chief Information Officer of the Commonwealth to (a) publish and maintain a list of the Commonwealth's security policies and standards with which state public bodies are required to comply, (b) ensure that transition meetings with state public bodies occur, and (c) document such transitions and any exemptions from the requirements of the bill.

6. **Budget Amendment Necessary:** Preliminary, see Item 8.

7. **Fiscal Impact Estimates:** Preliminary, see Item 8.

8. **Fiscal Implications:** The fiscal impact of this legislation is indeterminate. To the extent that the cyber security programs at state public bodies which are not currently under Virginia Information Technologies Agency's (VITA) program meet or exceed VITA's requirements, then little to no additional resources may be required. If those programs are currently below VITA's requirements, then additional resources may be required, but the amount would be dependent on the public body in question and the state of their existing cyber security program. Executive branch agencies should not require any additional resources, because they are already required to meet the provisions of this bill. However, legislative and judicial agencies, higher education institutions, and authorities will be the most affected by this legislation and may require varying levels of additional resources if any.

The legislative branch currently has a minimum of 30 sensitive systems that would require regular security audits. The Auditor of Public Accounts (APA) indicates that a single system audit costs between \$30K- \$50K each, and each system would need to be audited once every 3 years. The APA has indicated that it may be possible to procure single contract for security audits similar to the financial audit contract they currently have, however cost estimates for this are currently unknown.

This legislation contains an enactment clause that requires for state public bodies previously excluded from these requirements to work with the Chief Information Officer to transition and implement the provisions of this bill.

9. Specific Agency or Political Subdivisions Affected: All state public bodies.

10. Technical Amendment Necessary: No

11. Other Comments: Companion to HB1095