
A BILL FOR AN ACT

RELATING TO INCIDENT RESPONSE.

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

1 SECTION 1. The legislature finds that the State is under
2 constant threat of security breaches and cyber attacks. The
3 State's executive department computer networks provide and
4 control critical services to all of the State's residents.
5 These networks are responsible for operations of the State's
6 financial services, telecommunications, agricultural operations,
7 legal affairs, transportation system, educational and career
8 development programs, health care systems, and public safety
9 response. Protection of these systems is of the utmost
10 importance for the State.

11 The legislature further finds that an incident response
12 plan for each State department prepares the departments to
13 respond in the event a cyber attack occurs. The Hawaii
14 cybersecurity, economic, education, and infrastructure security
15 coordinator oversees cybersecurity and cyber resiliency matters
16 in the State. The legislature further finds that the
17 cybersecurity, economic, education, and infrastructure security



1 coordinator must protect the State through an incident response
2 plan for each executive department in the State that shall work
3 in concert as a comprehensive statewide plan.

4 The purpose of this Act is to require the cybersecurity,
5 economic, education, and infrastructure security coordinator to
6 develop and maintain an incident response plan to cyber attacks
7 for each executive department in the State.

8 SECTION 2. Section 128B-1, Hawaii Revised Statutes, is
9 amended to read as follows:

10 " ~~§128B-1~~ **Cybersecurity, economic, education, and**
11 **infrastructure security coordinator; powers and duties.** (a)

12 There is established the full-time Hawaii cybersecurity,
13 economic, education, and infrastructure security coordinator to
14 oversee cybersecurity and cyber resiliency matters, including
15 cybersecurity, economic, education, and infrastructure security
16 for the State. The coordinator shall be placed within the state
17 department of defense.

18 (b) The coordinator shall be selected by the state
19 adjutant general based on the recommendations of the various
20 agencies, departments, and private entities that will partner
21 with the coordinator.



1 (c) The coordinator shall partner with representatives
2 from the following entities:

- 3 (1) The Hawaii fusion center;
- 4 (2) The Hawaii state cyber resiliency center;
- 5 (3) Federal government agencies;
- 6 (4) State government agencies;
- 7 (5) The counties of the State;
- 8 (6) Institutions of higher education; and
- 9 (7) Other entities within the power, water,
10 communications, transportation, and finance sectors,
11 including public utilities, private telecommunications
12 companies, airlines, financial institutions, and
13 private information technology companies.

14 (d) Notwithstanding any law to the contrary, the
15 coordinator, through its various partnerships, shall develop the
16 requirements and methods for:

- 17 (1) Improving cyber resiliency within the State through
18 the development of a structure that shall include
19 education, cybersecurity, and critical infrastructure
20 protection;



H.B. NO. 2755

- 1 (2) Improving the State's critical infrastructure network
2 and resiliency, including identifying
3 interdependencies of critical infrastructures, points
4 of connection between critical infrastructures, the
5 most critical nodes, and the cascading effects of a
6 cyber-attack on these points of connection between
7 critical infrastructure;
- 8 (3) Improving the State's cybersecurity by using existing
9 resources within the State;
- 10 (4) Examining specific requirements and actions to
11 accelerate the growth of the cybersecurity industry in
12 the State;
- 13 (5) Defining the requirements and opportunities to secure
14 state, federal, and private moneys for cybersecurity
15 activities and related educational programs;
- 16 (6) Forming partnerships to implement cyber resiliency
17 structures and protocol to identify and share
18 information about possible cyber-attacks and mitigate
19 damage and recover quickly and efficiently from cyber-
20 attacks; and



1 (7) Expanding the State's cybersecurity and cyber
2 resiliency understanding and workforce through
3 education.

4 (e) Using the requirements and methods developed under
5 subsection (d), the coordinator, in partnership with the chief
6 information officer, shall develop and maintain an incident
7 report plan for each executive department.

8 ~~(e)~~ (f) The coordinator may request the assistance of
9 other departments, agencies, and private companies, both inside
10 and outside of the State to carry out its duties.

11 ~~(f)~~ (g) For the purposes of this section:

12 "Coordinator" shall mean the Hawaii cybersecurity,
13 economic, education, and infrastructure security coordinator.

14 "Cyber resiliency" shall mean the ability to complete
15 vulnerability assessments, identify potential cyber-attacks,
16 mitigate losses from cyber-attacks, and recover quickly and
17 efficiently from cyber-attacks."

18 SECTION 3. Statutory material to be repealed is bracketed
19 and stricken. New statutory material is underscored.

20 SECTION 4. This Act shall take effect upon its approval.

21



H.B. NO. 2755

1

INTRODUCED BY:

James H. Matlock
W

Lyn DeLoite

On James

K. L.

Tom Barr

Beth Lukens

Paul King

[Signature]

JAN 27 2016



H.B. NO. 2755

Report Title:

Cybersecurity; Incident Response Plan.

Description:

Requires the cybersecurity, economic, education, and infrastructure security coordinator to develop and maintain an incident response plan to cyber-attacks for each executive department in the State.

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

