Report No. 2009-05

February 18, 2009

Kate Brown, Secretary of State

Charles A. Hibner, Director, Audits Division

Secretary of State Audit Report

Department of Administrative Services: Enterprise Security Office Review

Summary

BACKGROUND AND PURPOSE

The Department of Administrative Services (department) is the central administrative agency of Oregon state government.

In 2005, the legislature enacted Oregon Revised Statute (ORS) 182.122 giving the department responsibility and authority for information systems security in the executive department. Department management assigned primary responsibility for compliance with this statute to its Enterprise Security Office (ESO). The ESO operating budget for the 2007-2009 biennium was approximately $11.3 million.

The objectives of this audit were to evaluate the ESO's progress in fulfilling the requirements of ORS 182.122 and determine whether the ESO appropriately managed the enterprise infrastructure projects it undertook.

RESULTS IN BRIEF

We found that the department implemented forensic techniques and controls and developed policies and plans for responding to security incidents. However, the department had not:

- developed complete security plans and associated standards, policies, and procedures;
- conducted vulnerability assessments of agency information systems;
- reviewed or verified the security of information systems; or
- ensured remedial actions were undertaken to resolve identified security issues.

As a result, the department had not fully complied with the statutory mandate to establish an enterprise security system or program to protect the availability, integrity or confidentiality of the state's information systems.

The department also did not appropriately manage its project to implement centralized Identity and Access Management (I&AM) or its project to issue digital certificates. As a result, it is unlikely the state will realize appreciable security benefit from the approximately $14 million the ESO spent on these projects.

RECOMMENDATIONS

We recommend that the department:

- develop a comprehensive state information security plan with associated standards, policies and procedures to ensure appropriate security measures are defined for all critical information assets or asset classes;
- ensure vulnerability assessments of agency information systems are conducted and obtain and utilize the results of assessments performed by agencies for security planning purposes;
- develop and implement plans to review and verify the security of information systems operated by or on behalf of state agencies;
- develop procedures to ensure that appropriate remedial actions will be taken to resolve identified security issues;
- establish an appropriate project management framework to better control information technology security projects so that requisite project management tasks are completed before projects are approved; and
- discontinue further I&AM development until the department has established a business need, obtained sufficient stakeholder buy-in, and developed a viable project plan.

AGENCY'S RESPONSE

The Department of Administrative Services partially agrees with four of the recommendations and agrees with two. The department's response is attached to this report, beginning on page 7.

Background

The Department of Administrative Services (department) is the central administrative agency of Oregon state government.

In 2005, the Oregon Legislature passed House Bill 3145, which was enacted into law as Oregon Revised Statute (ORS) 182.122. This statute gave the department broad responsibility and authority for information systems security in the executive department, including taking all measures reasonably necessary to protect information systems and their data. Although the statute assigns ultimate responsibility for security to the department, it requires the department to collaborate with affected agencies.

Department management assigned primary responsibility for compliance with this statute to the manager of the department's Enterprise Security Office (ESO). The ESO is a component of the department's Enterprise Information Strategy and Policy Division.

The ESO operating budget for the 2007-2009 biennium was approximately $11.3 million. These funds came from assessments the department charged to other state agencies. In addition, since May 2005, the ESO spent approximately $11.5 million from proceeds of Certificates of Participation (COP) to partially fund security infrastructure projects.

The objectives of this audit were to evaluate the ESO's progress in fulfilling the requirements of ORS 182.122 and to determine whether the ESO appropriately managed the enterprise infrastructure projects it undertook.

Audit Results

The Department Had Not Completed All Mandated Security Requirements

ORS 182.122 requires the department to take all measures reasonably necessary to protect the availability, integrity or confidentiality of information systems or the information stored in information systems. It also requires the department to:

- establish information systems security plans, standards, policies, and procedures;
- conduct vulnerability assessments of agency information systems;
- verify the security of information systems;
- ensure remedial actions are undertaken when necessary;
- develop policies to respond to security incidents; and
- establish use of forensic techniques.

Within the context of generally accepted security standards and practices, these security elements are a partial but vital subset of measures that would be reasonably necessary to ensure security of enterprise information assets.

