

## Oregon Gets Cybersecurity Booster Shot with Governor's Approval of Senate Bill 90

News Staff | June 30, 2017



The increasing attention on cybersecurity in the wake of large-scale breaches and ballooning cyberthreats has forced many states to re-evaluate and restructure their approaches. Most recently, Oregon took a hard look at the landscape and opted for some significant changes — implementing most of them in a 2016 executive order before officially codifying them into law June 29.

In Sept. 2016, Gov. Kate Brown outlined the need for a more focused cybersecurity posture in Executive Order 16-13, which opened the door for the Office of the State Chief Information Officer to assume a more enterprise role across the largely federated state landscape. Brown's signature on Senate Bill 90 cemented this new approach permanently.

[Back in March](#), CIO Alex Pettit voiced his support for the legislation, explaining that it would unify the state's disparate cybersecurity forces under his office's authority. One challenge facing the state's various agencies, Pettit said at the time, was that many were without dedicated IT personnel, let alone dedicated cybersecurity staff.

The CIO compared the connected but standalone state agencies to castles with wide moats and high walls, but little protection against quickly spreading fires from neighbors. The newly minted law provides the tools and authority to address this issue.

The new law centralizes the power of the state CIO when it comes to cybersecurity; allows the office to draw from cybersecurity and IT staff within the various agencies; and mandates agency cooperation with the CIO's office on cybersecurity. Though staff can be reassigned as the CIO sees fit, they can also be left in place within their home agencies at the CIO's discretion.

Like other states, Oregon's SB 90 also formalizes the creation of an organization tasked with making cybercentric decisions for the state. The Oregon Cybersecurity Advisory Council would consist of nine voting members and an undetermined number of non-voting members, which would all be appointed by the CIO. Of the nine members, at least two must be from a post-secondary educational institution, and state law enforcement agency. All members are required to be from "cyber-related" industries in the state.

Additionally, the law makes way for the Oregon Cybersecurity Center of Excellence, which would be tasked with inter- and intra-agency coordination, threat response, and information-sharing operations related to state and national cybersecurity issues. These portions of the law will take effect Jan. 1, 2018.

<http://www.govtech.com/policy/Oregon-Gets-Cybersecurity-Booster-Shot-with-Governors-Approval-of-Senate-Bill-90.html>