# IT Interface Controls

Joint Legislative Audit and Review Committee

September 26, 2018

**Shauna Good**, Principal Performance Auditor

**Diana Evans**, Assistant Audit Manager

**Jon Howard**, Assistant State Auditor

# About this presentation

The audit does not name agencies

**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;

# How this audit differs from IT security audits

| This audit reviewed: | IT security audits review: |
| --- | --- |
| Security controls specific to IT interfaces files | Security controls across entire IT systems |
| Controls designed to ensure data is secure, complete and accurate | Controls designed to prevent cyberattacks |

# Effects of IT security breaches and unreliable data

- Effects of security breach
  - Legal and regulatory violations
  - Decreased customer satisfaction
  - Eroded public trust
  - Significant costs
- Effects of unreliable data
  - Service delivery failure
  - Interrupted client benefits
  - Under- or over-billing

# Selecting interfaces

Interface

- Hardware
- Software
- Human processes

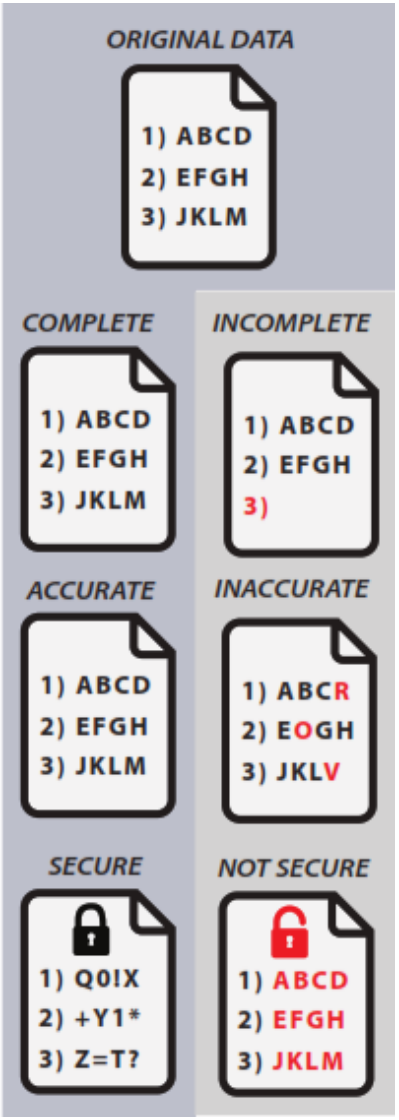
We identified 13 interfaces at 5 agencies

- Essential to state operations
- Process confidential information

# Audit objectives

Do selected agencies' information systems have interface controls to ensure the state's data is:

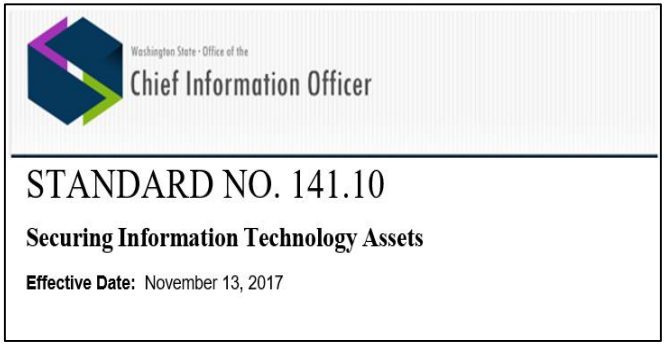
- ✓ Complete
- ✓ Accurate
- ✓ Secure



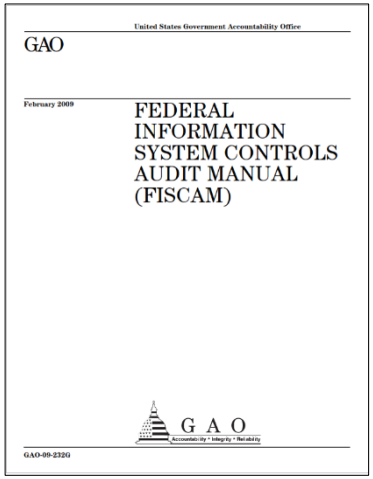
# Scope and methodology

Reviewed agencies' IT security controls to see if they align with:

- Required state IT security standards (OCIO 141.10)




- The Federal Information System Controls Audit Manual (FISCAM)



# Overall, agencies had adequate controls

| Agency | Interfaces | Complete? | Accurate? | Secure in transit? | Secure at rest? |
|---|---|---|---|---|---|
| **Agency 1** | Interface 1 | ✓ | ✓ | ✓ | ✓ |
| | Interface 2 | ✓ | ✓ | ✓ | ✓ |
| | Interface 3 | ✓ | ✓ | ✓ | ✓ |
| **Agency 2** | Interface 1 | ✓ | ✓ | ✓ | No |
| | Interface 2 | ✓ | ✓ | ✓ | No |
| | Interface 3 | — | — | ✓ | No |
| **Agency 3** | Interface 1 | ✓ | ✓ | ✓ | ✓ |
| **Agency 4** | Interface 1 | ✓ | ✓ | ✓ | ✓ |
| | Interface 2 | ✓ | ✓ | ✓ | ✓ |
| | Interface 3 | ✓ | ✓ | ✓ | ✓ |
| | Interface 4 | ✓ | ✓ | ✓ | ✓ |
| **Agency 5** | Interface 1 | No | ✓ | ✓ | ✓ |
| | Interface 2 | — | — | ✓ | ✓ |

# Accuracy and completeness results

**Accuracy**

All agencies had adequate controls to ensure accurate data

**Completeness**

One agency had no process to identify and correct records that did not transfer

- The agency did not incorporate reconciliation controls when designing the system

# Security results

**Broad access**

One agency gave all individuals with a login ID permissions to modify data for three interfaces, due to:

- Incorrect file configuration
- Lack of effective access review process

**IT developer access**

The same agency granted some IT developers the ability to modify data files without review or approval

- Allows developers to quickly resolve data transfer issues

# Recommendations and actions taken

To address issues with *completeness*, **Agency 5** should design and implement effective controls over the completeness of data transfers, such as reconciliations between sending and receiving systems

**Agency 5** staff responded they have implemented a reconciliation process

# Recommendations and actions taken

To address issues with *security*, **Agency 2** should:

- Limit access to the interface data to only those whose job duties specifically require access to the data
- Develop and employ a process to periodically evaluate who has access to the interface files and remove access when it is no longer needed
- Develop procedures for reviewing, testing and approving changes made by developers

In response to the security issues, **Agency 2** staff developed a remediation plan and submitted it to auditors

# Contacts

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

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

**Shauna Good, CPA**
Principal Performance Auditor
(360) 725-5615
Shauna.Good@sao.wa.gov

**Diana Evans, CPA**
Assistant Audit Manager
(360) 725-5426
Diana.Evans@sao.wa.gov

**Jon Howard, CISA**
Assistant State Auditor
(360) 725-5420
Jonathan.Howard@sao.wa.gov