

JAN 25 2023

---

---

# A BILL FOR AN ACT

RELATING TO OFFENSIVE CYBERSECURITY.

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

1           SECTION 1. Chapter 27, Hawaii Revised Statutes, is amended  
2 by adding a new subpart to part VII to be appropriately  
3 designated and to read as follows:

4           "Subpart . Offensive Cybersecurity Program

5           **§27-A Definitions.** As used in this subpart:

6           "Agency" means any executive branch agency of the State or  
7 any county agency.

8           "Breach":

9           (1) Means unauthorized access or acquisition of  
10 computerized data that has not been secured by  
11 encryption or other methods or technology that renders  
12 electronic files, media, or databases unreadable or  
13 unusable; and

14           (2) Does not include the good faith acquisition of  
15 personal information by an employee or agent of the  
16 employee if the personal information is not used or  
17 subject to further unauthorized disclosure.



1 "Common vulnerability scoring system" refers to the open  
2 industry standard, which is maintained by the Forum of Incident  
3 Response and Security Teams or a successor entity, for assessing  
4 the severity of computer system security vulnerabilities and  
5 uses a numerical score to help organizations properly assess and  
6 prioritize their vulnerability management processes.

7 "Criminal justice information" means private or sensitive  
8 information collected by federal, state, or county law  
9 enforcement, including:

- 10 (1) Fingerprints or other biometric information;
- 11 (2) Criminal background and investigation information; and
- 12 (3) Personal information.

13 "Cybersecurity" means processes or capabilities, wherein  
14 systems, communications, and information are protected and  
15 defended against damage, unauthorized use or modification, and  
16 exploitation.

17 "Cybersecurity strategy" means a vision, plan of action, or  
18 guiding principles, but does not mean an associated operational  
19 plan.



1 "Denial of service attack" means an attack against a  
2 computer system designed to make the system inaccessible to  
3 users.

4 "Financial information":

5 (1) Means banking, credit, or other account information  
6 that, if accessed without authorization, may result in  
7 potential harm to a person; and

8 (2) Includes account numbers or codes, credit card  
9 expiration dates, credit card security codes, bank  
10 account statements, and records of financial  
11 transactions.

12 "Health insurance information" means a person's health  
13 insurance policy number or subscriber identification number and  
14 any unique identifier used by a health insurer to identify a  
15 person.

16 "Identity theft or identity fraud" means all types of crime  
17 in which a person wrongfully obtains and uses another person's  
18 personal data in a way that involves fraud or deception, most  
19 commonly for economic gain.



1 "Malware":

2 (1) Means software or firmware intended to perform an  
3 unauthorized process that will have an adverse effect  
4 on the confidentiality, integrity, or availability of  
5 an information system; and

6 (2) Includes a virus, worm, trojan horse, spyware, adware,  
7 or other code-based system that infects hosts.

8 "Medical information" means a person's medical history,  
9 mental or physical condition, or medical treatment or diagnosis  
10 by a health care professional.

11 "Office" means the office of enterprise technology  
12 services.

13 "Penetration testing" refers to a method for gaining  
14 assurance in the security of an information technology system by  
15 attempting to breach some or all of that system's security,  
16 using tools and techniques that a bad actor may use.

17 "Personal information":

18 (1) Means a person's first name or first initial and last  
19 name in combination with the following when names and  
20 data are not encrypted:

21 (A) The person's social security number;



- 1 (B) The person's driver's license number;
- 2 (C) The person's Hawaii state identification card
- 3 number;
- 4 (D) The person's financial institution account
- 5 number, credit card number, or debit card number
- 6 in combination with required security codes,
- 7 access codes, or passwords that permit access to
- 8 a person's financial accounts;
- 9 (E) The person's date of birth;
- 10 (F) The maiden name of the person's mother;
- 11 (G) Medical information;
- 12 (H) Health insurance information;
- 13 (I) An identification number assigned to the person
- 14 by the person's employer in combination with
- 15 security codes, access codes, or passwords; or
- 16 (J) The person's digitized or other electronic
- 17 signature; and
- 18 (2) Does not include information available to the public
- 19 from federal, state, or county government records.
- 20 "Ransom" means a payment for services or goods to a
- 21 malicious agent to:



- 1 (1) Decrypt data on a computer system;
- 2 (2) Retrieve lost or stolen data; or
- 3 (3) Prevent the disclosure and dissemination of
- 4 information.

