Improving State IT Security: An overview of performance audits

Joint Legislative Audit and Review Committee

January 10, 2019

Joseph Clark, Performance Auditor

Patrick Anderson, Performance Auditor

William Clark, Performance Auditor

Security is important, so we audit it

- IT security affects everyone
  - Data breaches
  - Critical services
- State agencies must protect their systems and data
- Because of this, we performed three audits assessing IT security and related practices

Audit overview – Cyber 4

- 2018 cybersecurity performance audit of three volunteer state agencies
- Fourth in this series of audits, covering 15 agencies
- Assessed *network and application security*

Audit overview – Safe Data Disposal

- Included 28 state agencies
- Focuses on *destruction of data* prior to hardware surplus
- Follow-up to a safe data disposal audit from 2014

Audit overview – Vendor Contract Assurances

- Assessed seven contracts at five agencies
- Assessed *agency contracts with IT vendors* for:
  - Security requirements
  - Assurances protecting the state in the event of a breach
- Also assessed agency vendor monitoring practices

Common themes

All three audits:

- Conducted primarily by State Auditor's Office auditors and IT security specialists
  - Cybersecurity audit also used contractors for penetration testing
- Assessed agencies against state requirements and leading practices
- Found agencies could do more, and should improve their documentation

Protecting sensitive information

Confidentiality is key

RCW 42.56.420

Security.

The following information relating to security is exempt from disclosure under this chapter:

(4) Information regarding the infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities, and other such information the release of which may increase risk to the confidentiality, integrity, or availability of agency security, information technology infrastructure, or assets;

Audit #1

Cyber 4:

Continuing opportunities to improve state IT security

Audit scope

- Assessed security at three agencies by asking:
  - Can selected agencies make their IT systems more secure, and better align their IT security practices with state requirements and leading practices?

- All three agencies volunteered

Methodology – Part 1

Can selected agencies make their IT systems more secure … ?

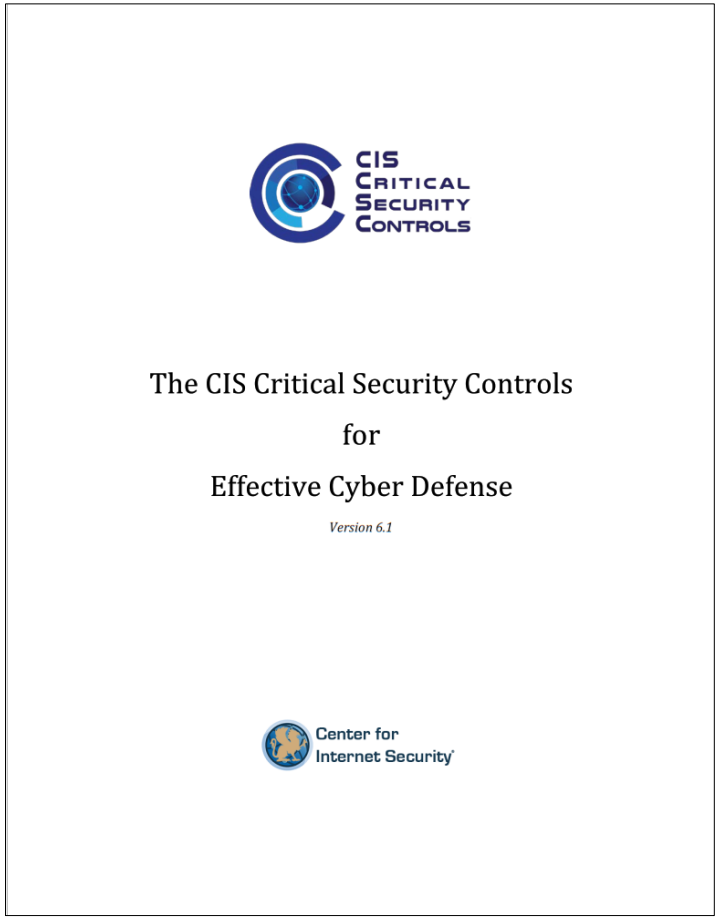
- Penetration testing of each agency's network and applications
  - External
  - Internal