Although the statute does not require the department to follow a particular security standard, the statute's requirements are congruent with the generally accepted international security standards found in ISO 27001 and 27002.[1]

Using these standards, we evaluated the department's efforts to comply with specific requirements of the statute. We found that the department implemented forensic techniques and controls and developed policies and procedures for responding to security incidents. However, the department had not:

- developed complete security plans and associated standards, policies, and procedures;
- conducted vulnerability assessments of agency information systems;
- reviewed or verified the security of information systems; or
- ensured remedial actions were taken to resolve identified security issues.

As a result, we concluded that the department had not fully complied with the statutory mandate to establish an enterprise security system or program to protect the availability, integrity or confidentiality of the state's information systems.

The Department Did Not Develop an Adequate or Complete Security Plan

ORS 182.122 (2) specifies that "The Oregon Department of Administrative Services has responsibility for and authority over information systems security in the executive department, including taking all measures reasonably necessary to protect the availability, integrity or confidentiality of information systems or the information stored in information systems." This section further requires the department to collaborate with other state agencies and "establish a state information systems security plan and associated standards, policies and procedures."

Security standard practices outlined in ISO 27001 indicate that security plans should be formulated using a systematic process. That process should begin by identifying assets and assessing the associated risks posed by threats and vulnerabilities. Once this has been

[1] International Standard ISO/IEC 27001and 27002 are official publications of the International Organization for Standardization and the International Electrotechnical Commission.

determined, controls such as those found in ISO 27002 should be chosen and applied to protect assets based on the risk tolerance of an organization and relative importance of the respective assets or asset classes.

ESO staff identified a variety of documents they said represented the state security plan. These documents included the enabling legislation (ORS 182.122), an associated Oregon Administrative Rule (OAR 125-800), seven high-level policies, and the ESO's draft strategic plan. The ESO also indicated it was developing an enterprise security architecture, and would include that documentation in the state security plan once the architecture was completed. Staff also indicated that no associated standards or procedures had been developed.

We evaluated the above documents to determine whether they fulfilled the requirements of section (2) of ORS 182.122. We also evaluated the strategies ESO staff used to produce those deliverables. We found that the state security plan included some important elements of security but did not effectively identify or address how information assets would be secured.

Notably absent from the state security plan were details regarding how the state's most critical and valuable information assets and infrastructure would be protected. For example, the state security plan did not address how the State Data Center and the applications it hosts would be secured or how confidential information should be safely stored or transmitted. Furthermore, the state security plan did not provide enterprise standards for common security elements such as identity and access management, encryption, or wireless transmissions.

Although the ESO did not have an adequate state security plan, it did assign affected state agencies to develop their own security plans. Department policy number 107-004-052 requires state agencies to "…develop and implement information security plans, policies and procedures that protect its information assets from the time of creation, through useful life and through proper disposal." However, the policy did not require the plans to be completed until July 2009. As of August 2008, no state agencies, including the department, had submitted their security plans to the ESO for review. In addition, the ESO was unsure how these plans would be used to achieve ORS 182.122 directives after those plans are submitted.

We believe one reason the security planning weaknesses occurred was that ESO staff did not follow some key generally accepted security planning practices and methodologies as outlined in ISO 27001, including identifying:

- the assets to be protected;
- specific threats to assets;
- the vulnerabilities (as discussed later in this report) that might be exploited by the threats; and
- options for mitigating the associated risks.

Rather, the ESO chose in 2007 to contract with an external firm to perform high-level business risk assessments at various agencies. This approach provided some insights regarding gaps in basic security processes. However, it focused on policy level issues and did not address technical vulnerabilities associated with the State Data Center or with critical enterprise applications.

Based on the above, we concluded that the department had not fully complied with section (2) of ORS 182.122. As a result, the state did not have a uniform or enterprise approach for securing information systems. In effect, the current state of statewide security plans, policies, standards and procedures has not significantly changed since the enactment of the statute in 2005. Thus, the state has not yet realized the benefits that could have been derived from taking the prescribed centralized security planning strategy.

We recommend the department fully comply with ORS 182.122 section (2) by developing a comprehensive state information security plan with associated standards, policies and procedures. The plan, including associated deliverables, should be formulated using recognized international methodologies and standards, such as those found in ISO 27001. In developing the state security plan, the department should ensure appropriate security measures, such as those found in ISO 27002, are defined for all critical information assets or asset classes based on their vulnerabilities, threats, and overall risk.

