Secretary of State Audit Report

Kate Brown, Secretary of State

Gary Blackmer, Director, Audits Division

Computer Controls for the Oregon Benefit Information System Need Attention

Summary

One mission of the Oregon Employment Department (department) is to "support economic stability for Oregonians and communities during times of unemployment through the payment of unemployment benefits." Toward that end, the department's Unemployment Insurance Division Benefits section provides partial wage replacement income to workers who are unemployed through no fault of their own. The department uses the Oregon Benefit Information System (OBIS) to process unemployment claims and payments. During state fiscal year 2011, the department processed approximately $2.3 billion worth of benefits through this system.

The primary purpose of this audit was to review and evaluate the effectiveness of key general and application controls over the computing environment at the department. We found that reasonable efforts were being made to ensure transactions were complete, accurate and valid during input, processing and output. However, the department could improve its handling of unusual or complicated claims and overpayments.

Although identified overpayments only represent about one percent of total payments, about $23 million, or 57%, of certain detected overpayments were not processed to enable collection by the department for more than six months. We identified about $6 million in additional overpayments that were missing from the overpayment queue and would likely not ever be processed. The department also routinely handled certain overpayments by paying claimants again without considering the amount they already paid. These procedures increased the total amount they overpaid these claimants from approximately $4.1 million to over $9.6 million. One manager explained that federal requirements make certain corrections for overpayments extremely time-consuming for a section that already had a backlog of work.

The department can also better document and manage changes to computer code for its mainframe systems such as OBIS. We noted several change control weaknesses that collectively increase the risk that programmers could introduce unauthorized and untested changes to the system.

We found assurance that regular backups of system and data files were created at the State Data Center, but detailed procedures are needed that define how the system would be recovered in the event of a disaster.

We also found that data security controls could be improved. We communicated detailed security matters to the department in a separate confidential memo, as provided in ORS 192.501 (23).

Agency Response

The agency response is attached at the end of the report.

Background

The Oregon Employment Department (department) was created in 1993. One of its missions is to "support economic stability for Oregonians and communities during times of unemployment through the payment of unemployment benefits." To achieve this mission, the department's Unemployment Insurance (UI) Division Benefits section provides partial wage replacement income to workers who are unemployed through no fault of their own. These payments are funded through a variety of sources, including federal funds and the Oregon Unemployment Insurance Trust Fund. The source of the trust fund money is Oregon employers who pay a payroll tax for each of their employees. Employers are assessed a tax rate based the age of their business, how many of its employees have had to draw benefits from the fund, and the overall state tax schedule.

The department uses several computer applications to administer the Unemployment Insurance program. In 1993, the department developed the Oregon Benefit Information System (OBIS) to establish and process initial and ongoing UI benefit claims. Over the past several years, the department has developed additional systems to support OBIS. Payment methods have also changed over time, and currently most payments are made through electronic deposits. In fiscal year 2011, about $2.3 billion were paid in UI benefits through OBIS, with support from the other systems.

The mainframe computer system housing OBIS is located at the State Data Center (SDC) under the Department of Administrative Services (DAS), and responsibility for general controls over the application and platform was shared between the department and DAS. Department staff are responsible for maintaining the computer code.

Oregon has experienced very high unemployment as a result of the recession. The unemployment rate rose from 6.3% in January 2008 to 11.1% in January 2011. Because regular unemployment benefits were only intended to last 26 weeks, the state and federal government extended covered benefits several times to assist individuals whose unemployment exceeded the normal benefit timeframe. These programs changes significantly complicated the department's work at a time when claim volume almost doubled.

Accurately processing unemployment claims requires inputs from several key sources. Claimants are required to provide accurate and complete personal information regarding their claim and efforts to find new employment. Employers are asked to report their employees' wages and unemployment taxes they pay, and verify that the separation was for reasons covered by the program. The federal government has provided strict guidelines regarding client eligibility, program benefits and timelines for providing these services.

