H-0998.3

HOUSE BILL 1929

State of Washington 65th Legislature 2017 Regular Session

By Representatives Hudgins and Harmsworth

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

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

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

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

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

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

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

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

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

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

--- END ---