Office of the Washington State Auditor
Pat McCarthy

Performance Audit

IT Interface Controls

September 17, 2018

Washington's state agencies need complete and accurate data to deliver services effectively and efficiently. In some cases, the critical data comes from another agency or system through an interface. An interface is a combination of hardware, software and human processes that allows information to move from one system to another. Interface controls are the processes designed to ensure the accurate, complete, and secure transmission and processing of the data between systems. Without reliable data, the state may fail to deliver services, eligible clients may not receive benefits, or billing could be incorrect. The Office of the Washington State Auditor reviewed 13 interfaces at five state agencies and examined whether interface controls were sufficient.

Auditors found most of the interfaces had adequate controls; however, there were a few opportunities for improvement. One agency did not have controls in place to ensure access to data was restricted to only those agency and contracted staff authorized to view or change the data, while another did not have reconciliation procedures to ensure data was complete.

Report Number: 1022174

Table of Contents

The mission of the Washington State Auditor's Office

Provide citizens with independent and transparent examinations of how state and local governments use public funds, and develop strategies that make government more efficient and effective.

The results of our work are widely distributed through a variety of reports, which are available on our website and through our free, electronic **subscription service**.

We take our role as partners in accountability seriously. We provide training and technical assistance to governments and have an extensive quality assurance program.

For more information about the State Auditor's Office, visit **www.sao.wa.gov**.

Americans with Disabilities

In accordance with the Americans with Disabilities Act, this document will be made available in alternative formats. Please email Communications@sao.wa.gov for more information.

State Auditor's Office contacts

State Auditor Pat McCarthy
360-902-0360, Pat.McCarthy@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

Kathleen Cooper – Director of Communications
360-902-0470, Kathleen.Cooper@sao.wa.gov

To request public records

Public Records Officer
360-725-5617, PublicRecords@sao.wa.gov

Introduction

Computer systems in state government frequently share data with other systems that support various state and federal services. Agencies need complete and accurate data to deliver services effectively and efficiently. Without reliable systems and reliable data, the state may fail to deliver services, eligible clients may not receive benefits, and under- or over-billing could occur.

The state also must protect the millions of sensitive and confidential records exchanged daily between its systems from intentional or unintentional disclosure, loss, and unauthorized use. Data breaches can have significant consequences, such as legal and regulatory violations, decreased customer satisfaction, and eroded public trust. A 2017 study by the Ponemon Institute, a research center that focuses on privacy, data protection and information security policy, found that a data breach costs government an average of $110 per record lost. These costs can include:

- Engaging forensic experts to determine the cause and breadth of the incident
- Hotline support for affected people
- Notifying affected people
- Providing people with free credit monitoring subscriptions
- Paying fines. For example, the U.S. Department of Health and Human Services' Office for Civil Rights may impose fines when protected health information is breached.

Strong system interface controls can help protect data

An interface is a combination of hardware, software and human processes that allows information to move from one system to another. Interface controls are automatic or manual processes designed to ensure transmission and processing of information between systems is complete and accurate. Consider a customer who places an order for medication online. The order is not complete if the pharmacy does not fill all the prescriptions in the order. The order is not accurate if the pharmacy gives the wrong dosage.

Interface controls also ensure that data is secure. Using the pharmacy example, the order is not secure if a hacker or others can see a customer's prescriptions. Strong interface controls protect the security of data both in transit and at rest. Data in transit is data moving from one location to another. Data at rest is data stored on a server, within a specific location, waiting to be processed.

State agencies are required to follow Washington State Office of Financial Management (OFM) and Washington State Office of the Chief Information Officer (OCIO) policies. OFM requires state agencies to develop controls to "provide for accountability of the state's assets and compliance to its laws and regulations" (*State Administrative & Accounting Manual*). OCIO policies require agencies to protect the state's data. The *Federal Information System Controls Audit Manual* (FISCAM) offers leading practices that apply to system interfaces. Following these requirements and practices can help agencies ensure data exchanged between systems are complete, accurate and secure.

