

AUDIT REPORT

Oregon Department of Human Services: Security Controls for Computer Applications



Bill Bradbury, Secretary of State
John Lattimer, Director, Audits Division

Summary

PURPOSE

The objective of our audit was to evaluate the adequacy of the Department of Human Services security controls for computer applications intended to protect health and welfare information.

RESULTS IN BRIEF

Security has not received an appropriate level of attention and resources. As a result, the department is unable to protect confidential health and welfare information and has incurred loss due to employee theft.

RECOMMENDATIONS

We recommend that executive management make security a priority by:

- Establishing a security framework and developing a long-range security plan that identifies and prioritizes security needs based on risk.
- Immediately implementing those recommendations for which it has the available resources.

- Immediately remove confidential information from its manuals and websites.

We recommend that the department:

- Recover overpayments made to clients.
- Investigate cases in which fraud may have occurred.
- Develop and implement policies and procedures addressing related parties.
- Provide training to staff on how to identify potential fraud and develop guidelines for referring cases for investigation.

We recommend that branch managers ensure that welfare cases are more closely reviewed to ensure that appropriate payments are made and case management activities are performed.

AGENCY RESPONSE

The Department of Human Services generally agrees with the recommendations.

Background

The Department of Human Services (department) was created by the 1971 Oregon Legislature as the state's health and human services agency. The department is comprised of six divisions and three program offices. In addition, there are more than 150 field offices that directly serve several hundred thousand Oregonians through programs such as food stamps, Medicaid, long-term care, child protection and mental health care.

To administer the health and welfare programs, the department relies on numerous computer applications. The department's Office of Information Services provides systems development support for these systems.

Department Funding

The department's legislatively adopted budget for the 99-01 biennium shows:

- General fund and lottery funds of \$2.284 billion dollars, or 21.5 percent, of the state's total.
- Other funds of \$708 million dollars, or 5 percent, of the state's total.
- Federal funds of \$4.356 billion dollars, representing 76 percent of the state's total federal funds.

The legislatively adopted budget for the department's Office of Information Services for the 1999-01 biennium dedicated more than \$21 million dollars to systems engineering, which includes application systems support.

Security Framework

For security to be successfully implemented and maintained, executive management must clearly establish and communicate to all appropriate parties the framework and intent of security. The framework should establish the organization's overall approach to security and internal control to ensure protection of resources and maintain integrity of computer systems. Specifically, the framework should:

- Comply with overall business objectives.
- Minimize risks through preventive measures, timely identification of irregularities, limitation of losses and timely restoration of business processes.

- Specify the purpose and objectives of security, the management structure and the scope within the organization.
- Define and assign responsibilities for implementation of security at all levels.
- Specify the definition of penalties and disciplinary actions associated with failing to comply with security and internal control policies.
- Define criteria for periodic reevaluation of the framework to support responsiveness to changing organization, environmental and technical requirements.

Audit Results

The Department of Human Services relies on various manual and automated controls to safeguard information. However, security has not received an appropriate level of attention and resources necessary to adequately protect its systems and data. Because of the sensitive nature of the department's business processes, we have issued a separate report outlining specific details of our work as well as recommendations to improve systems security. This confidential report was prepared in accordance with ORS 192.501 (23), which allows exemption of such information from public disclosure.

The department performed an analysis of its security system in 1991 that identified several weaknesses. In addition, internal auditors made specific recommendations to management in a report dated May 14, 1999 to improve its security systems. Although management hired a security manager, as recommended, as of April 2001, it has not implemented any other recommendations.

Because executive management has not taken action to address known security issues, the department is unable to keep health and welfare information confidential and has suffered loss due to employee theft.

Confidential Health and Welfare Information Was Disclosed on the Internet

The department is mandated in statute to make and enforce rules and regulations governing the custody, use and preservation of the contents of any record, file, paper or communication relating to welfare applicants and recipients. In addition, Congress recognized the need for national patient record privacy standards in 1996 when it enacted the Health Insurance Portability and Accountability Act.

During the course of our audit, we found that the department placed on its websites employee training manuals that contained confidential client and provider information. This information included active clients' social security numbers, case numbers, addresses, telephone numbers, medical payments issued, and sensitive narratives about the clients. Thus, this confidential health and welfare information was available to anyone with access to the Internet.

When brought to the attention of management, it indicated that the problem would be addressed immediately. As of August 2001, however, the department's websites continued to allow access to various manuals that contain confidential information.

As a result, the department may risk violating state and federal laws that require the safekeeping of welfare information and consequently may incur penalties.

Weak Security Controls Contributed to Employee Theft

To reduce the possibility of employee theft, the department should allow individuals access only to information needed to perform their jobs. Providing greater access may allow employees to circumvent controls, thus placing the department at risk of fraud, misuse and unauthorized alteration.

Since 1995, the department has incurred more than \$200,000 in loss directly related to employee theft. Review of those case files indicates that the employees involved in the thefts had inappropriate system access. In some instances, that access contributed to the employees' ability to commit theft.

One example occurred in October 2000, when an employee was dismissed for using client benefits for her own use. The employee was able to access client information, establish benefits, and obtain and use the benefits on two occasions.