Because of significant risk that claims may be fraudulent, the department has a special unit that investigates unusual claims and instances of likely fraud. The department also has personnel assigned to make decisions when claimant eligibility questions are raised, and has sections dedicated to resolving appeals of those decisions.

Audit Results

OBIS Controls Reasonably Ensured Accurate Payments, but Improvements are Needed to Better Handle Complicated Claims

Generally accepted controls for computer systems indicate that transaction data should be subject to a variety of checks for accuracy, completeness, and validity. Effective application controls include both manual and automated processes to ensure only complete, accurate, and valid information is entered into a computer system; data integrity is maintained during processing; and system outputs conform to anticipated results. Controls should also be in place to timely detect and correct errors that may occur during transaction input and processing.

The department has a variety of application controls to ensure the system processes transactions correctly and outputs occur as intended. Some of these controls include:

- automated routines within intake subsystems that require population of certain fields before transactions are accepted;
- manual comparisons of initial claim inputs to data obtained from the Social Security Administration, employers, and other reliable sources;
- OBIS-generated correspondence to claimants and employers to inform them of claims and to request additional information regarding claim accuracy or validity;
- various on-line edit and validation checks performed against data being processed;
- automated routines that suspend transactions with detected errors until the problems are resolved or overridden;
- processes to verify that printed check totals and electronic deposits match corresponding transaction totals processed through OBIS;
- automated restrictions on certain maintenance activities (e.g. an established overpayment cannot exceed the amount of the original payment); and
- reviews of key reports to ensure completeness of payment amounts.

These controls provide reasonable assurance that employment benefit claims paid through OBIS are complete, accurate and valid. However, we found the department could improve its handling of unusual or complicated claims and could process overpayments in a timelier manner.

Automated and manual input controls were not always effective for preventing errors

Data inputs should be validated and edited to provide reasonable assurance that erroneous data are detected or prevented before processing. When preventive measures are not possible or practical, detective and corrective measures may be implemented to further reduce the risk of errors or mitigate their adverse effects.

As we previously outlined, the department designed OBIS to appropriately control initial input and processing for most claims. However, the department did not always update the system to keep pace with some of the more complicated benefit program rule changes enacted by state and federal governments during the recent economic downturn. For example, staff had to manually perform important tasks such as examining previous claims and performing manual calculations in order to determine the correct benefit program to be charged.

As the list of program requirements, potential variants, and claim volume increased, the potential for human error likewise escalated. Given this environment, department management did not implement additional effective detective or corrective measures to counteract the increased risk of payment error. Specifically, we noted that staffs' manual inputs were not subsequently reviewed to ensure they were valid or accurate and it was unclear which of the system generated reports were actually used by staff. In addition, staff sometimes mistakenly approved higher risk claim payment transactions that the system appropriately suspended.

During fiscal year 2011, department staff identified overpayments totaling approximately $32.6 million that were not the result of fraud. These payment errors represented approximately one percent of total benefits paid. Although some of these errors could have been prevented through more robust input controls, others occurred when employers or claimants did not provide timely or accurate information regarding client eligibility.

Overpayment decisions were not always established in a timely manner

Regardless of how payment errors occur, controls should be in place to appropriately identify and correct them in a timely manner. As required by federal regulations, the department ensured payments to claimants and adjudication of eligibility questions were processed timely. However, they did not provide similar results in resolving known overpayments.

Once overpayments are discovered, staff must make an administrative decision that defines the amount of the overpayment. Without these decisions, the department cannot proceed with efforts to offset future benefits, collect reimbursements from claimants, or potentially garnish wages.

We evaluated selected overpayments that the department identified for benefit weeks during calendar year 2010 and the first 11 months of 2011 to determine whether the department timely established the required administrative overpayment decisions. During that period, the department identified non-fraud overpayments totaling approximately $56 million. Of these, staff established administrative overpayment decisions totaling approximately $41 million.

We evaluated the length of time it took department staff to establish the required administrative decisions that allow further actions to correct overpayments. As illustrated in the following table, about 14% of overpayment decisions were not processed until at least one year after staff was made aware of the overpayments, and another 43% took at least six months to process.

