



Oregon

Tina Kotek, Governor

Enterprise Information Services
Cyber Security Services
550 Airport Road SE, Suite C
Salem, OR 97301
503-378-2282

February 14, 2026

Senator Prozanski
Senate Committee on Judiciary
900 Court Street NE, S-415
Salem, OR 97301

Re: SB1516 End-to-End Encryption

Dear Senator Prozanski,

Enterprise Information Services has no position on SB1516. We are available to provide technical expertise to assist with informed decision making. We do not recommend defining security standards or architecture in statute due to the rapid rate at which technology changes.

End-to-end encryption (E2EE) is an industry term recognized as: *End-to-End Encryption (E2EE) is a secure communication process where data is encrypted on the sender's device and only decrypted on the recipient's device. It ensures that only the communicating users can access, read, or listen to messages, preventing intermediaries—including service providers, hackers, or government entities—from intercepting or accessing the data.* It is mostly used in individual-to-individual applications.

Oregon State Police (OSP) contracts with the automated license plate recognition (ALPR) provider, Axon. Axon provides an integrated ecosystem through a cloud-based and connected platform, Axon Evidence. This includes ALPR, Evidence management, In-Car MDT/Mobile devices and body cameras (following requirements in [ORS 133.741](#)). This software as a service (SaaS) ecosystem is built in Microsoft's Azure Government Cloud.

Microsoft Azure Government serves as the “bedrock” for Axon Evidence, providing cloud-based storage and digital evidence management. The environment is FEDRAMP-authorized and designed to meet the strict security requirements of CJIS (Criminal Justice Information Services).

As a SaaS provider, Axon does not employ E2EE security architecture. This means each law enforcement agency service subscriber does not retain encryption keys to their own data. As with many SaaS providers used by Oregon state agencies, encryption functionality and associated encryption keys are maintained by the vendor. Vendors providing services to Oregon state agencies are required to meet verifiable state security standards and encryption protocols. Those vendors supporting public safety state agencies must also meet CJIS standards and associated policy.

Mission: Mature enterprise technology governance, optimize investments, ensure transparency, provide oversight, and deliver secure and innovative solutions.

To employ the E2EE security architecture, Axon would have to change their business and security model and architecture at a steep cost. If Oregon is the only state mandating this architecture, it is unlikely the vendor would incur the cost to make this architectural change. The presents the risk with a high likelihood that OSP would not be able to renew the contract with Axon to maintain use of ALPR technology.

Upon a preliminary review of other state's legislation regarding ALPR¹, we did not find any that include specific technology architecture requirements for information security. Alabama law requires the third-party vendor to agree to and submit an ALEA CJIS Contractor/Vendor CJI Access Security Agreement. <https://admincode.legislature.state.al.us/api/rule/265-X-6-.08> Virginia law requires the system meets information security standards as established by the Virginia Information Technologies Agency. <https://law.lis.virginia.gov/vacodefull/title2.2/chapter55.6/>

I hope this information is helpful. If you have any questions or would like additional information, please contact our Legislative Director, Shirlene Gonzalez at 971-803-1766.

Sincerely,



Ben Gherezgiher
State Chief Information Security Officer

cc: Rebecca David, OSP

¹ <https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes>; <https://legislativeanalysis.org/wp-content/uploads/2025/09/Automatic-License-Plate-Recognition-Systems-Summary-of-State-Laws.pdf>