Secretary of State Audit Report

Kate Brown, Secretary of State

Gary Blackmer, Director, Audits Division

State Data Center: Faster Progress Needed on Security Issues

Summary

The Department of Administrative Services (DAS) is responsible for providing centralized computer services for state agencies, including operation of the State Data Center (SDC). State agencies use SDC resources to operate hundreds of computer applications, including mission critical systems that often contain citizens' confidential information. State agencies depend on these computer systems to carry out their operations, and on the SDC to provide a secure computing environment for hosting these systems.

The 2005 legislature authorized DAS to create the SDC by consolidating data centers previously operated by state agencies. One of the primary goals of this project was to resolve agencies' security issues by combining infrastructure and management to form one protective security umbrella.

In our prior audits of the SDC we identified significant security weaknesses that collectively heightened the risk that applications hosted at the SDC could be compromised. During this audit we confirmed that most of these security issues continued to exist. Because of the duration of these weaknesses, we expanded our audit work to determine why they were not resolved. This report addresses management elements relating to this portion of our audit. We excluded details regarding security findings and recommendations from this report in accordance with ORS 192.501 (23), which exempts sensitive information from public disclosure.

We found that a majority of SDC security issues were long-standing weaknesses that could be successfully mitigated without new or overly complex technical solutions. Some could be resolved by appropriately configuring or implementing the security systems the SDC has already acquired, while others necessitated developing and implementing fundamental security policies, procedures and standards. To resolve other security issues would require little effort from SDC technical staff but would require the attention and resources of state agencies to implement their part of the solutions. Thus, resolving SDC security issues in a timely manner requires both effective security governance and management.

We also found the SDC shared services governance structure is not effective for managing security in a timely manner. This structure is a

maze of boards, committees and sub-committees where an inordinate time may pass between when matters are first discussed and when they are finally approved. We reviewed the status of four priority security projects sponsored by the governing boards to correct security weaknesses identified by our 2008 audit and a subsequent vulnerability assessment. By September 2009, considerable discussion had taken place but little action had occurred to resolve the associated security risks. Specifically, none of the groups had forwarded final recommendations to the governing board, proposed solutions only partially addressed the identified problems, and it was unclear when, or if, some of the security weaknesses would be resolved. Members of the SDC governance body, including SDC management, indicated that difficulties in reaching agreement significantly hampered progress in resolving critical security weaknesses and in implementing other needed changes at the SDC.

Finally, delays in resolving security weaknesses also occurred because SDC management did not clearly define or communicate security standards, or assign overall responsibility for managing the security function. Many security weaknesses continued to exist simply because nobody was given the authority or responsibility to resolve them. Others languished because SDC management had not developed an adequate security plan with associated standards and procedures to provide appropriate security expectations or requirements.

After we completed fieldwork, the Enterprise Security Office (ESO) issued a draft Information Security Plan for the State of Oregon and an associated Statewide Information Security Standards document. Both were approved in principle by the DAS director and presented to state agencies in December 2009. Among other requirements, these documents direct the SDC to develop information security standards, plans, policies, and procedures to ensure its assets are appropriately protected.

Recommendations

To more quickly address security matters, we recommend revising the shared services governance structure. In addition, SDC should formally assign security responsibilities to an individual, develop and implement a security plan, and aggressively address past recommendations in our audits and consultant reports. Our recommendations are detailed at the end of the report.

Agency response

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

Background

The Department of Administrative Services (DAS) is responsible for providing centralized computer services for state agencies, including operation of the State Data Center (SDC). The approved budget for the SDC for the 2009-2011 biennium is approximately $165 million. To cover operating costs, the SDC charges agencies for services according to a predetermined rate schedule.

The SDC is comprised of a complex and extensive inventory of computer operating system platforms, networks, and associated enterprise security infrastructure. State agencies use these resources to operate hundreds of computer applications, including mission critical systems. These applications often contain citizens' confidential information such as personal income tax returns, social security numbers, driver license information, and confidential medical records.

The 2005 legislature authorized DAS to create the SDC by consolidating data centers previously operated by state agencies. Prior to the creation of the SDC, state agency managers controlled how their data centers and systems would be secured, allowing them to choose a level of security effort based on their individual tolerance for risk. In this decentralized environment, some agencies did not allocate the resources and expertise necessary to keep up with increasingly more complex and urgent security demands. One of the primary goals of SDC consolidation was to resolve agencies' security issues by combining infrastructure and management to form one protective security umbrella.

