

# S.B. NO. 1003

JAN 24 2013

---

## A BILL FOR AN ACT

RELATING TO INFORMATION TECHNOLOGY.

**BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:**

1           SECTION 1. Protecting and securing the State of Hawaii's  
2 information and data is a top concern in today's cyber world.  
3 The State must protect its technology from enemies both outside  
4 and within the State. To ensure the security of state  
5 government information and the data communications  
6 infrastructure from unauthorized uses, intrusions, or other  
7 security threats, the chief information officer should be given  
8 the responsibility and authority to direct the development,  
9 adoption, and implementation of policies, procedures, and  
10 standards and training personnel to minimize vulnerability to  
11 threats, regularly assess security risks, determine appropriate  
12 security measures, and perform security audits of government  
13 information systems and data communications infrastructures.

14           The purpose of this Act is to establish policies,  
15 procedures, and standards to identify and require the adoption  
16 of practices to safeguard information systems, data, and  
17 communications infrastructures; define the scope and regularity  
18 of security audits; and which bodies are authorized to conduct

1 security audits, which may include reviews of physical security  
2 practices.

3 SECTION 2. Chapter 27, Hawaii Revised Statutes, is amended  
4 by adding to part VII a new section, to be appropriately  
5 designated and to read as follows:

6 "§27- Additional duties of the chief information officer  
7 relating to security of government information.

8 (a) The chief information officer shall provide for  
9 periodic security audits of all executive branch agencies  
10 regarding the protection of government databases and data  
11 communications.

12 (b) Security audits may include, but are not limited to,  
13 on-site audits as well as reviews of all written security  
14 procedures and documented practices. The chief information  
15 officer may contract with a private firm or firms that  
16 specialize in conducting these audits. All departments,  
17 agencies, boards, or commissions subject to the audits  
18 authorized by this section shall fully cooperate with the entity  
19 designated to perform the audit. The chief information officer  
20 may direct specific remediation actions to mitigate findings of  
21 insufficient administrative, technical, and physical controls

S.B. NO. 1003

1 necessary to protect state government information or data  
2 communication infrastructures.


3 (c) The provisions of this section shall not infringe upon  
4 responsibilities assigned to the state comptroller, the  
5 legislative auditor, or other statutory requirements.

6 SECTION 3. New statutory material is underscored.

7 SECTION 3. This Act shall take effect upon its approval.

8

9

INTRODUCED BY: 

10

BY REQUEST

11

**Report Title:**

Chief Information Officer; Information Technology; Security

**Description:**

Assigns to the Chief Information Officer the responsibility and authority to direct the development, adoption, and training of policies, procedures, and standards to minimize vulnerability to threats, regularly assess security risks, determine appropriate security measures, and perform security audits of government information systems and data communications infrastructures.

*The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.*

JUSTIFICATION SHEET

DEPARTMENT: Accounting and General Services

TITLE: A BILL FOR AN ACT RELATING TO INFORMATION TECHNOLOGY

PURPOSE: The purpose of this bill is to assign the Chief Information Officer the responsibility and authority to direct the development, adoption, and training of policies, procedures, and standards to minimize vulnerability to threats, regularly assess security risks, determine appropriate security measures, and perform security audits of government information systems and data communications infrastructures.

MEANS: Add a new section to part VII of chapter 27, Hawaii Revised Statutes.

JUSTIFICATION: Protecting and securing the State of Hawaii's information and data is a top concern in today's cyber world. The State must protect its technology from enemies both outside and within the State.

Assigning this responsibility to the State Chief Information Officer will ensure the security of state government information and the data communications infrastructure from unauthorized uses, intrusions, or other security threats.

At a minimum, these policies, procedures, and standards shall identify and require the adoption of practices to safeguard information systems, data, and communications infrastructures, as well as define the scope and regularity of security audits and which bodies are authorized to conduct security audits. The audits may include reviews of physical security practices.

Impact on the public: Improved security measures in protecting personal identifiable information, such as social security numbers, birthdates, and financial and banking information.

Impact on the department and other agencies: Improved and standardized policies, procedures, and processes for information assurance and privacy.

GENERAL FUND: None.

OTHER FUNDS: None.

PPBS PROGRAM  
DESIGNATION: AGS 130

OTHER AFFECTED  
AGENCIES: None.

EFFECTIVE DATE: Upon approval.