- Performed by contracted subject matter experts

Methodology – Part 2

Can selected agencies … ***better align their IT security practices with state requirements and leading practices?***

- Compared agency practices to internationally recognized Critical Security Controls
  - Informed by private- and public-sector stakeholders
  - Prioritize benefits



The controls we used

The Critical Security Controls we used:

- 1: Inventory of Authorized and Unauthorized Devices
- 2: Inventory of Authorized and Unauthorized Software
- 3: Secure Configurations for Hardware and Software
- 4: Continuous Vulnerability Assessment and Remediation
- 5: Controlled Use of Administrative Privileges
- 11: Secure Configurations for Network Devices

- Also assessed agencies against related state IT security standards
  - Approximately 1/3 of the full requirements

Results overview

- We found strengths in agencies' security, but also areas where agencies can improve security by:
  - Remediating vulnerabilities
  - Improved implementation and documentation of controls
- Agencies should increase compliance with state requirements
  - Often did not tailor documentation to meet their needs
- Agencies could use the Critical Security Controls to improve security

Agencies and OCS reported barriers

- Agency personnel reported resource constraints – specifically insufficient personnel – as a challenge
- The Office of CyberSecurity (OCS) has taken steps to help agencies in general improve security and compliance
- But OCS also cited insufficient resources to assist individual agencies

Recommendations

We recommend the three state agencies:

- Continue remediating issues identified during security testing
- Continue remediating gaps between agency IT security implementation or written policies and procedures and the state's IT security standards
- Consider also further aligning agency IT security controls with leading practices
- Continue periodically assessing IT needs and resources, including personnel and technology

Recommendations

We recommend Office of CyberSecurity:

- Continue to reach out to state agencies to identify what information would help agencies:
  - Incorporate detailed controls into their policies and procedures
  - Align agency practices with the state IT security standards
- Continue to develop and provide that additional clarity or guidance
- Continue to assess resources to better assist agencies in developing and implementing their IT security programs

Audit #2

Safe Data Disposal:

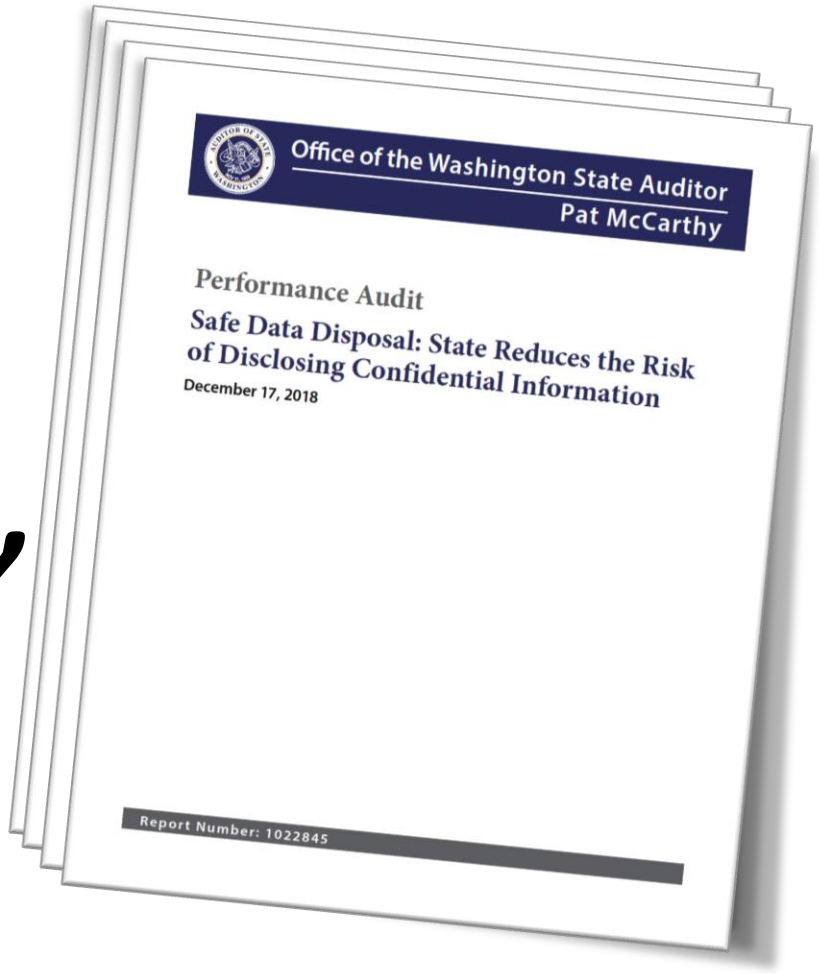
State reduces the risk of disclosing confidential information