State Agencies Depend on the SDC to Provide a Vital Layer of Security

By the beginning of 2007, 11 agencies had transferred their data center operations to the SDC. Because of difficulties encountered during this project, DAS management opted to relocate agency data centers to the SDC in their "as-is" state, stabilize operations, and then proceed with projects to reengineer the environment. As a result, many of the previously existing security issues, and the responsibility for resolving them, became the responsibility of the SDC.

As computer technology has advanced, state agencies have become dependent on computerized information systems to carry out their operations. In addition, heightened concerns of identity theft and the confidentiality of personal information have placed increasing security demands upon state agencies and the SDC to provide increased protection of these computer systems.

To counteract ever-growing threats to citizens' personal information, the 2007 legislature passed Senate Bill 583, requiring organizations to protect citizens' personally identifiable information by implementing robust security controls. As a result, agencies entrusted with personally

identifiable information must develop and maintain a security framework of policies, procedures, and technical strategies based on the business needs of its customers as well as current risk and vulnerability assessments. This framework should clearly define security roles and responsibilities, including governance of security functions. Management should also ensure technical controls are in place to protect the computing environment by providing a layered defense against internal and external threats.

The SDC staff is responsible for managing and securing the environment on which agency computer systems operate. In turn, state agencies continue to be responsible for operating and securing their respective computer applications. Because security is no stronger than its weakest link, both entities must ensure their individual security responsibilities are adequately performed.

Prior Audit Concerns

In September 2006, we issued an audit report titled *Department of Administrative Services: Computing and Networking Infrastructure Consolidation (CNIC) Risk Assessment*. We reported that project plans to create the SDC were incomplete because, among other things, they did not sufficiently address how critical security and disaster recovery services would be provided.

In July 2008, after agencies had moved to the SDC, we reconfirmed our previous concerns regarding SDC security in our audit report titled *Department of Administrative Services: State Data Center Review*. In that public report we communicated to DAS management that it had not yet provided a secure computing environment for SDC clients. That conclusion was based on the detailed findings and recommendations we provided to SDC management in an accompanying confidential audit report.

Subsequent to the above audits, DAS's Enterprise Security Office contracted with the United States Department of Energy, Pacific Northwest National Laboratory for a limited SDC security vulnerability assessment. That report, dated October 2008, confirmed the security concerns included in our previous confidential audit report, reemphasizing the need to resolve them.

In February 2009, we issued an audit, *Department of Administrative Services: Enterprise Security Office Review*, containing an evaluation of DAS's Enterprise Security Office. In that report we found that DAS's legislatively mandated state security plan did not contain details regarding how the SDC would be secured, including how confidential information should be safely stored or transmitted. We also found the state lacked enterprise standards for common security elements such as identity and access management, encryption, and wireless transmissions that impact SDC security.

In April 2009, we issued a confidential management letter to DAS management in conjunction with our annual audit of the state's Statewide

Financial Management Application and Oregon State Payroll Application. That letter indicated those systems were at increased risk because of specific security weaknesses at the SDC. We stressed that these weaknesses posed risks to many other systems hosted at the SDC.

In September 2009, we concluded this second annual audit of SDC computer controls, including security. The purpose of our audit was to provide internal control information to support our annual financial audits of agencies utilizing the SDC, and to provide DAS management information regarding SDC risks and controls.

This report addresses management elements related to the security portion of our audit. We will later issue a separate public report pertaining to operational controls.

Audit Results

Slow Progress on SDC Security Efforts

We found that SDC management and staff continued to provide adequate controls to limit physical access to the SDC and made incremental improvements to various SDC security processes such as firewall management. However, they have not yet resolved most of the security weaknesses we identified during previous audits. Collectively, these continued weaknesses could have costly and far reaching consequences, including a heightened risk that the security of applications hosted at the SDC could be compromised. Thus, urgent action is needed to resolve them.

Because of the duration of these weaknesses, we expanded our audit work to determine why they were not resolved. Based on this work, we found:

- Most SDC security weaknesses could be resolved without extensive agency involvement; others require a collaborative effort.
- The SDC shared services governance structure is not effective for managing security.
- SDC management had not established security standards or assigned overall responsibility for security.

We excluded detailed information relating to security findings and recommendations from this report. That information will be communicated to DAS under separate cover in accordance with ORS 192.501 (23), which exempts sensitive information from public disclosure.

Most SDC Security Weaknesses Could be Resolved Without Extensive Agency Involvement; Some Require a Collaborative Effort

While we cannot disclose the nature of the security weaknesses we identified during our audit, a majority of them were long-standing problems that do not require new or overly complex technical solutions on the part of the SDC. Rather, they require a concerted effort by SDC staff to ensure fundamental security processes are developed and implemented.