Based on assessed risk, this audit was designed to determine if there are opportunities to strengthen interface controls at five state agencies by answering this question:

- Do the selected state agencies' information systems have interface controls that effectively ensure the completeness, accuracy, and security of the state's data during transfer and at rest?

The audit examined 13 interfaces at five agencies. Because of the sensitivity of information contained in government systems, and under the authority of RCW 42.56.420(4), the agencies are not identified in this report.

Information system interfaces allow data to be exchanged between two systems

As shown in **Exhibit 1**, interfaces can share information between a variety of organizations. For example, an interface can be present between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The data exchanged might be a file consisting of one or more records which is processed at a later time, or it can be a real-time update. Interfaces are present between a variety of different types of state agency systems, including those housed on legacy mainframe systems, client server systems and third-party vendor systems. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Exhibit 1 – The 'I' in each row indicates where an interface facilitates the interaction

State agency	I	Person
State agency	I	State agency
State agency	I	Federal agency
State agency	I	Local government entity
State agency	I	Private company

Interfaces, both external and internal, should be effectively managed and controlled to deliver the required criteria for completeness, accuracy and security. When interfaces are not managed well, errors can arise between the sent and received data files, as illustrated in **Exhibit 2**. According to FISCAM Section 4.3, an effective interface has the following characteristics.

Complete – All transactions and events that should be recorded are recorded.

When data is transferred from one system to another, the risks associated with incomplete data are that records and dollar amounts are not completely transferred to the receiving system. In other words, if 10 records are expected to be transferred from system A to system B, all 10 records should be transferred to system B.

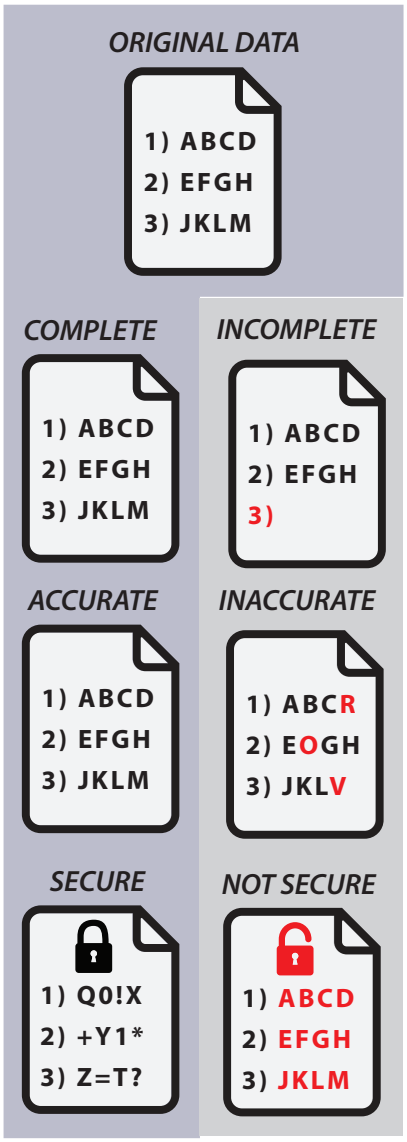
Accurate – Amounts and other data relating to recorded transactions and events are recorded correctly.

Data transfers to the receiving system should be accurate, meaning data should arrive exactly as it left the sending system. While completeness and accuracy are closely related, accuracy is more concerned with the details of the individual records that transfer. For example, an account number should have all the same digits, in the same order, in both systems.

Secure – Access to data is adequately restricted to reduce risk of intentional and unintentional disclosure, loss and unauthorized use.

Data transferring between two systems should be protected from external threats, such as hacking or theft. Data should also be protected from inappropriate use. Only staff who need to view or change interface data to perform their jobs should be granted access.

Exhibit 2 – An effective interface ensures the source data is received completely, accurately and securely



Scope and Methodology

Based on knowledge from auditing state agencies and previous system-related audit work, we selected five agencies for this assessment. With the involvement of key agency staff, we identified significant systems at each agency and selected 13 interfaces. We reviewed relevant standards and best practices, specifically OCIO 141.10, FISCAM, and OFM's State Administrative & Accounting Manual, to develop criteria for assessing the effectiveness of certain interface controls. We identified and tested relevant controls by interviewing key personnel, reviewing security access screens and reports, and observing agency input and output comparison processes.