Background

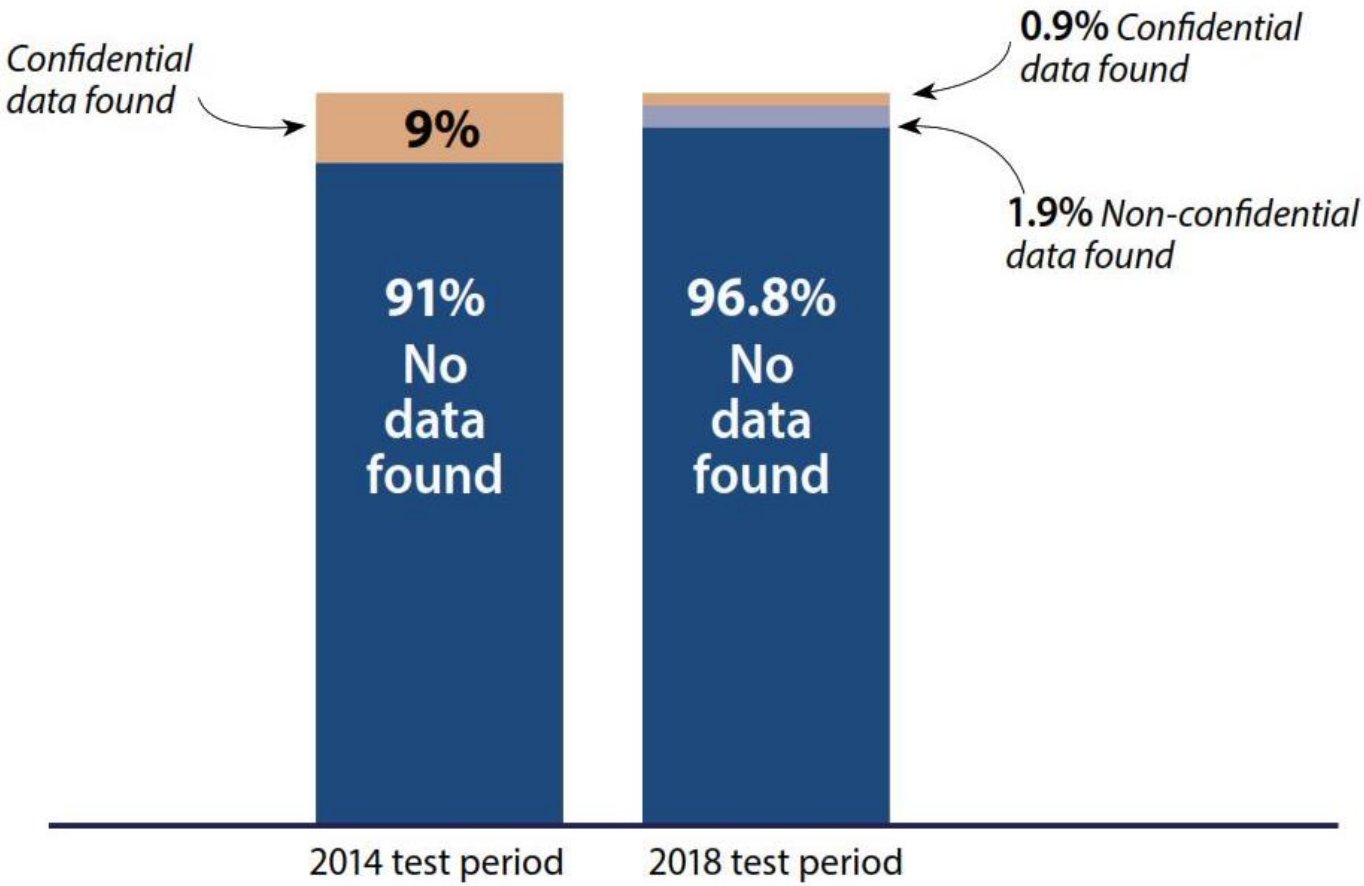
- The Department of Enterprise Services' surplus program helps agencies dispose of items they no longer need
- Responsibility to remove data rests with each agency