Agency's Response:

The department's response is attached to this report, beginning on page 7.

The Department Did Not Conduct Vulnerability Assessments of Agency Information Systems

Section (3)(c) of ORS 182.122 requires the department to "conduct vulnerability assessments of agency information systems for the purpose of evaluating and responding to the susceptibility of information systems to attack, disruption or any other event that threatens the availability, integrity or confidentiality of information systems or the information stored in information systems." Section (4) requires the department to contract with qualified vendors to conduct these vulnerability assessments.

According to ISO 27001, the information security risk assessment process should include steps to identify:

- information assets,

- threats to those assets,
- vulnerabilities that might be exploited by the threats, and
- the impacts or losses that may occur if vulnerabilities are exploited.

Information derived from vulnerability assessments enables managers to select controls that would most effectively protect specific information assets. Thus, conducting periodic vulnerability assessments is an integral part of establishing and maintaining an organization's security plan or program.

We evaluated the department's efforts to comply with the ORS 182.122 requirement to conduct vulnerability assessments. We found that the department had not conducted vulnerability assessments or contracted for that work to be done. Rather, it developed a master contract with a vendor to allow agencies to conduct vulnerability assessments at their discretion.

ESO staff indicated that as of June 2008, only two agencies used the contract for vulnerability assessment work. However, those agencies did not provide the ESO the results of those engagements.

The absence of current information regarding vulnerabilities and threats significantly weakened the department's security planning process. In addition, it increases the risk that information system weaknesses may not be identified and their associated risks appropriately mitigated.

We recommend department management ensure vulnerability assessments of agency information systems are conducted as required by ORS 182.122 and that the department obtain and utilize the results of assessments performed by agencies for security planning purposes.

Agency's Response:

The department's response is attached to this report, beginning on page 7.

The Department Did Not Review or Verify the Security of Information Systems

Subsection (3)(a) of ORS 182.122 requires the department to "review and verify the security of information systems operated by or on behalf of agencies."

ISO 27002 (section 15.2) indicates that "The security of information systems should be regularly reviewed. Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with applicable security implementation standards and documented security controls."

We noted that the department had not effectively reviewed or verified the security of agency information systems. ESO staff indicated their work in this area centered on the high-level business risk assessment. Staff also indicated that they had not yet developed procedures for performing a security review and planned to perform such reviews only at the request of agencies.

Without such reviews, the department would not necessarily know whether security policies, procedures or technical controls are operating as intended.

We recommend the department develop and implement plans as required by ORS 182.122 to review and verify the security of information systems operated by or on behalf of state agencies.

Agency's Response:

The department's response is attached to this report, beginning on page 7.

The Department Did Not Ensure Remedial Actions Were Taken to Resolve Identified Security Issues

Subsection (7) of ORS 182.122 requires the department to ensure that reasonably appropriate remedial actions are undertaken when the department finds that such actions are necessary due to weaknesses noted in vulnerability assessments, department reviews of agency security, results of forensic work, or in other evaluations and audits.

ISO 27002 (section 13.2) states "A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents."

We evaluated the department's compliance with this requirement. We found that the department had no formal plans to address issues that would be identified in vulnerability assessments. In addition, ESO staff indicated they did not follow up on findings contained in Secretary of State audit reports due to staffing and budget constraints.

ESO methodology to address this requirement was to rely on state agencies to ensure remedial actions are taken to resolve security issues. ESO staff indicated they planned to take necessary actions should agency efforts prove to be unsatisfactory. However, the ESO did not have formal procedures to ensure appropriate actions would be taken.

Based on the above, we concluded that the department's efforts were not sufficient to ensure appropriate remedial actions would be taken to resolve previously identified security issues.

Absence of a system to ensure remedial actions are undertaken increases the risk that security risks, threats and vulnerabilities will not be timely addressed.

We recommend the department develop procedures to ensure that appropriate remedial actions will be taken to resolve security issues identified in vulnerability assessments, department reviews of agency security, results of forensic work, or in other evaluations and audits.

Agency's Response:

The department's response is attached to this report, beginning on page 7.

The Department Had Policies and Plans for Responding to Security Incidents

Section (5) of ORS 182.122 directs the department to develop policies for responding to events that damage or threaten information systems and their data. It also defines what items must be specifically addressed in the policy.