Most of the SDC security weaknesses we identified involved process or system issues that were proprietary to the SDC and did not require state agencies' involvement to resolve them. Some of those problems could be resolved by appropriately configuring or implementing technical solutions the SDC has already acquired. Others could be resolved by developing and implementing applicable security policies, procedures and standards.

In a few instances, state agencies also need to change how they use SDC resources. For example, we identified insecure protocols that should have been specifically disallowed at the SDC according to best security practices,

but were allowed in order to accommodate agencies that had not updated their security practices. SDC staff indicated they offer agencies good security alternatives, but they did not require their use. These security issues require little effort from SDC technical staff but would require the attention and resources of state agencies to implement their part of the solutions.

The SDC Shared Services Governance Structure is Not Effective for Managing Security

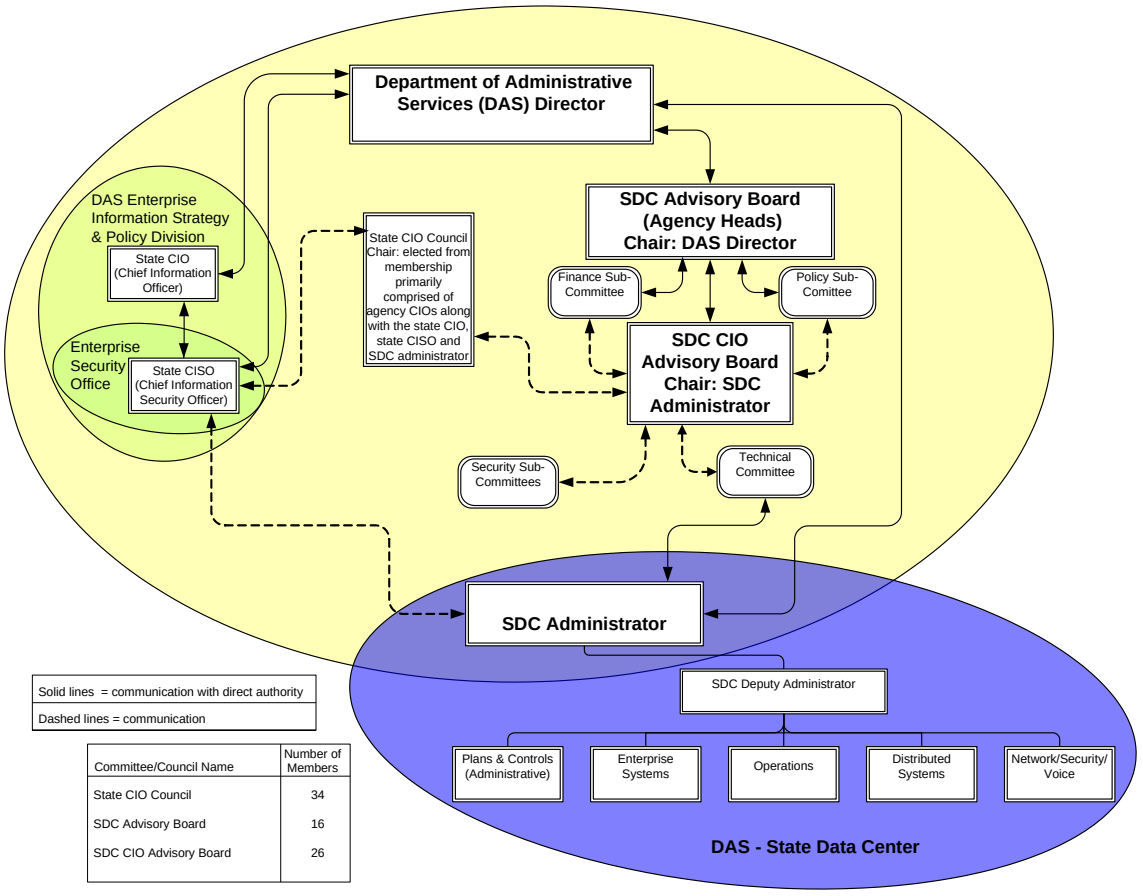
Although SDC staff are responsible for managing and operating security infrastructure, security issues involving state agencies are addressed through the SDC's shared services governance model. While Oregon statutes assign responsibility for security of information technology to DAS, agency officials believe a collaborative approach is most effective. As a result, the governance of the data center involves boards and committees comprised of customer agency heads, Chief Information Officer's (CIO's), technical experts, and business stakeholders, as well as SDC staff and DAS management. (see exhibit A) These boards and committees address a variety of SDC information technology issues, including security. The most significant of these governing bodies are the SDC Advisory Board and the SDC CIO Advisory Board.

