



# Washington State Auditor's Office

Troy Kelley

Independence • Respect • Integrity

## Opportunities to Improve State IT Security

While Washington has taken significant measures to protect the state from cyber threats, opportunities exist to strengthen the state's information technology (IT) security posture and reduce security risk. We found that the state's IT security standards align closely with leading practices, including its statewide approach to IT security management. We also found that agencies are not in full compliance with these standards. Through our compliance and application security testing, we found numerous issues at five selected agencies. We also found significant discrepancies between agency-reported compliance with state standards and our own results. This indicates the monitoring and reporting process currently used to develop a statewide picture of Washington's IT security risks is not functioning as intended.

### Responsibility for securing the state's IT environment is shared

In Washington, state law assigns the Office of the Chief Information Officer (OCIO) responsibility for developing and establishing IT security policies and standards and for monitoring agency compliance with those standards. Individual state agencies are responsible for complying with the state's IT security standards. The Consolidated Technology Services agency (CTS) provides agencies with enterprise IT security services and is the home of the state's Chief Information Security Officer.

### Testing identified non-compliance issues and security weaknesses

While we found the state has established strong IT security standards, our audit also found state agencies are not fully complying with these standards. We tested five of the 11 state IT security standards at five selected agencies, and found close to 350 instances – out of 1,035 security standard components tested – in which these agencies are not in full compliance.

Around three-quarters of the issues found were due to a lack of documentation, which typically represents less of a security risk than a lack of implementation. The areas where we found the most noncompliance issues were:

- application security, where we found issues such as a lack of documentation for application changes
- data security, where we found issues such as inadequate use of encryption
- operations management, where we found issues such as a failure to send backup data to an offsite location.

We conducted application security tests to assess whether applications and their underlying infrastructure were vulnerable to an attack. We found a total of 46 issues at the five selected state

Our audit focused on OCIO IT security standards 4 through 8, which are most critical for protecting the state from cyber threats

- 1**  **IT Security Program**  
Sets requirements for agencies' IT policies and procedures
- 2**  **Personnel Security**  
Controls that reduce risks of human error, theft, fraud or misuse
- 3**  **Physical & Environmental Protection**  
Controls for adequate physical security and environmental protections
- 4**  **Data Security**  
Sets controls around data in agency systems
- 5**  **Network Security**  
Controls to protect connections between agency systems and other networks
- 6**  **Access Security**  
Sets controls around who can actually access the data and how
- 7**  **Application Security**  
Requirements for system development controls, including ongoing maintenance
- 8**  **Operation Management**  
Guides day-to-day activities of IT security (such as data backup and disposal)
- 9**  **E-Commerce**  
Controls to reduce risks associated with doing business over the Internet
- 10**  **Security Monitoring & Logging**  
Controls to facilitate detection and auditing of unauthorized data processing activities
- 11**  **Incident Response**  
Procedures to facilitate response and reporting of system compromise

agencies; seven were rated critical (extreme impact to entire entity and almost certain to be exploited), and 12 were rated high (major impact to entire entity or individual program and can be exploited by attacker with minimal skills). All five agencies worked quickly to start fixing the issues we identified and some agencies reported using the information to improve other applications not included in testing.

## **The state's IT security standards align closely with leading practices, but improvements could be made**

We found no significant gaps between the state's IT security standards and leading practices. We did find a few areas where the OCIO could improve the standards by adding more details from leading practices, or clarifying language to ensure greater consistency in agency compliance. Examples of improvements include:

- Clarifying expectations for agency data-sharing agreements to ensure the safeguarding of confidential data
- Clarifying agency requirements for ensuring that external service providers meet state IT security standards
- Adding environmental protection requirements for agency data centers, such as emergency power, lighting, temperature and humidity controls

## **The state's process to monitor agency IT security compliance could be improved**

The state has an appropriate IT security framework that includes good statewide IT security standards, as well as a process to monitor and oversee compliance with those standards. However, the significant difference between what agencies reported to the OCIO and what we found during our audit points to the need for improvements to monitoring and oversight of agency compliance. This is particularly important because without complete and accurate information from state agencies, those responsible for IT security do not have the information needed to support those agencies, or effectively monitor IT security for the state.

## **Summary recommendations**

To help ensure the state maintains the integrity of its IT networks and systems, and to better protect the confidential information entrusted to the state, we recommend:

- The five selected state agencies continue remediating identified gaps in agency practices and documented policies, weaknesses identified through our application security testing, and provide accurate and complete reporting of agency compliance with, and deviations from, the state's IT security standards.
- The state's Chief Information Officer revise the state's IT security standards to more closely align with leading practices, and clarify those where our review found multiple agencies did not comply. And evaluate and revise the current process used for agencies to annually report the status of their compliance with, and deviations from, the state's IT security standards to ensure the process provides meaningful and accurate information.
- The state's Chief Information Security Officer and Chief Information Security Officer continue to collaborate to help agencies better understand the importance of complying with the state's IT security standards, and how best to do so.

### ***Reporting detailed results***

IT security information is exempt from public disclosure in accordance with RCW 42.56.420 (4).

To protect the IT security of our state, this report does not include the names of the five selected agencies, nor any detailed descriptions of our findings. Disclosure of such details could potentially be used by a malicious attacker against the state.

Detailed findings and recommendations were provided to each agency we reviewed, and to the OCIO and CTS.