ISO 27002 indicates that "Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported."

We evaluated the department's efforts to comply with this requirement. We found that the ESO had developed high-level plans for responding to security incidents. In addition, during November 2008, the department issued policy 107-004-120 *Information Security Incident Response* that more broadly defined the state's incident response program.

With the issuance of the above policy, we concluded that the department substantially complied with section (5) of ORS 182.122.

The Department Implemented Forensic Techniques and Controls

Subsection (6) of ORS 182.122 requires that the department, after consultation and collaborative development with agencies, implement forensic techniques and controls for the security of information systems. The ORS also specifies items that must be included in these techniques and controls, such as using specialized expertise and tools for analysis.

We found that the ESO complied with this section of ORS 182.122. Specifically, it ensured staff obtained the necessary training to gain specialized expertise and procured relevant forensic tools.

The ESO Did Not Effectively Manage Enterprise Security Infrastructure Projects

Organizations should manage security infrastructure projects to ensure they conform to enterprise security strategies and satisfy business needs. In that regard, a project management framework should be in place to ensure selected solutions conform to the chosen technological direction and are cost effective.

The project management framework should ensure that approval of enterprise security projects is based on the results of a thorough business needs analysis, feasibility studies and an appropriate cost-benefit analysis. Proper consideration should also be given to alternative solutions. In addition, the framework should ensure comprehensive project plans are developed to define how each phase of the project will be completed and the resulting system placed into production. To ensure project buy-in, the above plans should be reviewed and approved by affected stakeholders.

In January 2005, the ESO initiated a project to implement an automated enterprise system to manage user accounts and privileges. This project was initially budgeted at $13.4 million. ESO management also began a project in June 2006 to develop an enterprise program for issuing digital certificates. This project was to cost approximately $300,000.

We evaluated the above security infrastructure projects to determine whether they were appropriately managed to safeguard the state's investment. In the case of both projects, we found that ESO staff had not:

- established a viable business case or justification;
- performed appropriate feasibility or cost-benefit analysis;
- developed complete or appropriate project plans;
- defined the project's end state or how the system would fit into the state's current security architecture;
- obtained stakeholder commitment or approval or defined who would be responsible for operating the resulting systems; or
- appropriately considered alternative solutions.

In spring 2008, the ESO discontinued its plans to issue digital certificates. It did so after acquiring the required infrastructure and issuing only 100 certificates of the 2,000 it purchased.

As for the enterprise Identity and Access Management (I&AM) project, ESO staff indicated the COP funding expired on June 1, 2008. At that time, progress toward implementing an enterprise system was insignificant and the ESO did not have a viable plan to fund or fully implement its software solution. Only two minor agency applications were using the system and the ESO had no definitive plans to integrate other agency applications.

Furthermore, ESO managers were uncertain how much additional funding would be necessary to integrate other applications into the I&AM system. During our audit,

ESO staff was in the process of developing a business case to identify where I&AM would be hosted and how future operations would be funded. In addition, final ownership and responsibility for operating the system had not yet been determined.

Based on the above, we concluded it was unlikely the state would realize appreciable security benefit from the approximately $14 million the ESO has spent on these security projects to date. Approximately $11.5 million of this amount came from COP funding with the remainder from the ESO's operating budget.

These projects did not succeed because the ESO did not perform the necessary groundwork to establish viable business cases before initiating the projects. The ESO also lacked the necessary commitment from other state agencies to adopt the solutions. In addition, they did not establish either solution as an enterprise standard. Furthermore, the department did not have an appropriate project management framework to ensure these and other critical issues were resolved prior to project initiation or approval.

We recommend the department establish an appropriate project management framework to better control its information technology security projects. That framework should ensure requisite project management tasks are completed before projects are approved.

We also recommend the department discontinue further I&AM development until it has established a business need, obtained sufficient stakeholder buy-in, and developed a viable project plan.

Agency's Response:

The department's response is attached to this report, beginning on page 7.

Objectives, Scope and Methodology

The objectives of our audit were to determine:

1. the status of the ESO's compliance with the requirements of ORS 182.122, and
2. whether the ESO appropriately managed the enterprise infrastructure projects it undertook to safeguard assets.