Audit performed to standards

We conducted this performance audit under the authority of state law (RCW 43.09.470), approved as Initiative 900 by Washington voters in 2005, and in accordance with generally accepted government auditing standards as published in Government Auditing Standards (December 2011 revision) issued by the U.S. Government Accountability Office. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. See **Appendix A**, which addresses the I-900 areas covered in the audit. See **Appendix B** for a detailed description of the audit's methodology

Next steps

Our performance audits of state programs and services are reviewed by the Joint Legislative Audit and Review Committee (JLARC) and/or by other legislative committees whose members wish to consider findings and recommendations on specific topics. Representatives of the State Auditor's Office will review this audit with JLARC's Initiative 900 Subcommittee in Olympia. The public will have the opportunity to comment at this hearing. Please check the JLARC website for the exact date, time, and location (**www.leg.wa.gov/JLARC**). The State Auditor's Office conducts periodic follow-up evaluations to assess the status of recommendations and may conduct follow-up audits at its discretion.

Audit Results

Did selected state agencies have interface controls that effectively ensure the state's data transfers are complete, accurate and secure?

Answer in brief: For most interfaces included in the audit, agencies had adequate controls to ensure the completeness, accuracy and security of state data. However, there were a few opportunities to improve controls.

We gave the five state agencies comprehensive results of their individual agency's tests during the audit and at the conclusion of work. We also shared the detailed results with the Washington Technology Solutions, Office of Cyber Security. However, to protect the state's IT systems and the confidential and sensitive information contained in those systems, this report does not include the agencies' names or a complete description of the audit results.

Auditors reviewed 13 interfaces at five state agencies and examined the controls designed to ensure the data exchanged between systems was complete, accurate and secure. The table in **Exhibit 3** summarizes the results.

Exhibit 3 – Summary of results from review of system interfaces

Check mark given if the interface had adequate controls to meet criteria

Agency	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	*	*	✓	✓

** Not relevant for the tested interface.*

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 Washington state, this report does not include the names of the five selected agencies, nor any detailed descriptions of the findings. Disclosure of such detail could potentially be used by a malicious attacker against the state.

Controls at all five agencies were adequate to ensure *accurate* data, but one agency lacked adequate controls to ensure data was *complete*

Of the 13 interfaces reviewed, one at Agency 5 lacked adequate controls over completeness of data. At the time of the audit, the agency did not have a process to identify and correct records not transferred to the receiving system. Staff said the agency did not incorporate reconciliation controls when designing the system and that after it was placed into operation, addressing other issues were a higher priority. At the conclusion of this audit, agency staff said they had implemented a process to compare records in the sending system to those in the receiving system, however, auditors did not have the opportunity to test the effectiveness of this process.

Most interfaces had controls to ensure data was *secure*, but three interfaces at one agency did not

Data in transit

WaTech provides a service called the State Government Network (SGN) that allows agencies to share systems and data within the statewide private network. Washington's OCIO requires data be encrypted if it travels outside of the SGN; if it travels only inside the SGN, encryption is not required. Only one of 13 interfaces reviewed transmitted data outside the SGN and would require additional encryption. For this interface, the agency used another software solution called Secure File Transfer Protocol encryption to ensure data was secure during transit and met OCIO requirements.

Data in transit is data moving from one location to another.

Data at rest is data stored on a server, within a specific location, waiting to be processed.

Data at rest

Of the 13 interfaces reviewed, ten adequately secured data stored in interface files, but three, all at Agency 2, did not have controls to ensure data was secure. Auditors identified two issues with security for these interfaces.

First, all individuals with a network login ID had permissions that allowed them to modify data for all three interfaces, instead of just those who needed that access to perform their job duties. With this level of access, users could make unauthorized changes to data. In addition, excessive access to confidential data also increases the risk of unintentional disclosure, loss and unauthorized use. When auditors requested documentation showing who had access, agency staff recognized and reported the broad access, and further stated that it resulted from an incorrect file configuration. In addition, auditors found the agency lacked an effective process to periodically evaluate who had access to interface files and remove unnecessary access. A remediation plan was later submitted to the auditors during the audit.