The SDC Advisory Board is comprised of 16 members, including 11 agency heads, and is chaired by DAS's director. It interacts with several other SDC governance bodies including the SDC Executive Committee, SDC Finance Subcommittee, SDC Policy Subcommittee, SDC CIO Advisory Board, and the SDC Technical Committee. This board receives recommendations from the SDC Chief Information Officer (CIO) Advisory Board.

The SDC CIO Advisory Board is chaired by the SDC Administrator. This board interacts with several other SDC governance bodies, including the SDC Executive Committee, SDC management, SDC Technical Committee, SDC Finance Subcommittee, SDC Policy Subcommittee, CIO Council, and other SDC subcommittees as necessary.

According to their charters, these SDC governance committees are responsible for determining the strategic direction of the SDC regarding security. In addition, committee members are expected to perform managerial tasks such as providing human resources for developing security recommendations and for resolving SDC security issues.

Exhibit A - Governance Structure of the State Data Center



Committee/Council Name	Number of Members
State CIO Council	34
SDC Advisory Board	16
SDC CIO Advisory Board	26

For matters of security, the committees also receive advice from the State Chief Information Officer (CIO) and the Chief Information Security Officer. These two managers are part of DAS's Enterprise Information Strategy and Policy Division (EISPD).

We found that this governance structure expands the list of possible resources for resolving security and other issues; however, it is cumbersome and restricts SDC management's ability to implement effective security. In order for changes to be approved, agreement has to occur among committee members. In addition, the governing committees rely on other sub-committees to arrive at their proposed recommendations. For example, the SDC CIO Advisory Board receives the work product of the SDC Technical Committee before recommendations go to either the SDC or other committees. In addition, since the committees generally meet only once a

month, an inordinate time may pass between when matters are forwarded and when they are finally approved.

For example, in May 2008, we communicated to department management several critical SDC security issues. The criticality of these weaknesses was also reiterated to SDC management by an independent consultant in October 2008. In March 2009, DAS's director asked members from the SDC CIO Advisory Board to sponsor workgroups to develop solutions to fix four of the SDC security weaknesses identified by our audit and the vulnerability assessment.

In September 2009, we inquired regarding the status of these projects and found evidence of considerable discussion, but little action mitigating the associated security risks. Specifically, none of the groups had forwarded final recommendations to the governing board and workgroups had developed proposed solutions that only partially addressed the identified problems. In January 2010, SDC management acted on the proposal of one group, which partially addressed one of the weaknesses identified in our audit and the consultant's report. Based on meeting minutes, it was also unclear when, or if, some of the security weaknesses would be resolved. Members of the SDC governance body, including SDC management, indicated that difficulties in reaching agreement significantly hampered progress in resolving critical security weaknesses and in implementing other needed changes at the SDC.

Although it is important to consider the impacts that changes to security configurations may have on state agencies, DAS's "shared services" structure allows agencies to retain the status quo at the SDC and minimize the changes they may need to make to improve overall security. In addition, the use of already busy committee members with potentially conflicting time commitments and priorities further erodes the message of urgency and SDC staffs' ability to fix serious security weaknesses.

SDC Management had not Established Security Standards or Assigned Overall Responsibility for Security

Delays in resolving security weaknesses also occurred because SDC management did not clearly define or communicate security standards, or assign overall responsibility for managing the security function.

The Information Technology Governance Institute developed maturity models within CobiT [1] for scoring the effectiveness of controls over IT processes. This modeling method was developed by the Software Engineering Institute of Carnegie Mellon University and is based on best

[1] Control Objectives for Information and Related Technology (COBIT) is a publication of the IT Governance Institute (ITGI). The ITGI was established in 1998 to advance international standards in directing and controlling an enterprise's information technology.

industry standards. Organizations can use these metrics to determine how they are doing relative to industry standards. Maturity model scores range from 0 (non-existent) to 5 (optimized).

Applying this method, we concluded that controls for organizing and assigning responsibility for security at the SDC was at the level 1, initial or ad hoc state. According to the model, organizations at this level recognize an issue exists but have no standardized process to address it; have control processes that are neither formalized nor enforced; and use ad hoc approaches that tend to be applied on an individual or case-by-case basis.

Many security weaknesses continued to exist at the SDC simply because nobody was given the authority or responsibility to resolve them. Others languished because SDC management had not developed adequate security standards to provide appropriate expectations or requirements.