To achieve these objectives, we interviewed various department personnel, reviewed department documentation, and conducted tests. Tests included evaluation of project planning documents and verification of the existence of supporting documentation.

The scope of our review focused on controls implemented and actions taken by the ESO as they relate to the above audit objectives.

We used the IT Governance Institute's (ITGI) publication, "Control Objectives for Information and Related Technology," (CobiT) and International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 and 27002 to identify generally accepted and applicable internal 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 we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Oregon
Theodore R. Kulongoski, Governor

Department of Administrative Services
Office of the Director
155 Cottage Street NE, U20
Salem, OR 97301-3966
(503) 378-3104
FAX (503) 373-7643

February 12, 2009

Neal Weatherspoon, CPA, CISA, CISSP
Information Technology Audit Manager
Oregon Audits Division
255 Capitol Street NE, Suite 500
Salem, OR 97301

RE: Department of Administrative Services: Enterprise Security Office Review

Dear Mr. Weatherspoon:

The Department of Administrative Services (Department) appreciates the work that the Secretary of State's Audits Division has done at the Enterprise Security Office (ESO) over the past 10 months. We also appreciate the opportunity to respond to the findings and recommendations from the draft report, which we received on January 27, 2009.

Management believes this audit focused narrowly on implementation of Oregon Revised Statute (ORS) 182.122. We also feel the report implied that minimal activity has occurred to reduce information security risk across the enterprise. Although the Department agrees that more remains to be done, we also believe it's appropriate to acknowledge the important work that the ESO, the State Data Center (SDC), and state agencies have done to strengthen information security.

Rather than focus exclusively on information systems, the ESO has approached enterprise security holistically. Although ORS 182.122 primarily addresses information systems, the Department believes that protecting the public's information assets requires a broad focus on all forms of information assets. Information security requires adherence to the principles of confidentiality, integrity, and availability of information. To be effective and comprehensive, security systems must encompass people, processes, and technology. Although the technology component is important, it is only one aspect; it should not be the sole focus of a security program. To complete the essential task of raising security awareness throughout the state, the Department must devote attention to business practices as well as systems. Ultimately, the goal is to achieve a more secure environment in which participants manage information security effectively.

Although this audit devoted attention mainly to the ESO, ORS 182.122 addresses the Department as a whole and the responsibilities of state agencies. The SDC is another key player in securing information systems. Significant work has occurred since the establishment of the SDC—work that has upgraded the protection of information systems

operated on behalf of agencies (e.g., monitoring network traffic, identifying and reacting to threats through intrusion detection, intrusion prevention, hardened perimeter, log aggregation, incident response, wireless security, etc.) All these efforts contribute to better security for information systems across the enterprise.

In addition, we should recognize that various agencies with information systems undergo regular audits by external entities, such as the Internal Revenue Service. They must promptly remediate identified issues, including those that affect system security. These actions also contribute to reducing security risk.

The ESO works in close partnership with agencies to reduce exposure to information security risk. The Enterprise Information Security Advisory Board, comprised of agency directors, reviews ESO policies, plans, and projects and makes recommendations to the Department's Director.

Another body that helps guide ESO projects and programs is the Information Security Council, whose membership includes 35 agencies with technology and business representatives. The ESO has delivered enterprise security policies and facilitated forums, workshops, and training events specific to information security. It has also provided templates for security- and incident-response plans. ESO shares agencies' best practice documents and other resources on the its Web site, and sends regular newsletters to agencies and local governments. Since enactment of ORS 182.122, the Enterprise Security Office has encouraged agencies to give security a higher profile in their organizations. Subsequently, many agencies have demonstrated their commitment to security by designating an information security officer, and the majority of them have earned professional information security credentials.

The efforts by the Department and the agencies reflect a commitment to improving the information security posture of the state. Information security is—and will continue to be—a priority of the Department. We believe that important progress has occurred throughout state government in all domains of information security. We acknowledge that we will always see a need for continuous improvement in this important endeavor. In particular, we will turn our focus to information systems as we attempt to manage the whole of information security.

The audit report states "the Department had not fully complied with the statutory mandate to establish an enterprise security system or program to protect the availability, integrity, or confidentiality of the state's information systems." In light of the accomplishments noted above, the Department generally agrees we have more work to do toward full implementation of ORS 182.122. Below are the specific responses to the recommendations provided in the audit report.