Audit scope and objective

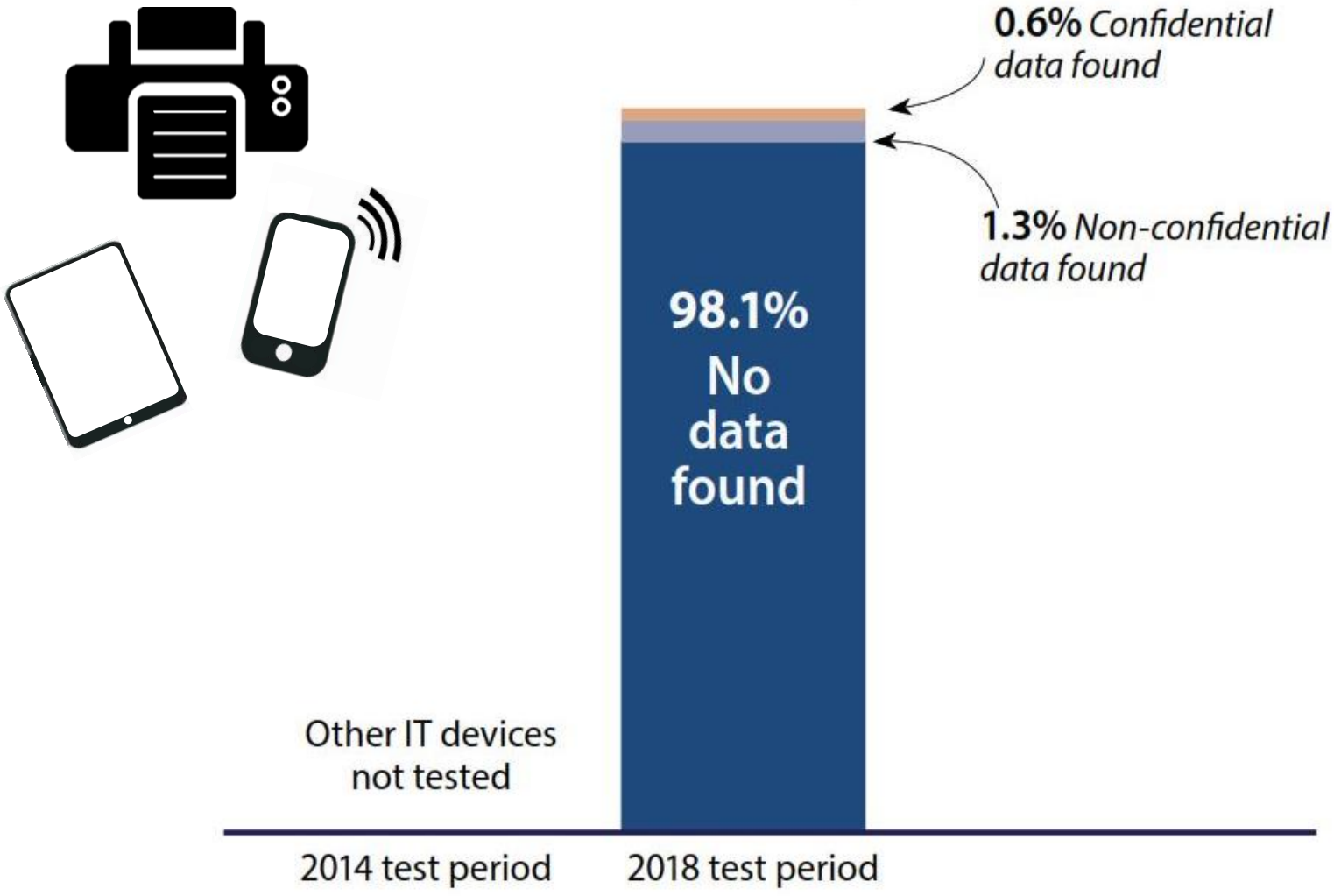
"Does the state have adequate controls in place to ensure that the surplus of state-owned IT devices do not disclose confidential data?"



