Cybersecurity, privacy and DSA best practices

Chapter 291, Laws of 2021, Section 4 required the Office of Cybersecurity (OCS) to research, examine and report on data protection best practices in collaboration with the Office of Privacy and Data Protection (OPDP) and the Attorney General's Office. The report was submitted Dec. 1, 2021. Key findings and recommendations related to cybersecurity, privacy and data sharing agreements (DSAs) are summarized in this document.

Cybersecurity

Washington state has a large and growing technology footprint. It faces persistent and increasingly sophisticated cyberattacks that threaten state agencies and the vendors agencies partner with. At the same time, the COVID-19 pandemic has dramatically changed how the state conducts business and the way Washingtonians access services. Our remote workforce accesses the State Government Network from home instead of the office. Higher risk transactions that used to be done in-person are now done remotely. State data and applications are steadily moving out of the state's data center and into the cloud. All of these changes have opened more avenues for bad actors to attack state systems. In this evolving landscape, data governance needs to be adaptive, implicit trust is no longer an option, visibility into threats needs to be improved, and security needs to be managed in the context of risk to business.

OCS recommends the state take the following steps to protect state data and systems:

- **Centralize and standardize data governance:** Washington can benefit from a centralized form of data governance that identifies and prioritizes desired business outcomes at the agency and enterprise level.
- **Adopt zero trust architecture:** The growth of ransomware attacks nationally, coupled with cloud adoption and the transition to a hybrid (remote) workforce requires the state of Washington to accelerate adoption of a Zero Trust Architecture to improve our security posture and increase our cyber-resiliency.
- **Implement enterprise identity and access management**: A robust Identity and Access Management (IAM) solution ensures that only the right people or machines have access to the appropriate assets for approved reasons, while keeping unauthorized access and fraud at bay.
- **Modernize security operations:** Washington needs to adopt modern, enterprise methods of data collection and analysis to improve detection capabilities against more elusive attacks across our large enterprise.
- **Establish an enterprise security risk management program:** An Enterprise Security Risk Management Program helps identify, evaluate and mitigate the likelihood and/or impact of security risk to the agency. This program allows risks to be quantified and prioritized in the context of the agency's mission and helps security professionals advise program owners in the process of making security risk management decisions that will in turn advance the overall mission of the agency.

Privacy

Privacy best practices can be broken into four separate categories: Privacy principles, privacy frameworks, laws and regulations, and maturity models.

- Washington State Agency Privacy Principles were finalized in 2020. These principles are not mandatory but help guide agency practices and decisions to maintain public trust. They will continue to be used as a communication tool to help shape a culture of privacy and as the backbone for other tools and resources.
- **Privacy frameworks** provide the structure and basis to implement privacy protections and operationalize a program. They are tailored during implementation to reflect applicable laws, the types of information held, and an organization's risk profile and resources. While flexibility is a benefit to frameworks, it does create the possibility of applying a framework in a way that is too lenient or too conservative.
- **Laws and regulations** set baseline requirements for many agencies but should not be mistaken for privacy frameworks. Compliance alone does not necessarily mean better privacy. A law might not establish strong enough protections to meet residents' expectations, contemplate new technology, or account for cultural context. This can create a gap between compliance and appropriate controls.
- **Maturity models** help organizations measure against the expectations and standards established by laws and frameworks. They add a quantitative measurement so an organization can determine not only what it needs or wants to do, but also how well it is doing it.

Although agencies should strive to implement frameworks and maturity models, successful implementation will likely require additional investments in OPDP and agency programs. Other opportunities to strengthen data protection that OPDP and agencies should pursue include:

- Developing, promoting and mandating training and awareness activities.
- Cultivating a community of professionals to share best practices and promote professional development.
- Designating agency privacy contacts to facilitate consistent communication and resource distribution.
- Developing and implementing resources that incorporate the Washington State Agency Privacy Principles, such as formal policies or privacy impact assessments.

Data Sharing Agreements

Agencies are required to enter DSAs to protect confidential information when sharing with contractors (RCW 39.26.340), requesting from other agencies (RCW 39.34.240), or doing any other sharing outside the agency (OCIO Security Standard 141.10). DSAs help ensure data is adequately protected, outline responsibilities if an incident occurs, and document who information is shared with and all the places it is stored.

Agencies should take steps to identify when a DSA is needed, implement appropriate DSAs, and ensure an adequate monitoring process.

- **Identify.** Data sharing should be understood as any act of making data available to third parties. This includes sharing extracts, data hosting and system access. To identify all situations where a DSA is necessary, agencies should track transmissions; build safeguards into existing processes such as the workflow to develop a new data product; and develop appropriate data sharing approval requirements.
- **Implement.** DSA terms, including the appropriate level of specificity, can vary significantly. To help agencies enter appropriate DSAs, WaTech published Data Sharing Agreement Implementation Guidance. WaTech also published two sample DSAs tailored for different types of relationships.
- **Monitor.** Executing a DSA is not the end of appropriate third-party management. At a minimum, agencies should ensure they can identify all existing DSAs, assign responsibility to monitor them, consider compliance and enforcement controls, and certify disposal when data is no longer needed.