Time between Overpayment Identification and Setup	Overpayment Amount	Percent of Total
0 to 3 Months	$13 million	31.7%
3 to 6 Months	$4.7 million	11.5%
6 to 12 Months	$17.6 million	43.1%
More than 12 Months	$5.6 million	13.7%
Total	$41 million	100%

In addition, we identified overpayments totaling approximately $14.8 million that had not yet been processed. Department managers indicated that approximately $6 million of these were not even in the queue for establishing overpayment decisions, indicating it was unlikely they would ever be processed.

The department indicated that paperwork relating to overpayments is automatically routed to the central office. However, no tracking mechanism was in place to ensure this paperwork was received or that overpayment decisions would be established in a timely manner. In addition, management noted that limited staffing and heavy workload contributed to the inappropriate lag time in setting up overpayment decisions. To address this problem, for part of 2011 department managers temporarily shifted some of the unit's administrative tasks to other cost centers.

Overpayment corrections did not always comply with federal requirements

Errors occurring during processing should be promptly and accurately corrected. State and federal regulations provide strict requirements regarding payment of unemployment benefits including limits on how much claimants may receive from regular benefits or from state and federal extensions. Since funding from these various programs may come from different sources, it is important that claims are accurately established and errors, should they occur, are appropriately resolved.

There were instances where the department's methodology for correcting certain overpayments did not comply with federal requirements.[1] Specifically, the department sometimes paid claimants twice for the same benefit week. For example, one claimant was paid an average of $501 per week for 12 weeks. When staff discovered these weeks should have been paid using a different benefit program the department paid these same weeks at the correct rate of $179 per week, bringing the total weekly amount paid to $680. Since the original payment was $322 greater than it should have been, making the additional payment to correct the error only compounded the problem.

We reviewed situations where the department paid two different claims for the same benefit week as described above. From January 2010 through November 2011, the department initially paid $9.6 million to claimants that included overpayments of approximately $4.1 million. After making the additional payments to correct the administrative errors, the total amount the department paid to claimants totaled approximately $15.1 million and the total amount they overpaid more than doubled.

One department manager indicated that state and federal laws and regulations made it difficult for staff to correct this type of payment error without creating additional overpayments. We noted that the department identified another method of processing these types of claims that would reduce the amount of overpayment. However, management instructed staff to use it only for claims meeting certain characteristics, since the associated paperwork was time-consuming and would need to be performed by the same personnel who were already working on an overpayment backlog.

Federal and state law indicates that recovery of overpayments may be waived when the claimant did not cause the overpayment and claimed hardship. The department includes the forms to request this exemption with overpayment decision paperwork sent to claimants. Since claimants receiving most overpayments are unemployed, it is unlikely the state could fully recover overpayment amounts.

The Department Does Not Adequately Control Changes to System Code

Mainframe computer programs are generally written using a programming language such as Cobol. These languages allow programmers to write statements, referred to as source code, that represent the actions a programmer wants the computer to take. Source code must be translated or compiled into a computer-readable format before it may be used for processing.

[1] See Audit Report 2012-08 (Statewide Single Audit Report, FY 2011), pp. 97-98.

Program source code should be strictly managed to ensure only tested and approved modifications are compiled and implemented in production. To ensure this occurs, access to code should be strictly limited and monitored. In addition, proposed changes to code should be independently tested and compared to the latest version of authorized code to ensure only appropriate modifications are made. Procedures should also be in place to document key system design requirements and specifications.

Department management indicated they implemented policies and procedures for developing new systems, but that these did not apply to the more routine programming changes they make to its existing mainframe systems such as OBIS. For controlling these changes, department management chose to take a less formal approach, predominately trusting their experienced programmers to perform only the assigned tasks as intended. Management does track some system maintenance activities and provides workflows through its Service Request System. However, in some cases, little documentation existed outside of program code to substantiate what was actually done.