Confidential data found on state computers decreased from 2014

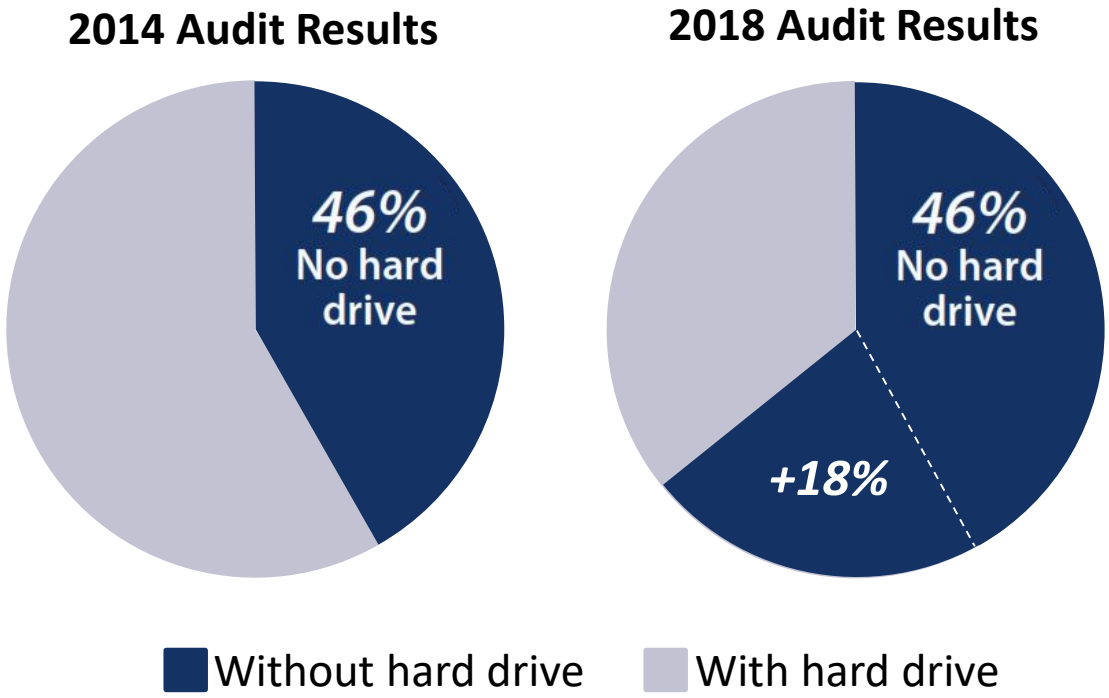


Other surplused IT devices yielded similar results

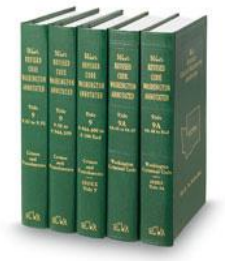


Fewer computers with hard drives are being sent to surplus

- Agencies are eliminating the risks by removing and destroying hard drives
- More computers are being sent to surplus without hard drives



Agency gaps in policies and procedures



Washington state law

Washington State · Office of the
Chief Information Officer

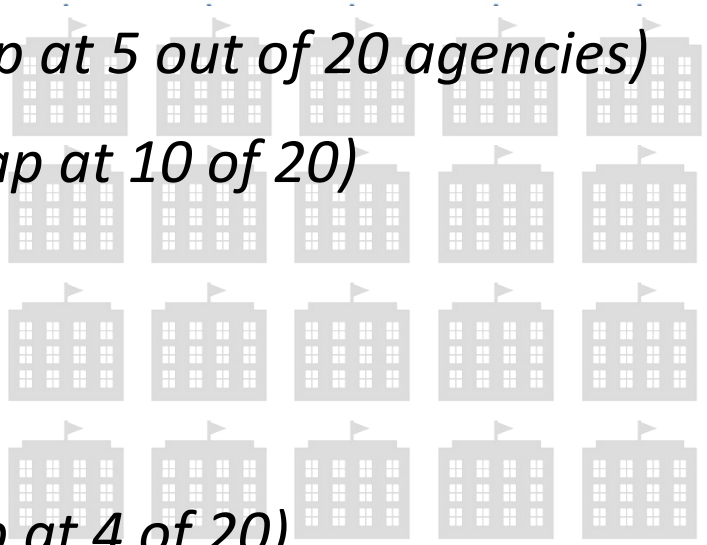
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Agency gaps in policies and procedures

