THE SENATE
THIRTY-SECOND LEGISLATURE, 2023
STATE OF HAWAII

S.B. NO. 1478
S.D. 1
H.D. 1

A BILL FOR AN ACT

RELATING TO OFFENSIVE CYBERSECURITY.

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

SECTION 1. Section 27-41.1, Hawaii Revised Statutes, is amended by adding a new definition to be appropriately inserted and to read as follows:

""Office" means the office of enterprise technology services established pursuant to section 27-43."

SECTION 2. Section 27-43.5, Hawaii Revised Statutes, is amended to read as follows:

"**[~~[~~]§27-43.5[~~]~~] Additional duties of the chief information officer relating to security of government information[~~.~~]; offensive cybersecurity program; establishment; reporting.** (a) The chief information officer shall provide for periodic security audits of all executive branch departments and agencies regarding the protection of government information and data communication infrastructure.

(b) Security audits may include on-site audits as well as reviews of all written security procedures and documented practices. The chief information officer may contract with a private firm or firms that specialize in conducting security audits; provided that information protected from disclosure by federal or state law, including confidential tax information, shall not be disclosed. All executive branch departments, agencies, boards, or commissions subject to the security audits authorized by this section shall fully cooperate with the entity designated to perform the audit. The chief information officer may direct specific remedial actions to mitigate findings of insufficient administrative, technical, and physical controls necessary to protect state government information or data communication infrastructure.

(c) There is established within the office an offensive cybersecurity program, which shall:

(1) Analyze cybersecurity threats;

(2) Evaluate and provide intelligence regarding cybersecurity;

(3) Promote cybersecurity awareness, including awareness of social engineering threats;

(4) Conduct penetration testing among state and county agencies to evaluate the security of state and county information technology systems;

(5) Conduct agent-based security and ensure that assets are being inventoried and managed according to best practices;

(6) Use the common vulnerability scoring system to evaluate the severity of vulnerabilities in information technology systems across state and county agencies and prioritize remediation; and

(7) Take other proactive measures to ensure increased cybersecurity for state and county agencies.

(d) State and county agencies shall disclose to the office an identified or suspected cybersecurity incident that affects the confidentiality, integrity, or availability of information systems, data, or services. Disclosure shall be made expeditiously and without unreasonable delay. Cybersecurity incidents required to be reported include suspected breaches; malware incidents that cause significant damage; denial of service attacks that affect the availability of services; demands for ransom related to a cybersecurity incident or unauthorized disclosure of digital records; instances of identity theft or identity fraud occurring on a state or county agency's information technology system; incidents that require response and remediation efforts that will cost more than $10,000 in equipment, software, and labor; and other incidents the state or county agency deems worthy of communication to the office; provided that:

(1) Until a cybersecurity incident is resolved, a state or county agency shall continue to disclose details regarding a cybersecurity incident to the office, including:

(A) The number of potentially exposed records;

(B) The type of records potentially exposed, including health insurance information, medical information, criminal justice information, regulated information, financial information, and personal information;

(C) Efforts the state or county agency is undertaking to mitigate and remediate the damage of the incident to the agency and other affected agencies; and

(D) The expected impact of the incident, including:

(i) The disruption of the state or county agency's services;

(ii) The effect on customers and employees that experienced data or service losses; and

(iii) Other concerns that could potentially disrupt or degrade the confidentiality, integrity, or availability of information systems, data, or services that may affect the State or a county; and

(2) The legislative and judicial branches may disclose to the office cybersecurity incidents that affect the confidentiality, integrity, or availability of information systems, data, or services.

(e) The office shall adopt rules pursuant to chapter 91 regarding the procedures and form in which state and county agencies shall disclose cybersecurity incidents to the office.

(f) The office, to the extent possible, shall provide consultation services and other resources to assist state and county agencies and the legislative and judicial branches in responding to and remediating cybersecurity incidents.

(g) No later than twenty days prior to the convening of each regular session, the chief information officer shall submit a report to the legislature that includes:

(1) All disclosed cybersecurity incidents required pursuant to this section;

(2) The status of those cybersecurity incidents; and

(3) Any response or remediation taken to mitigate the cybersecurity incidents.

The office shall ensure that all reports of disclosed cybersecurity incidents are communicated in a manner that protects victims of cybersecurity incidents, prevents unauthorized disclosure of cybersecurity plans and strategies, and adheres to federal and state laws regarding protection of cybersecurity information.

[~~(e)~~] (h) This section shall not infringe upon responsibilities assigned to the comptroller or the auditor by any state or federal law."

SECTION 3. (a) No later than January 1, 2026, the office of enterprise technology services shall:

(1) Complete an initial round of penetration testing on the information technology systems of each state and county agency;

(2) Assess vulnerabilities within those systems using the common vulnerability scoring system; and

(3) Work with state and county agencies to identify and address any vulnerability threats identified having a benchmark score exceeding 3.9 on the common vulnerability scoring system.

(b) No later than twenty days prior to the convening of the regular session of 2026, the office of enterprise technology services shall submit a report to the legislature describing the office's progress in meeting the requirements of this section.

SECTION 4. There is appropriated out of the general revenues of the State of Hawaii the sum of $ or so much thereof as may be necessary for fiscal year 2023-2024 and the sum of $ or so much thereof as may be necessary for fiscal year 2024-2025 for the software, services, and   full-time equivalent (FTE) permanent positions necessary to establish an offensive cybersecurity program.

The sums appropriated shall be expended by the office of enterprise technology services for the purposes of this Act.

SECTION 5. Statutory material to be repealed is bracketed and stricken. New statutory material is underscored.

SECTION 6. This Act shall take effect on June 30, 3000.

S.B. NO. 1478 S.D. 1 H.D. 1

Report Title:
Offensive Cybersecurity Program; Office of Enterprise Technology Services; Report; Positions; Appropriation

Description:
Establishes an offensive cybersecurity program within the office of enterprise technology services to analyze and evaluate cybersecurity threats and increase cybersecurity awareness and education. Establishes a goal for all state and county agencies to identify and address vulnerabilities having a benchmark score exceeding 3.9 on the common vulnerability scoring system by 1/1/2026. Makes appropriations and authorizes the establishment of positions. Requires reports. Effective 6/30/3000. (HD1)

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