
HOUSE BILL 1929

State of Washington

65th Legislature

2017 Regular Session

By Representatives Hudgins, Harmsworth, and Tarleton

Read first time 02/02/17. Referred to Committee on State Govt,
Elections & IT.

1 AN ACT Relating to building a more robust state information
2 technology security posture by leveraging assets at the military
3 department and other agencies responsible for information technology
4 systems and infrastructure; and amending RCW 43.105.215.

5 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

6 **Sec. 1.** RCW 43.105.215 and 2015 3rd sp.s. c 1 s 202 are each
7 amended to read as follows:

8 (1) The office shall establish security standards and policies to
9 ensure the confidentiality, availability, and integrity of the
10 information transacted, stored, or processed in the state's
11 information technology systems and infrastructure. The director shall
12 appoint a state chief information security officer. Each state
13 agency, institution of higher education, the legislature, and the
14 judiciary must develop an information technology security program.

15 (2) Each state agency information technology security program
16 must adhere to the office's security standards and policies. Each
17 state agency must review and update its program annually and certify
18 to the office that its program is in compliance with the office's
19 security standards and policies. The office shall require a state
20 agency to obtain an independent compliance audit of its information
21 technology security program and controls at least once every three

1 years to determine whether the state agency's information technology
2 security program is in compliance with the standards and policies
3 established by the agency and that security controls identified by
4 the state agency in its security program are operating efficiently.

5 (3) In the case of institutions of higher education, the
6 judiciary, and the legislature, each information technology security
7 program must be comparable to the intended outcomes of the office's
8 security standards and policies.

9 (4) The office may test the security of any state agency's
10 information technology systems and infrastructure, including online
11 applications, to identify and mitigate system vulnerabilities. The
12 office shall coordinate with the state agency being tested as
13 necessary so that business operations and service delivery are not
14 disrupted by the testing. The office may assist agencies in the
15 remediation of any vulnerability identified by the testing. Results
16 of the testing must be shared with the agency tested. Testing of
17 institutions of higher education, the judiciary, and the legislature
18 may only be conducted at the institution's request.

19 (5) The state military department, at the request of the entity
20 involved in the management of critical infrastructure to be tested,
21 may conduct independent security testing, including compliance
22 audits, penetration testing, risk assessments, and vulnerability
23 assessments, of the information security of any private entity
24 operating within this state, or unit of local government of this
25 state, involved in the management of critical infrastructure. The
26 state military department may assist the entity in the remediation of
27 any vulnerability identified by the testing. Results of the review
28 and progress of remediation efforts must be shared with the state
29 chief information security officer, the utilities and transportation
30 commission, and the entity reviewed.

31 (6) For the purposes of this section, "critical infrastructure"
32 means systems and assets, managed by local governments or private
33 sector entities, whether physical or virtual, so vital to the United
34 States that the incapacity or destruction of such systems and assets
35 would have a debilitating impact on security, economic security,
36 public health or safety, or any combination of those matters.

--- END ---