Program change control weaknesses posing the most significant risk included the following:

- The department did not adequately restrict programmers' access to production and source code libraries.
- Developers did not provide or retain adequate documentation of automated system controls or design specifications.
- Testing plans were not required and test results were not always documented or retained.
- Independent technical reviews of code modifications were not always performed. In addition, no documented requirements or expectations existed regarding the intended content or scope of these reviews.
- Code compares were not performed during programmers' review of modified code and before code was moved to the production environment.
- Processes were not in place to ensure adequate version control of source code. While logs were available that show movement of code to production, they are not used to monitor changes.
- Programmers did not always use the Service Request System to track programming changes.

Collectively, these weaknesses greatly increase the risk that department programmers could introduce unauthorized and untested changes to the system. Should this occur, the department could experience costly errors or delays in processing unemployment benefits. In fact, this happened when a programming error caused some claimants to be paid benefits for more weeks than they were authorized to receive under the rules of the program. Overall, this error resulted in overpayments of approximately $52,000 during fiscal year 2011.

Disaster Recovery Strategies Need Attention

Our third audit objective was to determine whether OBIS could be restored in a timely manner after a major disruption. Organizations should ensure usable backups are regularly performed in accordance with a defined back-up strategy. This strategy should ensure all critical files are copied as frequently as needed to meet business requirements and are securely stored at both on-site and off-site locations. In addition, disaster recovery procedures should be well-documented to facilitate proper and timely system reconstruction in the event of a major disruption. These procedures should also be tested periodically to ensure that they will function as planned. Without such procedures, the department could experience inordinate delays in restoring the system after a disaster that could severely impact the agencies' ability to provide mission critical services to Oregon citizens.

We reviewed the department's backup and recovery procedures and found that staff ensured regular backups of critical OBIS data and system files were created at the State Data Center. However, it was unclear whether all files needed for restoration of OBIS were included in these backups. Department managers indicated they rely on the State Data Center to create backup tapes designated for off-site storage and to perform most of the steps necessary to recover the system from the tapes in a disaster recovery scenario. However, the State Data Center has not fully developed detailed procedures that define how they would restore infrastructure or developed timelines and priorities for restoring agency applications and data. In addition, neither the State Data Center nor the department has conducted full tests to determine if, how, or when recovery could occur. As a result, the department does not have sufficient assurance that the system could be timely recovered in the event of a disaster.

We noted that the department's business continuity plans indicate the potential for partnering with the State of Utah to process claims on behalf of Oregon. We applaud this potential innovative solution to mitigate some of the effects of a disaster. However, the department and the state of Utah have not developed procedures or conducted tests to determine whether or how this resource could be realized. As such, it too provides insufficient assurance that the system could be timely recovered.

System Security Should be Improved

The integrity of computer systems and other information assets is preserved by controls that protect the environment in which systems operate, as well as controls that protect individual systems. In addition, when an organization relies on an external service provider to host its computer systems, it should formally define each party's responsibilities and specific expectations regarding security. It should also obtain assurance that critical security requirements are fulfilled.

Our final audit objective was to determine whether system information was protected against unauthorized use, disclosure, modification, damage, or loss. To achieve this objective, we evaluated controls the department used to secure the system, and considered security measures provided for department systems hosted at the State Data Center.

The department has done much to establish a security management program and provide logical access controls to protect OBIS and its data. However, these efforts were not always sufficient or effective. In addition, our separate audit of controls at the State Data Center identified security weaknesses that increased the risk that the system could be compromised.

Because of the sensitive nature of system security, we communicated additional details regarding our specific findings and recommendations regarding this matter to the department in a confidential letter in accordance with ORS 192.501 (23), which exempts such information from public disclosure.