Second, some IT developers have the ability to modify data files for two of the interfaces without review and approval, which is prohibited by state requirements. Developers were given this level of access to resolve issues that might arise during data transfers. Granting developers this type of access presents increased risk because their ability to manipulate the system's software code enables them to modify files without leaving an audit trail. If the agency grants developers this type of access, leading practices suggest that it establish a process to clearly document, track and approve any changes developers make, but Agency 2 management did not have such a process.

Recommendations

While most interfaces reviewed had controls in place, for those that did not, we make the following recommendations. These recommendations have been communicated directly to the agencies in detail.

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

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 review, testing and approval of changes made by developers

Agency Response

JAY INSLEE
Governor

STATE OF WASHINGTON

WASHINGTON TECHNOLOGY SOLUTIONS

1500 Jefferson Street SE □ Olympia, Washington 98504-1501 □ (360) 407-8700

September 12, 2018

The Honorable Pat McCarthy
Washington State Auditor
P.O. Box 40021
Olympia, WA 98504-0021

Dear Auditor McCarthy:

On behalf of the audited agencies, thank you for the opportunity to review and respond to the State Auditor's Office (SAO) performance audit report, "IT Interface Controls."

We agree that effective interface controls are essential to ensure systems pass accurate and secure information and continually strive to improve our IT infrastructure.

We appreciate the report acknowledging that overall most interfaces reviewed have adequate controls. We also appreciate the suggestions provided by your staff for continued improvement.

Sincerely,

Vikki Smith
Acting Director and State CIO

cc: David Postman, Chief of Staff, Office of the Governor
Kelly Wicker, Deputy Chief of Staff, Office of the Governor
Keith Phillips, Director of Policy, Office of the Governor
Scott Frank, Director of Performance Audit, Washington State Auditors' Office
Inger Brinck, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor
Scott Bream, Chief Information Security Officer, Washington Technology Solutions

OFFICIAL STATE CABINET AGENCY RESPONSE TO PERFORMANCE AUDIT ON IT INTERFACE CONTROLS – SEPTEMBER 12, 2018

This management response to the State Auditor's Office (SAO) performance audit report received August 22, 2018, is provided by the Office of the Chief Information Officer on behalf of the audited agencies.

SAO PERFORMANCE AUDIT OBJECTIVES:

The SAO sought to answer this question:

1. Do the selected state agencies' information systems have interface controls that effectively ensure the completeness, accuracy, and security of the state's data during transfer and at rest?

The report states that most interfaces reviewed had controls in place, for those that did not, we make the following recommendations.

SAO Recommendation 1: 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.

STATE RESPONSE:

We have designed and implemented a delta difference comparison which compares data differences for the system identified in the audit. We will continue to analyze our systems and identify and implement additional controls as necessary to ensure completeness of data transfers.

Action Steps and Time Frame

- Design and implement controls for completeness of data transfers. *Completed.*

SAO Recommendation 2: 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 review, testing and approval of changes made by developers.

STATE RESPONSE: We value the review of our interface controls and have already implemented corrective actions to ensure our data at rest is only accessed by those whose job duties specifically require access to the data. We will continue to monitor this access on an ongoing basis.

Action Steps and Time Frame

- Developed and implemented a process to limit access to interface files. *Completed April 20, 2018*
- Develop procedures to document, track and approve changes made by developers. *By March 31, 2019*

Appendix A: Initiative 900

Initiative 900, approved by Washington voters in 2005 and enacted into state law in 2006, authorized the State Auditor's Office to conduct independent, comprehensive performance audits of state and local governments.

Specifically, the law directs the Auditor's Office to "review and analyze the economy, efficiency, and effectiveness of the policies, management, fiscal affairs, and operations of state and local governments, agencies, programs, and accounts." Performance audits are to be conducted according to U.S. Government Accountability Office government auditing standards.