Most agencies had written policies for disposing of IT equipment, but some did not fully incorporate state requirements or best practices.

Gaps included steps to:

- Verify data has been removed *(a gap at 5 out of 20 agencies)*
- Train surplus and disposal staff *(a gap at 10 of 20)*
- Retain records of disposed surplus property *(a gap at 4 of 20)*
- Maintain clear policies on how to dispose of other IT devices *(a gap at 4 of 20)*



Recommendations

Audited agencies

- Confidential letters containing detailed information were issued to agencies

Guidance for all Washington state agencies

- Annually review policies and procedures
- Ensure state requirements are applied
- Include state-approved methods for erasing data on mobile devices

Audit #3

State IT Applications:

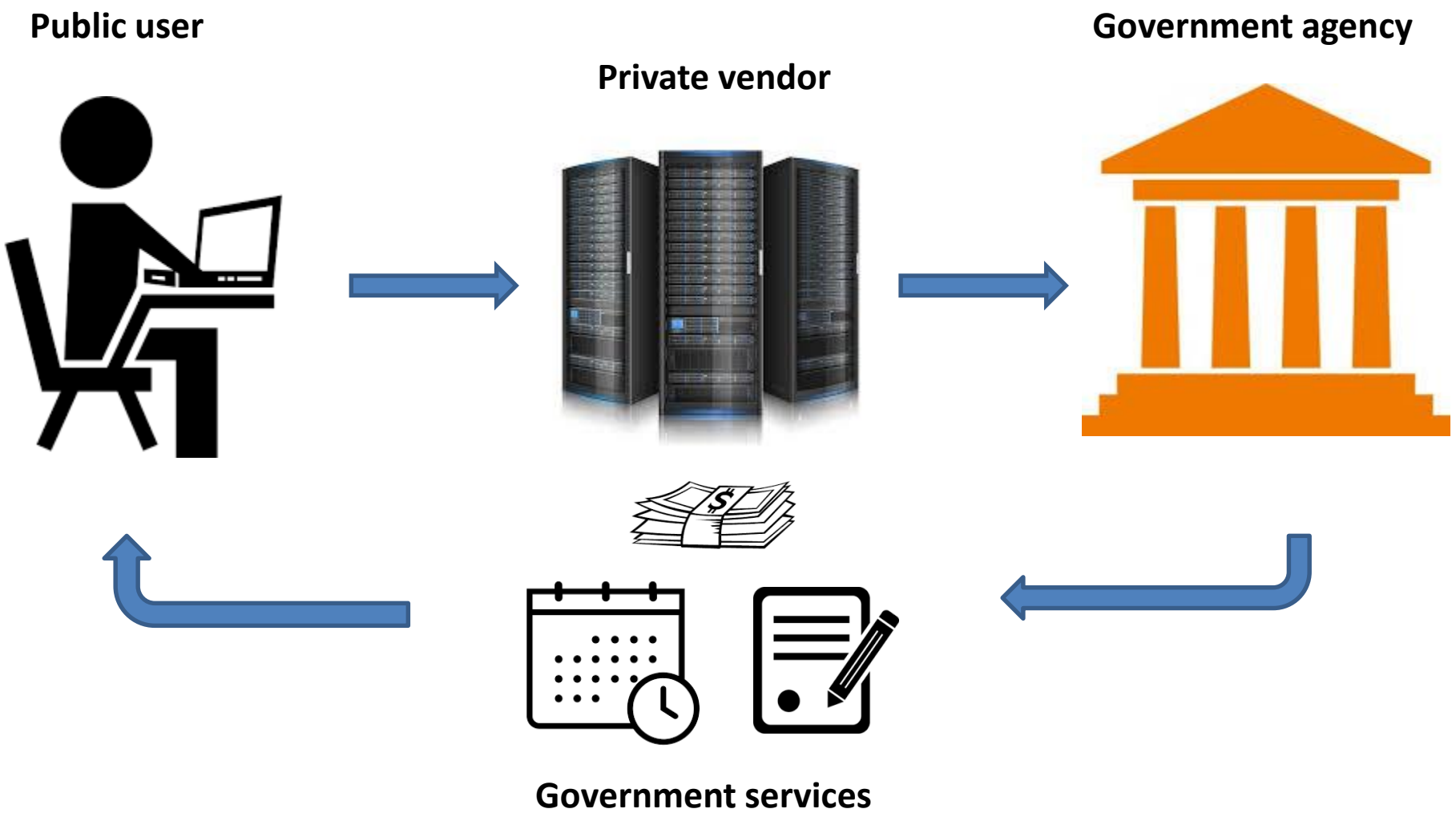
Contract assurances for vendor-hosted state IT applications