Recommendations

We recommend that department management:

1. Take steps to better ensure accurate payment of Unemployment Insurance claims by establishing:
    - additional automated or manual processes to better prevent system input errors;
    - more robust error detection procedures to identify payment anomalies and ensure their timely correction;
    - procedures to ensure that identified overpayments are monitored to ensure that associated overpayment decisions are appropriately generated;
    - staffing requirements for the overpayment unit to ensure timely processing of overpayment decisions; and
    - procedures for correcting overpayment errors that ensure compliance with federal regulations.
2. Develop and implement change management controls to:
    - better restrict programmers' access to production and source code libraries;
    - ensure development, retention, and maintenance of automated system control documentation and design specifications;
    - establish requirements for developing, documenting and retaining testing plans and test results associated with all program code changes;
    - establish requirements and expectations for technical reviews, such as code compares, and ensure these reviews are independently performed for all code changes before code is moved to the production environment;
    - ensure processes are in place to ensure adequate version control of source code; and
    - ensure all change management steps and approvals are appropriately documented and retained.

3. Ensure all necessary OBIS files have been backed up and are available for restoration, and work with the State Data Center to develop detailed procedures that fully define how the system should be recovered in the event of a disaster or significant disruption. Once established, those procedures should be periodically tested and adjusted as necessary to ensure timely recovery will occur.

4. Resolve the security weaknesses we identified in our confidential management letter and work with the State Data Center to ensure the department's security expectations are clearly established and fulfilled.

Objectives, Scope and Methodology

The purpose of our audit was to review and evaluate the effectiveness of key general and application controls over the computing environment at the Oregon Employment Department. Our specific objectives were to:

- Determine whether information system controls provide reasonable assurance that Unemployment Insurance transactions remain complete, accurate and valid during input, processing and output.
- Determine whether changes to computer code are appropriately controlled to ensure integrity of information systems and data.
- Determine whether information system files and data are appropriately backed up and can be timely restored in the event of a disaster or major disruption.
- Determine whether information systems and data are protected against unauthorized use, disclosure, modification, damage, or loss.

The scope of our audit included selected portions of the Oregon Benefits Information System (OBIS), including establishment of initial claims, processing of continued claims, and actions related to administrative decisions.

We primarily focused on controls in effect from July 1, 2010 – December 31, 2011. However, some of our data included payments outside of this time period, as stated in the report.

We conducted interviews with department personnel and observed department operations and processes. In addition, we examined technical documentation relating to OBIS and its architecture.

To evaluate unemployment insurance processing controls, we:

- Examined selections from the department's benefit manual.
- Interviewed managers regarding procedures and controls for claim input and maintenance.
- Tested claim data for various characteristics, such as calculation of benefit amounts, determination of claim validity, and determination of whether correspondence to employers was generated and whether responses from employers were evaluated and used.
- Tested claim payment data covering "weeks claimed" from the first week of 2010 through week 48 of 2011 for various characteristics. For example, we:
    - evaluated whether payment limits were exceeded;
    - reviewed claimant eligibility for payment based on answers to certification questions;

  - reviewed whether claims were paid when claim characteristics indicated they should be denied or stopped;
  - examined whether multiple claims were paid for the same benefit week; and
  - reviewed whether weeks paid that had denying administrative decisions against them had associated overpayments established.

To evaluate program change management controls, we reviewed the department's change management policies and procedures, reviewed logical access to file locations, and performed a limited review of supporting documentation for selected changes.

To determine whether OBIS could be restored in the event of a disaster, we reviewed backup schedules, examined disaster recovery plans and restoration procedures, and reviewed disaster recovery test results performed by the State Data Center.

To determine whether logical access to OBIS was provided in accordance with a demonstrated need, we:

- evaluated the methods by which users were provided access to transactions, including review of associated system documentation, and how these were requested, granted, and closed;
- tested whether selected users' access matched request forms; and
- tested whether terminated employees had their access removed from the system.

To evaluate security management practices, we examined security policies, procedures and plans, evaluated security monitoring processes, and examined incident response plans and practices. We also reviewed the results of our most recent audit of security at the State Data Center.

Because of its sensitive nature, we communicated detailed information relating to security findings and recommendations to the department under separate cover in accordance with ORS 192.501 (23), which exempts sensitive information from public disclosure.

