# Office of the Governor
# State of Oregon

**EXECUTIVE ORDER NO. 16-13**

**UNIFYING CYBER SECURITY IN OREGON**

WHEREAS, information systems, networks, and critical infrastructure around the world are threatened by increasing and evermore sophisticated cyber-attacks; and

WHEREAS, the people of and businesses operating within Oregon have entrusted state government with a large repository of information that they expect will be protected and secured; and

WHEREAS, information is a strategic asset of the state of Oregon that should be managed and secured as a valuable state resource; and

WHEREAS, the continuous and efficient operation of state government information systems is both vital and necessary to the mission of providing government services in Oregon; and

WHEREAS, vulnerabilities of the state's information systems underscore the need to enhance the security of Oregon information systems, networks, and critical infrastructure; and

WHEREAS, aging information technology infrastructure and antiquated legacy information systems in use by state agencies remain vulnerable to cyberattack, placing private information about state employees and their dependents, consumers of state services, taxpayers, and the residents and businesses of Oregon at risk; and

WHEREAS, responsibility and accountability for the security of state information systems is currently dispersed and decentralized with the exception of the enterprise information resources, technology, and telecommunications infrastructure managed and overseen by the State Chief Information Officer.

WHEREAS, ORS 182.122 imposes on state agencies the responsibility to secure their information systems or implement information security plans, policies, standards, and procedures established by the State Chief Information Officer; and

WHEREAS, unification of the state's cyber security functions under the leadership of the State Chief Information Officer is necessary to protect the availability, integrity, and confidentiality of state information systems and the information stored in state information systems pursuant to ORS 182.122;

**NOW, THEREFORE IT IS HEREBY DIRECTED AND ORDERED:**

1. All state agencies within the Executive department as defined in ORS 174.112, except the Secretary of State, State Treasurer, Attorney General of Oregon, Oregon Bureau of Labor and Industries, State Lottery, and public universities listed in ORS 352.002, shall carry out the actions necessary to unify information technology (IT) security functions.

2. Beginning on the effective date of this Executive Order, the State Chief Information Officer (CIO), or designee of the State CIO, and state agencies specified in section 1 shall work cooperatively to prepare for and develop a plan to execute the transfer of agency IT security functions and employees to the Office of the State CIO (OSCIO) by November 1, 2016.

3. In accordance with the plan, the Director of each state agency specified in section 1 shall deliver to the State CIO, or designee of the State CIO, all records related to the performance of the agency IT security functions transferred to OSCIO.

4. The Director of each state agency specified in section 1 shall execute a "Job Rotation — External Agreement" to assign employees engaged primarily in the performance of agency IT security functions to OSCIO. The job rotation shall begin within one month of the effective date of this Executive Order and shall end on June 30, 2017, or at a time decided by the mutual agreement of the sending agency's Director and the CIO. The sending agency shall continue to be responsible for the employees' compensation for the duration of the job rotation assignment.

5. The State CIO shall take possession of the records, and take charge of the employees specified in section 4, subject to the terms of the "Job Rotation — External Agreement," the state's ordinary practices in performing such agreements, applicable collective bargaining agreements, and other applicable law. As necessary to accomplish the missions and goals of the state and state agencies, the State CIO, or the State CIO's designee, may immediately redeploy transferred employees back to their respective agency of origin under the continuing supervision of the State CIO, or the State CIO's designee.

6. State agencies shall assist OSCIO and provide access to personnel and other resources necessary to successfully execute the job rotation.

7. The DAS Director, or designee of the DAS Director, shall ensure compliance with all applicable policy provisions and collective bargaining agreements,

including providing any notices required thereunder within the applicable time periods.

8. All state agencies shall cooperate in the development of and follow the plans, rules, policies, and standards adopted by the State CIO. Further, all state agencies shall provide OSCIO with full cooperation in the implementation of a statewide agency-by-agency risk-based security assessment and remediation program. The State CIO shall determine and charge the costs incurred by the program for third-party security evaluations, vulnerability assessments, other related technical services, and remediation measures to the state agencies that the State CIO serves. The state agency shall pay the cost to the State CIO in the same manner that other claims are paid. Additionally, state agencies will conduct and document the completion of OSCIO approved information security awareness training for all agency employees on an annual basis; report security metrics using methodologies developed by the OSCIO; and participate in activities coordinated by the OSCIO in order to better understand and address security incidents and critical cyber security threats to the state.

9. This Executive Order shall remain in effect until it is otherwise modified, amended or terminated.

Done at Salem, Oregon, this 12th day of September, 2016.

Kate Brown
GOVERNOR

ATTEST:

Jeanne P. Atkins
SECRETARY OF STATE