The report contained the following recommendation to the Department: **Develop a comprehensive state information security plan with associated standards, policies**

and procedures to ensure appropriate security measures are defined for all critical information assets or asset classes.

The Department partially agrees with this recommendation. ESO uses the International Standards Organization (ISO) 27001 and 27002 security standards throughout all its information security policies and plans. It is comprised of 11 domains, which includes the three domains that primarily address information systems security: Communications & Operations Management; Information Systems Acquisition, Development and Maintenance; and Access Control.

ESO was in the process of drafting a strategic security plan at the time of the audit. While this plan is largely complete, as a result of issues raised during the audit, ESO is drafting a more specific enterprise-level information security plan based on ISO 27002. It outlines specific activities, as well as roles and responsibilities for the ESO, SDC, and state agencies. The enterprise security architecture, currently under development, will be referenced in the plan.

The Department respectfully disagrees with statements about current enterprise information security policies. The audit appears to conclude that no policies were developed to address information system security. Of the seven information security polices adopted since 2007, five address securing and protecting information systems and data as outlined in the three ISO Domains noted earlier. These are: Acceptable Use Policy and Employee Security Policy – Access Control Domain; Information Asset Classification Policy and Transporting Information Assets Policy – Communications & Operations Management Domain and Access Control Domain; Controlling Portable & Removable Storage Devices Policy – Communications & Operations Management Domain, Information Systems Acquisition, Development and Maintenance Domain, and Access Control Domain.

The report contained the following recommendation to the Department: **Ensure vulnerability assessments of agency information systems are conducted and obtain and utilize the results of assessments performed by agencies for security planning purposes.**

The Department partially agrees with this recommendation. Assessments of state information systems have occurred, but the Department agrees more assessments are needed. Since 2006, ESO has contracted with a third party, accredited by Payment Card Industry (PCI), to conduct quarterly system security assessments for agencies that use e-commerce. The scans ensure compliance with PCI standards. ESO reviews all scan results, and agencies must remediate any identified issues. Re-scans then occur to verify compliance. Based on issues raised during the audit, the ESO arranged for a third party to conduct a vulnerability assessment at the SDC in late 2008. A plan is being developed that requires action from the SDC, ESO and agencies to address the identified issues. ESO will monitor implementation and remediation activities.

As mentioned in the audit, the ESO established a master contract in 2006 with a third-party consultant to provide security assessment and planning services for ESO and agencies to utilize. The ESO is developing a plan to increase agency information system vulnerability assessments through ESO's use of this contract tool, and as part of its quarterly third-party scanning activities. The assessment plan will include criteria for selecting agencies, determining the assessment scope, monitoring and verifying remediation activities, and tracking trends. Agency assessments will be under way by June, 2009.

In addition to information systems vulnerability assessments, the ESO has completed the second annual cycle of an Information Security Business Risk Assessment of 12 agencies. These agencies represent a cross-section of large, medium, and small organizations in various lines of business. An independent third party conducts this assessment, based on the 11 domains of ISO 27002, which includes the three domains related to information systems. Agencies received their individual results mapped to the Capability Maturity Model (developed by Carnegie Mellon), so they can track their progress on reducing risk. The results for 2008 show that participating agencies are making progress in reducing their risk exposure. This assessment occurs annually. Two new agencies are incorporated each year on a rotational basis, so more agencies have an opportunity to participate in this program. Results from this assessment inform the ESO's Key Performance Measure and the ESO Strategic Plan.

The report contained the following recommendation to the Department: **Develop and implement plans to review and verify the security of information systems operated by or on behalf of state agencies.**

The Department partially agrees with this recommendation. Work has been done to achieve PCI systems compliance. In addition to the PCI compliance scans, a third-party assessment of the information systems in the SDC occurred in late 2008. As noted previously, ESO will develop a plan to do more assessments of agency information system vulnerability as part of its third-party-conducted quarterly scanning activities. ESO will conduct agency information security assessments. ESO will continue to conduct, with third-party consultants, the annual Information Security Business Risk Assessment and follow-up on agency progress.