We used the IT Governance Institute's publication, "Control Objectives for Information and Related Technology," (COBIT), and the United States Government Accountability Office's publication "Federal Information System Controls Audit Manual" (FISCAM) to identify generally accepted control objectives and practices for information systems.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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.

Oregon

John A. Kitzhaber, MD, Governor

Employment Department
875 Union St NE
Salem, OR 97311-0024
(503) 947-1394
TTY-TTD 711

WORKSOURCE OREGON

August 3, 2012

Gary Blackmer, Director, Audits Division
Secretary of State
255 Capitol Street NE, Suite 500
Salem, OR 97310

RE: Secretary of State Audit Report, *Computer Controls for the Oregon Benefit Information System*

Dear Director Blackmer:

This is in response to the Secretary of State's (SOS) final report on the findings and recommendations contained in the above-referenced final audit report of the Oregon Employment Department's (Department) Oregon Benefit Information System (OBIS). The Audit covered the time period of July 1, 2010 through December 3, 2011.

Finding 1: OBIS Controls Reasonably Ensured Accurate Payments, but Improvements are Needed to Better Handle Complicated Claims

The auditors noted that the Department has a number of applications and controls in place to ensure that unemployment insurance benefits are paid in a timely and accurate manner but pointed out that we could improve the handling of unusual or complicated claims and that we could process our overpayments in a timelier manner. The auditors specifically identified that (1) automated and manual input controls were not always effective for preventing errors; (2) overpayment decisions were not always established in a timely manner; and (3) overpayment corrections did not always comply with federal requirements. We agree with the auditors on all accounts and have taken the following corrective actions in order to more accurately process complicated claims and to more quickly identify and establish overpayments.

The Department has taken corrective action by creating a new automatic stop that will prevent the system from making duplicate benefit payments for the same benefit week. The stop remains in place until reviewed and inactivated. A mandatory comment is required when the flag is inactivated. Corrections to existing programming prevents the system from making payments exceeding a claimant's weekly benefit amounts and the system produces comments documenting any manual adjustments. Our process for handling claims where it is determined benefits should have been paid under a different unemployment program has also been modified as another way of preventing duplicate payments for the same week. Corrective action involving claimants who received benefits in excess of their maximum weekly benefit amount due to system error involved both establishing the overpayments that were made as well as correcting the system error. Besides stopping the system error that created the overpayments and establishing those that were made, the Benefit Payment Control (BPC) management is developing a more robust system report using our Business Intelligence tool that will identify any payment made in excess of the claimant's maximum weekly benefit amount, for any program. This report will be run regularly to assist with identifying and remediating any future system errors that might cause too high of a weekly payment to be made and will also assist with the timely establishment of any resulting overpayments. We anticipate that this report will be completed and in use by September 30, 2012. Lastly, the Unemployment Insurance Benefits management team collaboratively responded to the need to properly staff its overpayment unit by pooling its staff resources in the short term while we pursue supplemental federal funding and other avenues to ensure that the overpayment unit remains properly staffed in the future.

Finding No. 2: The Department Does Not Adequately Control Changes to System Code

The auditors found that although management does track some system maintenance activities and provides workflows through its Service Request System (SRS), little documentation exists outside of program code to verify work was completed. The auditors reported program change control weaknesses increase risk of programmers introducing unauthorized and untested changes to the system. The Department agrees with the auditors and we have taken steps to reduce risks though policy and procedure updates, peer review, and improved monitoring.

The Department's Service Request System (SRS) was implemented late in the 2009-2011 biennium to replace a paper-based tracking system. The Department intends to expand the use of the SRS to a more complete change control system. The first phase was for application development tracking only; planned future phases will include access management request, and a more detailed application program change log. Formal procedures and guidelines will be developed in support of the consolidation of change management methods and expand to include testing and quality assurance procedures, including emergency procedures when there is an operational impact that needs to be corrected immediately. Version control tools now available from the State Data Center (SDC) are being evaluated and will be included in the change control process where their use will improve process tracking and effectiveness. The Department recognizes the need to develop training for program area staff on what needs to be included in a request for change and what responsibilities belong to the requestor. Accordingly, the Department's IT staff will work with business stakeholders to develop appropriate materials.