In addition, the law identifies nine elements that are to be considered within the scope of each performance audit. The State Auditor's Office evaluates the relevance of all nine elements to each audit. The table below indicates which elements are addressed in the audit. Specific issues are discussed in the Results and Recommendations section of this report.

I-900 element		Addressed in the audit
1.	Identify cost savings	**No.** The audit focused on the accuracy, completeness and security of system interface data and not on cost savings.
2.	Identify services that can be reduced or eliminated	**No.** The scope of the audit included only system interfaces, which are necessary to share information between systems.
3.	Identify programs or services that can be transferred to the private sector	**No.** The audit focused on the accuracy, completeness and security of data in state agency system interfaces and not on whether programs or services could be transferred to the private sector.
4.	Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**Yes.** The audit identified gaps in system interface controls.
5.	Assess feasibility of pooling information technology systems within the department	**No.** The audit focused on the accuracy, completeness and security of data and did not include an analysis of the feasibility of pooling information technology systems.
6.	Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**Yes.** The audit analyzed system interface control functions and made recommendations to improve them.
7.	Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.** The audit did not identify any necessary statutory or regulatory changes.
8.	Analyze departmental performance data, performance measures and self-assessment systems	**No.** While the audit did review system interface processes, it did not include a review of departmental performance measures or self-assessment systems.
9.	Identify relevant best practices	**Yes.** The audit identified best practices for system interface controls.

Appendix B: Methodology

Auditors evaluated controls over the completeness, accuracy, and security of data within interface files and in transit between interface files. The audit scope was limited to only the interface files and did not include reviews of the entire sending and receiving systems.

Selecting state agencies for audit

Based on knowledge from auditing state agencies and previous system-related audit work, we selected five agencies for this assessment. We reviewed agencies using both legacy systems and newer replacement systems. We also included agencies that interface confidential data and financial data with other entities.

Selecting systems and interfaces for testing

With the involvement of key agency internal audit and IT staff, we identified significant systems for each agency, which we defined as systems with a high volume of transactions or high dollar amounts in transactions and/or systems that processed confidential information.

We interviewed agency staff to gain an understanding of the incoming and outgoing interfaces and using that information, along with knowledge gained during other audits, we selected 13 system interfaces for testing at the five state agencies.

Control testing and assessment

We reviewed relevant standards and best practices, specifically Washington State Office of the Chief Information Officer (OCIO) policy 141.10 and the Federal Information System Controls Audit Manual (FISCAM), to develop criteria for assessing the effectiveness of certain interface controls. Leading practices drawn from these sources addressed the key areas of concern: completeness, accuracy and security.

Completeness and Accuracy

Auditors reviewed completeness and accuracy using leading practices from FISCAM that include:

- Procedures are in place to reasonably assure that the interfaces are processed completely and accurately.
- The interfaced data is reconciled between the sending and receiving application to ensure that the data transfer is complete and accurate.
- Errors during interface processing are identified and promptly investigated, corrected and resubmitted for processing.
- Data files are not processed more than once.

Security

Auditors reviewed security using leading practices from FISCAM and requirements from the OCIO that include:

FISCAM Section 4.3:

- Controls should be in place to ensure access is limited.
- All changes to configuration, including emergency changes, should be appropriately documented and approved.

OCIO Standard No. 141.10 4.4 Secure Data Transfer:

- Agencies must appropriately protect information transmitted electronically. Confidential information that is specifically protected from disclosure by law that is transmitted outside of the State Governmental Network requires encryption such that:
  (1) All manipulations or transmissions of data during the exchange are secure.
  (2) If intercepted during transmission the data cannot be deciphered.

OCIO Standard No. 141.10 7.2.(2) Application Development

- Agencies must implement separation of duties or other security controls between development, test and production environments. The controls must reduce the risk of unauthorized activity or changes to production systems or data including but not limited to the data accessible by a single individual.

Auditors then determined which audit objectives were relevant to the identified interface. For example, a receiving system might collect confidential data which could be used for initial research. In this instance, the completeness of the data is not critical, but the confidential data that is collected must be protected. Once we identified the relevant controls, we tested them by interviewing key personnel, reviewing security access screens and reports, and observing agency input and output comparison processes.