Conclusion and Recommendation

This situation exists because executive management has not made security of its systems a priority. In addition, the department has not identified and prioritized its security needs and established a long-range plan to build adequate security into its systems. Immediate action can be taken on some of the recommendations made by the department's internal auditors and as communicated in our separate report. However, the cost of implementing other recommendations may require significant commitment and long-range planning on behalf of department management.

We recommend that executive management make security a priority by:

- Establishing a security framework and developing a long-range security plan that identifies and prioritizes security needs based on risk.
- Implementing immediately those recommendations for which it has the available resources.

We also recommend that management immediately remove confidential information from its manuals and websites.

Other Matters

During the course of our audit, we found that management does not always perform a sufficient review of welfare client cases to ensure appropriate payments are made and that case management activity is performed. Specific examples follow.

Case Manager Provided Incorrect Information

Oregon law requires that when a client is living with another individual, the client disclose the financial agreement between the parties. This information is critical because it affects the amount of benefits that the client receives.

During our review, we identified one department employee who misreported the financial agreement between herself and her son. As a result, this employee's son received more benefits than he should have. The employee confirmed that she knew the information provided would affect the level of benefits paid to her son.

We also found that documentation supporting other payments issued to the employee's son was limited. We asked the branch manager to review and verify that those payments were appropriate. The branch manager was unable to find satisfactory

support for \$991 in payments made to the client. Included in this total was \$450 for housing, \$350 for emergency assistance, and \$100 for personal needs.

In addition, the case manager, a friend of the employee, paid the employee's son \$87 for work supplies even though the request had been denied by the assessment worker. According to the Branch Manager, if the assessment worker denies a request the caseworker should not overrule the decision.

Caseworkers Inappropriately Issued Domestic Violence Funds

The department provides emergency assistance up to \$1,200 to stabilize a client's living situation in cases of domestic violence. The intent is to keep the victim safe, remove the violence as early as possible and, if needed, help the client flee the situation.

During the course of our audit, we identified three domestic violence payments to one client, totaling almost \$1,350, that did not meet the department's guidelines. We also found that the caseworker did not develop a case plan to deal with the alleged violence as prescribed in agency guidelines.

When brought to the manager's attention, she also reviewed the supporting documentation and discussed the file with the caseworkers. The manager agreed that the funds were issued inappropriately because there were no verifying facts about safety concerns.

Although domestic violence funds can be issued to help a family flee a violent situation, in this instance the funds were issued to move the client closer to the former spouse, the alleged perpetrator.

A Case Manager Did Not Report a Potential Fraud

In May 2000, a caseworker discovered one client, who had been receiving disability benefits, withheld employment information at the time of recertification. Although the client reported she had no income, the client had actually been employed for approximately 10 months at one of the department's branch offices. The caseworker referred the case to the overpayment unit for recovery, but she did not refer the case for investigation as a potential fraud. Furthermore, the overpayment unit did not begin action to recover the funds until May 2001.

As a result, the client received excess benefits totaling \$5,917 in cash and food stamp benefits, which was not investigated and potentially prosecuted.

DHS Employee Authorized Herself to Use a Family Member's Welfare Benefits

During our review, we identified instances in which clients had authorized department employees to pick up and use their food stamp benefits. In one instance, the employee authorized herself by signing the client's name although the employee did not have legal authority to sign on behalf of the client. In this case, the client had previously authorized this employee (a relative) and did provide a new authorization upon request.

Unless a review of case file information is conducted, the department does not have a method for identifying all circumstances in which an employee has been given, or taken, such authorization. As a result, the department is at risk that an employee could misappropriate funds for his or her personal use.

Conclusion and Recommendation

For these four examples, management did not perform a sufficient review of the welfare cases and did not ensure that case management activities were performed. In addition, the department does not have policies and procedures addressing related parties, and has not effectively trained staff how to identify potential fraud and when to refer for investigation.

We recommend that branch managers ensure welfare cases are more closely reviewed to ensure that appropriate payments are made and case management activities are performed.

We also recommend that the department:

- Recover overpayments made to the above clients.
- Investigate cases in which fraud may have occurred.
- Develop and implement policies and procedures addressing related parties. At a minimum, branch management should closely monitor those case files.
- Provide training to staff on how to identify potential fraud and develop guidelines for referring cases for investigation.

Objectives, Scope and Methodology

The objective of our audit was to evaluate the adequacy of the department's security controls for computer applications intended to protect health and welfare information. These controls include policies and procedures to establish the department's security framework and intent, ensure that security is addressed as part of every system development and modification effort, and ensure that security administration activities are effective. Although much of our

fieldwork was performed at selected branch offices, we also evaluated most of the department's centralized security policies, procedures and functions. To select the branch offices included in our testing, we evaluated the access awarded to staff within each branch, compared the services offered and considered prior occurrences of fraud.

We conducted our fieldwork at various intervals between December 1999 and May 2001. To achieve our audit objective, we interviewed department personnel, examined documents supporting security controls and procedures, and observed security practices. We evaluated compliance with applicable laws, rules, and regulations pertaining to systems security. We also designed and performed tests to determine if selected controls existed and were working as intended.