In the near term, corrective action has been taken to better restrict programmer access to production and source code libraries. Management from the Department's Unemployment Insurance and IT divisions reviewed and restricted programmer access to production and source code libraries to the minimum number required for support needs. With the small number of mainframe staff available to complete maintenance and updates to these libraries, the Department will look for appropriate monitoring software to further reduce risk.

Finding No. 3: Disaster Recovery Strategies Need Attention

The auditors found that it was not clear if the Department's backup and recovery procedures include all files needed for restoration of OBIS, and further found that the State Data Center (SDC), which manages agency systems and data, does not have detailed procedures for recovery of infrastructure, applications, and data critical for agency business continuity. They noted that routine testing has not included mainframe recovery where OBIS resides resulting in the

Department not having sufficient assurance that OBIS could be timely recovered in the event of a disaster. We agree with this finding as mainframe testing and recovery has not been fully completed since 2005, before systems were consolidated at the SDC. However, the Department does have some level of confidence that it can fully recover from a disaster based on a 2011 independent review and testing of business continuity and disaster recovery plans. The Department also successfully tested partial recovery of mainframe systems in 2011 at the SDC. In addition, while this audit was in progress, the Department had to recover mainframe production data due to an infrastructure failure at the SDC. Following business continuity and disaster recovery plans, data recovery was completed in a matter of hours, thus giving the Department some confidence that full mainframe recovery can be routinely performed. In order to reduce risks further of OBIS systems and data recovery, the Department plans to participate in the upcoming SDC full mainframe recovery test scheduled for January 2013, and will work with the SDC to update those plans to include the steps the SDC will take to recover systems infrastructure. .

Finding No. 4: System Security Should be Improved

The auditors noted that the Department has done much to establish a security management program and provide logical access controls to protect OBIS and its data, yet the efforts were not always sufficient. They also noted that a separate audit of controls of the State Data Center identified security weaknesses that increased risk of system compromise. We agree with auditors that security controls and measures at the Department need improvement, and are awaiting receipt of the confidential letter in order to appropriately address risks identified.

The Oregon Employment Department takes the results of this audit seriously, and worked closely with the auditors throughout the duration of the audit to review and correct issues as they were identified. We have benefited greatly from the audit process and the results and believe that we have taken appropriate corrective action to rectify all of the findings and implement the recommendations contained in the report. If you require any further information, please contact David Gerstenfeld, Assistant Director for Unemployment Insurance at (503) 947-1707 or at David.K.Gerstenfeld@state.or.us .

Sincerely,

Laurie A. Warner
Director

Cc: William Garber, Deputy Director SOS Audits Division
Neal E. Weatherspoon, Audit Manager, SOS Audits Division
Erika A. Ungern, Principal Auditor, SOS Audits Division
David K. Gerstenfeld, Assistant Director, Unemployment Insurance

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of her office, Auditor of Public Accounts. The Audits Division exists to carry out this duty. The division reports to the elected Secretary of State and is independent of the Executive, Legislative, and Judicial branches of Oregon government. The division audits all state officers, agencies, boards, and commissions and oversees audits and financial reporting for local governments.

Audit Team

William K. Garber, CGFM, MPA, Deputy Director

Neal E. Weatherspoon, CPA, CISA, CISSP, Audit Manager

Erika A. Ungern, CISA, Principal Auditor

Glen D. Morrison, CISA, Staff Auditor

Rebekah D. Tambe, Staff Auditor

Matthew C. Owens, Staff Auditor

This report, a public record, is intended to promote the best possible management of public resources. Copies may be obtained from:

internet: http://www.sos.state.or.us/audits/index.html

phone: 503-986-2255

mail: Oregon Audits Division
255 Capitol Street NE, Suite 500
Salem, OR 97310

The courtesies and cooperation extended by officials and employees of the Oregon Employment Department during the course of this audit were commendable and sincerely appreciated.