

---

HOUSE BILL 2172

---

State of Washington

65th Legislature

2017 Regular Session

By Representative Hudgins

Read first time 03/22/17. 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; amending RCW 43.105.215; and creating a  
5 new section.

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

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

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

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

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

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

10 (4) The office may test the security of any state agency's  
11 information technology systems and infrastructure, including online  
12 applications, to identify and mitigate system vulnerabilities. The  
13 test must apply framework from the cybersecurity excellence  
14 assessment criteria, when available, or similar objective criteria to  
15 give measurable results for state agencies' information technology  
16 systems and infrastructure. The office shall coordinate with the  
17 state agency being tested as necessary so that business operations  
18 and service delivery are not disrupted by the testing. The office may  
19 assist agencies in the remediation of any vulnerability identified by  
20 the testing. Results of the testing must be shared with the agency  
21 tested and legislative members upon request in accordance with  
22 subsection (7) of this section. Testing of the judiciary and the  
23 legislature may only be conducted at the institution's request.

24 (5) The state military department, at the request of the entity  
25 involved in the management of critical infrastructure to be tested,  
26 may conduct independent security testing, including compliance  
27 audits, penetration testing, risk assessments, and vulnerability  
28 assessments, of the information security of any private entity  
29 operating within this state, or unit of local government of this  
30 state, involved in the management of critical infrastructure. The  
31 state military department may assist the entity in the remediation of  
32 any vulnerability identified by the testing.

33 (6) The chief information security officer, the utilities and  
34 transportation commission, and the state military department must  
35 meet regularly to share information, trends, and best practices  
36 regarding information technology systems and infrastructure security.

37 (7) The office must mutually develop procedures with the  
38 legislature, including enforceable nondisclosure agreements, for  
39 providing information about the state's cybersecurity infrastructure,  
40 performance, posture, and results of testing conducted under

1 subsection (4) of this section to members of the state legislature to  
2 enable them to effectively perform their constitutional duties.

3 (8) For the purposes of this section:

4 (a) "Critical infrastructure" means systems and assets, managed  
5 by local governments or private sector entities, whether physical or  
6 virtual, so vital to the United States that the incapacity or  
7 destruction of such systems and assets would have a debilitating  
8 impact on security, economic security, public health or safety, or  
9 any combination of those matters.

10 (b) "Cybersecurity excellence assessment" means an assessment of  
11 enterprise cybersecurity operational performance using a framework  
12 approved by the national institute of standards and technology,  
13 United States department of commerce.

14 NEW SECTION. Sec. 2. If specific funding for the purposes of  
15 this act, referencing this act by bill or chapter number, is not  
16 provided by June 30, 2017, in the omnibus appropriations act, this  
17 act is null and void.

--- END ---