Vendor-Hosted IT Applications

Washington agencies rely on vendors to provide IT services and operate systems critical to the state

- Payment processing
- Communication services
- Applications and licensing

Vendor-Hosted IT Services



Why we did this audit

- Outsourcing services to private vendors is on the rise
- When vendors manage agency applications, the state relinquishes direct control over security
- Risks related to state IT assets are growing

Audit objectives

This audit assessed whether selected agencies:

1. Included appropriate provisions in each contract to address the state's IT security requirements

2. Followed leading practices to ensure vendor compliance with the IT security requirements in their contracts

3. Included provisions in vendor contracts to protect the state in case of a data breach

Audit scope and methodology

- Seven contracts from five agencies
- IT applications needed to:
  - Be hosted by a third-party vendor
  - Be critical to the mission of the agency
  - Contain confidential state information
- Reviewed contract language and monitoring practices

Was vendor compliant with standards and requirements?

Vendors are required to comply with state and agency-specific IT security standards

- Most contracts required vendors to comply with the state's general IT security standards
- Only one included the agency's specific requirements
- Two contracts did not require vendor compliance with either state or agency IT security requirements

How are agencies monitoring their vendors?

- Agencies did not use formal risk assessment results to develop contracts
- Only two of the five agencies actively monitored their vendors' compliance with most contractual security requirements
- Most agencies required vendors to adhere to the state's IT standards, but none verified compliance in accordance with contractual provisions
- Agencies could do more to specify roles and responsibilities and communicate regularly with vendors about IT security

What protections have agencies included in their contracts?

- All seven contracts included indemnification language
- Timelines for notifying the state of a data breach were longer than the state's security policies
- One contract required cyber-liability insurance, and two other vendors carry the insurance

Recommendations

- Agencies should comply with state requirements and follow leading practices
- DES should include specific IT guidance in its policies and procedures for contracting
- OCIO should provide more guidance and clarity to agencies for vendor compliance
- Create a forum with OCIO, DES and agencies' IT personnel to discuss leading practices in IT contracting

Closing remarks

- The state must protect its data, from the time it is obtained until it is destroyed
- Technological change and emerging risks require continued vigilance
- Security practices must meet state requirements, and should be supplemented with leading practices where necessary

Contact

Pat McCarthy
State Auditor
Pat.McCarthy@sao.wa.gov
(360) 902-0360

Scott Frank
Director
of Performance Audit
Scott.Frank@sao.wa.gov
(360) 902-0376

Troy Niemeyer
Assistant Director
of State Audit
Troy.Niemeyer@sao.wa.gov
(360) 725-5363

Duane Walz
Assistant Audit Manager
Duane.Walz@sao.wa.gov
(360) 725-5594

Joseph Clark, CISA
Performance Auditor
Joseph.Clark@sao.wa.gov
(360) 725-5572

Patrick Anderson
Performance Auditor
Patrick.Anderson@sao.wa.gov
(360) 725-5634

William Clark
Performance Auditor
William.Clark@sao.wa.gov
(360) 725-5632