5 "Regulated information" means information and information  
6 technology resource protection requirements established by the  
7 federal government and regulating organizations.

8 "Regulating organizations" means organizations that  
9 establish laws, regulations, policies, guidelines, and  
10 standards, including the Federal Bureau of Investigation,  
11 Internal Revenue Service, Social Security Administration,  
12 Federal Deposit Insurance Corporation, United States Department  
13 of Health and Human Services, Centers for Medicare and Medicaid  
14 Services, and Payment Card Industry Security Standards Council.

15 "Significant damage" means:

- 16 (1) A degradation in or loss of mission capability to an  
17 extent and duration that the agency is not able to  
18 perform one or more of its primary functions;
- 19 (2) Damages of \$10,000 or more to agency assets as  
20 estimated by the agency;



1 (3) A financial loss of \$10,000 or more as estimated by  
2 the agency; or

3 (4) Harm to persons involving loss of life or serious  
4 life-threatening injuries.

5 "Social engineering":

6 (1) Means the tactic of manipulating, influencing, or  
7 deceiving a person to gain control over a computer  
8 system or steal personal or financial information; and

9 (2) Includes the use of psychological manipulation to  
10 trick users into making security mistakes or giving  
11 away sensitive information, such as "phishing" or  
12 baiting.

13 **§27-B Offensive cybersecurity program.** There is  
14 established within the office an offensive cybersecurity  
15 program, which shall:

16 (1) Analyze cybersecurity threats;

17 (2) Evaluate and provide intelligence regarding  
18 cybersecurity;

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



- 1           (4) Conduct penetration testing among state and county  
2                   agencies to evaluate the security of state and county  
3                   information technology systems;
- 4           (5) Conduct agent-based security and ensure that assets  
5                   are being inventoried and managed according to best  
6                   practices;
- 7           (6) Use the common vulnerability scoring system to  
8                   evaluate the severity of vulnerabilities in  
9                   information technology systems across state and county  
10                  agencies and prioritize remediation; and
- 11          (7) Take other proactive measures to ensure increased  
12                  cybersecurity for agencies.

13           **§27-C Memorandums of understanding; mutual aid agreements.**

- 14   (a) The office may enter a:
  - 15           (1) Memorandum of understanding with other state, local,  
16                   or tribal governments of the United States for  
17                   purposes of ensuring the confidentiality,  
18                   availability, and integrity of state, local, and  
19                   tribal information systems and data, including  
20                   consulting, developing cybersecurity strategy,





1 prevention of cybersecurity incidents, and response  
2 strategies to cybersecurity incidents; and

3 (2) A mutual aid agreement with other state, local, or  
4 tribal governments of the United States agreeing to  
5 the reciprocal exchange of resources and services for  
6 mutual benefit of the parties related to cybersecurity  
7 efforts for the purposes of responding to or  
8 mitigating active cybersecurity incidents.

9 (b) As used in this section, "state" means a state of the  
10 United States, the District of Columbia, Puerto Rico, the United  
11 States Virgin Islands, or any territorial or insular possession  
12 subject to the jurisdiction of the United States.

13 **§27-D Disclosures of cybersecurity incidents.** (a) State  
14 and county agencies shall disclose to the office an identified  
15 or suspected cybersecurity incident that affects the  
16 confidentiality, integrity, or availability of information  
17 systems, data, or services. Disclosure shall be made  
18 expediently and without unreasonable delay. Cybersecurity  
19 incidents required to be reported include:

- 20 (1) Suspected breaches;
- 21 (2) Malware incidents that cause significant damage;



1 (3) Denial of service attacks that affect the availability  
2 of services;

3 (4) Demands for ransom related to a cybersecurity incident  
4 or unauthorized disclosure of digital records;

5 (5) Instances of identity theft or identity fraud  
6 occurring on an agency's information technology  
7 system;

8 (6) Incidents that require response and remediation  
9 efforts that will cost more than \$10,000 in equipment,  
10 software, and labor; and

11 (7) Other incidents the agency deems worthy of  
12 communication to the office.