Scope Limitation

During the audit, we reviewed reports of employee theft to identify potential risk indicators of fraud. One such indicator was an employee having the same address as a welfare client. To evaluate this risk, we requested that the department's Office of Information Systems (OIS) provide computer files containing relevant client payment information. Although the department complied with our request, the information provided was not complete. During our fieldwork, we identified additional payment information that should have been included in the computer files provided by OIS. As a result, the client files reviewed and our conclusions may have been different.

Information System Controls

Information system controls are typically classified as general controls or application controls. General controls protect the environment in which software applications process data. Application controls relate to specific processing requirements of individual software applications. Key to the effective operation of both general and application controls is providing processes to ensure systems security.

Security controls are designed to protect information against unauthorized use, disclosure or modification, damage or loss. These controls ensure that access to systems, data and programs is restricted to authorized users and takes into consideration confidentiality requirements, access control, user identification, users demonstrated need, incident escalation procedures, security administration, and user training and monitoring.

During our audit we used the Information Systems Audit and Control Foundation's (ISACF) publication "Control Objectives for Information and Related Technology" (COBIT) to identify generally accepted and applicable internal control objectives and practices for security. ISACF is a worldwide organization dedicated to research, develop, and publicize generally accepted information technology control objectives and audit guidelines. We conducted our audit according to generally accepted government auditing standards.



Oregon

John A. Kitzhaber, M.D., Governor

Department of Human Services

Office of the Director
500 Summer St. NE, E15
Salem, OR 97301-1097
503-945-5944
Fax: 503-378-2897
TTY: 503-945-5928

August 8, 2001

John Lattimer, Director
Audits Division, Secretary of State
255 Capitol St. NE Suite 500
Salem, OR 97310

Dear Mr. Lattimer,

The purpose of this letter is to respond to the Systems Security Audit issued by your office. The Department of Human Services is in general agreement with the findings and recommendations. The importance of appropriate information systems security combined with improved business practices are a priority for us, particularly during this time of transition to an integrated department. As such, we will elevate the discussion about security and implement those recommendations that can be done immediately within available resources. We have already removed confidential information that was on our websites; in addition, will be taking the following actions:

1. Through our recently established security task group, develop a long-term security framework that addresses technology and business practices issues with priorities for implementation.
2. In terms of the employee theft cited in your report, we had previously taken action on those cases; however, we will also investigate the systemic issues associated with them and take actions to prevent recurrences.
3. Develop a communication and training plan around security issues.
4. Review overpayment procedures to ensure recovery of identified overpayments made to clients.
5. Develop policies regarding related parties.

We commend your audit team and appreciate the recommendations that underscore the need to implement security as a routine part of our business.

Sincerely,

Bob Mink
Director

Cc: Mike Greenfield, Director, Department of Administrative Services
"Assisting People to Become Independent, Healthy and Safe"
An Equal Opportunity Employer

This report, which is a public record, is intended to promote the best possible management of public resources. Copies may be obtained by mail at Oregon Audits Division, Public Service Building, Salem, Oregon 97310, by phone at 503-986-2255 and 800-336-8218 (hotline), or internet at Audits.Hotline@state.or.us and <http://www.sos.state.or.us/audits/audithp.htm>.

AUDIT ADMINISTRATOR: Nancy L. Young, CPA, CISA

AUDIT STAFF: *Jamie Breyman • Cynthia Cox • Darrin Hotrum • Donna Ross • Virginia (Ginger) Teller • Raul Valdivia*

DEPUTY DIRECTORS: Sharron E. Walker, CFE, CPA • Cathy Pollino, CFGM, MBA

The courtesies and cooperation extended by the officials and staff of the Department of Human Services were commendable and much appreciated.

Auditing to Protect the Public Interest and Improve Oregon Government

OFFICE OF THE
SECRETARY OF STATE

Bill Bradbury
Secretary of State



AUDITS DIVISION
John Lattimer
Director

(503) 986-2255
FAX (503) 378-6767

Auditing for a Better Oregon

The Honorable John Kitzhaber, M.D.
Governor of Oregon
254 State Capitol
Salem, Oregon 97310-4047

Bob Mink, Director
Oregon Department of Human Services
500 Summer Street NE
Salem, Oregon 97310-1012

The attached report presents the results of our evaluation of security controls at the Department of Human Services (department). During our review, we reviewed policies and procedures relating to security, interviewed personnel, examined documents supporting security controls, and observed security practices.

During the review, we found that security has not received an appropriate level of attention and resources. As a result, the department is unable to protect confidential health and welfare information and has incurred loss due to employee theft. The report includes recommendations intended to improve the department's security. Specifically, the department's executive management should make security a priority by establishing a security framework and developing a long-range plan that identifies and prioritizes security needs based on risk.

Because of the sensitive nature of the department's business processes, we have issued a separate report outlining specific details of our work as well as recommendations. This confidential report was prepared in accordance with ORS 192.501 (23), which allows exemption of such information from public disclosure.

OREGON AUDITS DIVISION

John N. Lattimer
Director

Fieldwork Completion Date:
May 31, 2001