The report contained the following recommendation to the Department: **Develop procedures to ensure that appropriate remedial actions will be taken to resolve identified security issues.**

The Department agrees with this recommendation. The ESO security assessment plan will include a process for tracking issues and validating remediation. ESO will work with agencies to help them address assessment issues; however, each agency has responsibility for complying with federal and state regulations and enterprise policies, and remediating vulnerabilities in a timely manner.

The report contained the following recommendation to the Department: **Establish an appropriate project management framework to better control information technology security projects so that requisite project management tasks are completed before projects are approved.**

The Department partially agrees with this recommendation. Important elements of effective project initiation were missing in the Identity & Access Management (I&AM) project. There was no cost-benefit analysis or business case in 2005 when the enterprise project was authorized. In the future, ESO will work to complete appropriate and timely business case and feasibility studies at the initiation of large projects to assist in planning.

However, there was a project management framework established for the execution of the project. ESO uses Project Management Body of Knowledge (PMBOK) which is the accepted industry standard and is the framework selected and endorsed by the state. All the project managers who worked on I&AM have project manager certification. The I&AM project implemented the key elements of PMBOK, including project management plans, tracking issues, bi-weekly status reporting, contract management, bi-weekly stakeholder meetings, ongoing assessment of risks, and continuous process improvement. The project had third-party Quality Assurance oversight since inception. I&AM was implemented with the assistance of a consultant, this work followed state procurement processes and deliverables were reviewed for completeness and adherence to the contract prior to acceptance and payment.

The report contained the following recommendation to the Department: **Discontinue further I&AM development until the department has established a business need, obtained sufficient stakeholder buy-in, and developed a viable project plan.**

The Department agrees with this recommendation. In December, 2007, the project was ready to transition to a program; however the Policy Option Package (POP) presented to agency heads vetting the Department requests was not approved. At that time the infrastructure was complete, and additional applications and directories could be added to the initial ones developed in the project. The POP would have taken the project to a program that would have added applications and directories as agencies were ready. In order to determine if it was prudent to continue the project into limited production, and if the benefits would warrant continued investments, a business case was initiated in January, 2008. There will be no further work on the project until a decision is made on future action.

With respect to auditors' comments concerning digital certificates, the Department respectfully disagrees. ESO launched a digital certificate pilot project. The results provided valuable information on the viability of initiating an enterprise program. The pilot was implemented in conjunction with Oregon State Treasury. The goal was to better understand the implications of using digital certificates in a small, controlled environment. Infrastructure was implemented to accommodate the pilot but, to be cost-effective, it was not scoped to support an enterprise program. The ESO established a

State of Oregon Certificate Policy and Certificate Practice Statement, as well as a Certificate Policy Management Board comprised of agency representatives. All these are basic requirements of a Public Key Infrastructure program and were required for the pilot. The pilot provided many valuable lessons learned, however, based on agency interest, cost, and complexity. The Department determined that the state was not prepared to launch an enterprise digital certificate program at that time. A reference to digital certificates will be included in the Enterprise Security Architecture.

The Department appreciates the time and efforts of your staff in analyzing and discussing the important issues at the ESO. We partially agree with the findings as stated in the report. If you have any further questions, please don't hesitate to contact Theresa Masse, Chief Information Security Offer at (503) 378-4896 or Theresa.A.Masse@state.or.us. Thank you for the opportunity to respond.

Sincerely,

Scott L. Harra
Director
Department of Administrative Services

cc: Kristine M. Kautz, DAS Deputy Director
Charles Hibner, Director, Audits Division
Dugan A. Petty, State Chief Information Officer
Theresa A. Masse, State Chief Information Security Officer
Pamela J. Stroebel Valencia, DAS Chief Audit Executive

Secretary of State
Audits Division

255 Capitol St. NE, Suite 500
Salem, OR 97310

Auditing to Protect the Public Interest and Improve Oregon Government

AUDIT MANAGER: *Neal E. Weatherspoon, CPA, CISA, CISSP*

AUDIT STAFF: *Erika A. Ungern, CISA*
Kate Riley, CISA
Edward P. Angle, CFE
Teresa L. Furnish

DEPUTY DIRECTOR: *William K. Garber, MPA, CGFM*

Courtesies and cooperation extended by officials and staff of the Department of Administrative Services were commendable and much appreciated.

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

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

Phone: *at 503-986-2255*

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