13 (b) Until a cybersecurity incident is resolved, an agency  
14 shall continue to disclose details regarding a cybersecurity  
15 incident to the office, including:

16 (1) The number of potentially exposed records;

17 (2) The type of records potentially exposed, including  
18 health insurance information, medical information,  
19 criminal justice information, regulated information,  
20 financial information, and personal information;



1 (3) Efforts the agency is undertaking to mitigate and  
2 remediate the damage of the incident to the agency and  
3 other affected agencies; and

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

5 (A) The disruption of the agency's services;

6 (B) The effect on customers and employees that  
7 experienced data or service losses; and

8 (C) Other concerns that could potentially disrupt or  
9 degrade the confidentiality, integrity, or  
10 availability of information systems, data, or  
11 services that may affect the State or a county.

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

16 (d) The office shall adopt rules pursuant to chapter 91  
17 regarding the procedures and form in which an agency shall  
18 disclose cybersecurity incidents to the office.

19 (e) The office, to the extent possible, shall provide  
20 consultation services and other resources to assist agencies and



1 the legislative and judicial branches in responding to and  
2 remediating cybersecurity incidents.

3 (f) No later than twenty days prior to the convening of  
4 each regular session, the office shall submit a report to the  
5 legislature that includes:

- 6 (1) All disclosed cybersecurity incidents required  
7 pursuant to this section;
- 8 (2) The status of those cybersecurity incidents; and
- 9 (3) Any response or remediation to mitigate the  
10 cybersecurity incidents.

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

17 **§27-E Rules.** The office may adopt rules pursuant to  
18 chapter 91 necessary to implement the purposes of this chapter."

19 SECTION 2. Chapter 27, Hawaii Revised Statutes, is amended  
20 by designating sections 27-41 to 27-45 as subpart A, entitled  
21 "General Provisions".



1 SECTION 3. (a) No later than January 1, 2025, the office  
2 of enterprise technology services shall:

3 (1) Complete an initial round of penetration testing on  
4 the information technology systems of each agency;

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

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

11 (b) No later than twenty days prior to the convening of  
12 the regular session of 2025, the office of enterprise technology  
13 services shall submit a report to the legislature describing the  
14 office's progress in meeting the requirements of this section.

15 (c) As used in this section, "agency", "common  
16 vulnerability scoring system", and "penetration testing" shall  
17 have the same meanings as in section 128B-A, Hawaii Revised  
18 Statutes.

19 SECTION 4. There is appropriated out of the general  
20 revenues of the State of Hawaii the sum of \$ or so  
21 much thereof as may be necessary for fiscal year 2023-2024 and



1 the same sum or so much thereof as may be necessary for fiscal  
2 year 2024-2025 to:

3 (1) Perform the duties assigned to the office of  
4 enterprise technology services by this Act, including  
5 the creation of an offensive cybersecurity program;  
6 and

7 (2) Establish full-time equivalent ( FTE)  
8 permanent positions necessary to perform the functions  
9 required by this Act.

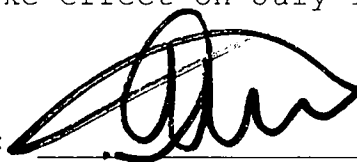
10 The sums appropriated shall be expended by the office of  
11 enterprise technology services for the purposes of this Act.

12 SECTION 5. In codifying the new sections added by  
13 section 1 and referenced in section 3 of this Act, the revisor  
14 of statutes shall substitute appropriate section numbers for the  
15 letters used in designating the new sections in this Act.

16 SECTION 6. This Act shall take effect on July 1, 2023.

17

INTRODUCED BY:

A handwritten signature in black ink, appearing to be "Alu", written over a horizontal line.

**Report Title:**

Offensive Cybersecurity; Office of Enterprise Technology Services; Program; Established; Appropriations

**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. Requires the program to conduct penetration testing of state agencies to identify vulnerabilities and assess the severity of computer system security vulnerabilities using the Common Vulnerability Scoring System. 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 January 1, 2025. Authorizes the Office of Enterprise Technology Services to enter into memorandums of understanding and mutual aid agreements with other governments within the United States. Makes appropriations and authorizes the establishment of positions.

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