In September 2009, the Enterprise Security Office (ESO) issued a draft Information Security Plan for the State of Oregon. The ESO also issued a draft of the associated Statewide Information Security Standards in November 2009. Both documents were approved in principle by the DAS director and presented to state agencies in December 2009. These documents for the first time provide high-level guidance regarding how security will be achieved for State of Oregon computer systems and infrastructure. Among other requirements, the statewide plan directs the SDC to develop information security standards, plans, policies, and procedures to ensure its assets are appropriately protected.

Recommendations

We recommend that DAS management revise the shared services governance structure to facilitate timely resolution of security issues. SDC governance should ensure that customers' needs are appropriately considered without encumbering SDC staffs' ability to implement timely solutions or carry out their security responsibilities.

We also recommend that SDC management:

- Formally assign an individual to be responsible for assuring both physical and logical access of SDC information assets. This individual should be accountable to senior management and have the authority and resources to implement security measures according to the enterprise security plan and its associated standards.
- Develop and implement an SDC security plan with associated standards and procedures in accordance with the proposed Information Security Plan for the State of Oregon and the associated Statewide Information Security Standards document.
- Take aggressive action to implement the recommendations included in our confidential security reports and the Pacific

Northwest National Laboratory's security vulnerability assessment.

Objectives, Scope and Methodology

The purpose of our audit was to provide internal control information to support our annual financial audits of agencies utilizing the SDC, and to provide DAS management information regarding SDC risks and controls. Our specific audit objectives were to determine whether the SDC provided:

1. a controlled and stable operating environment for agency and enterprise applications; and

2. the necessary security framework to protect agency and enterprise applications and their data.

We expanded our audit work to determine why prior audit findings relating to security were not resolved. This report addresses management elements relating to that portion of our audit. We will later issue a separate public report pertaining to operational controls. Because of its sensitive nature, we excluded detailed information relating to security findings and recommendations from this report. That information will be communicated to DAS under separate cover in accordance with ORS 192.501 (23), which exempts sensitive information from public disclosure.

During our audit, we interviewed various department and customer agency personnel, observed operations, reviewed department documentation, and conducted various tests. To determine whether the SDC provided a controlled and stable operating environment, we evaluated controls, processes and procedures for:

- establishing customer service level agreements;
- managing performance and capacity;
- ensuring continuous service;
- identifying and allocating costs;
- managing problems and incidents;
- controlling infrastructure configurations;
- managing data;
- protecting the physical environment; and
- managing operations.

To determine whether the SDC provided the necessary security framework to protect agency and enterprise applications and their data, we evaluated SDC:

- security plans, policies, procedures, standards, and performance metrics;

- asset, system, and configuration inventory information and documentation relating to network architecture;
- internal and external audit, risk, and vulnerability assessment reports, and the status of prior report findings;
- selected logical and physical access listings, access policies, and the related system parameters;
- processes and practices governing security testing, surveillance and monitoring;
- processes for reporting and resolving security violations and incidents;
- use of encryption; and
- processes and tools for managing and protecting operating system configurations.

We used the IT Governance Institute's (ITGI) publication, "Control Objectives for Information and Related Technology," (COBIT), the Office of Government Commerce's (OGC) IT Infrastructure Library (ITIL) and the United State's 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
Theodore R. Kulongoski, Governor

Department of Administrative Services
State Data Center
530 Airport Road S.E.
Salem, OR 97301
PHONE: (503) 378-2176
FAX: (503) 378-2736

March 2, 2010

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

Re: *Audit Report (State Data Center: Faster Progress Needed on Security Fixes)*

The Department of Administrative Services' response to that Report follows.

General response

Thank you for providing us the audit report entitled *State Data Center: Faster Progress Needed on Security Fixes*. This report contains general information regarding security findings previously identified and a recommendation to resolve at a faster pace.

As a preface to the recommendation responses that appear below, the Department of Administrative Services (DAS) wishes to highlight a few main points regarding security at the State Data Center. First, the information assets housed at the SDC are safely protected behind multiple layers of security. These layers provide a shield that fends off thousands of attempted external attacks and intrusions daily. DAS management recognizes that additional layers of security would aid in enhancing the state's security position, as the Secretary of State's audit points out. Since the audit team completed its field work in June 2009, the SDC has started implementing many of the auditor's recommendations. As the SDC seeks to address those recommendations, it takes the following factors into consideration:

- The risk the vulnerability presents
- The availability of resources to address the vulnerability
- Other competing demands for new services and increasing technology capacity needs
- The potential impact on the ability of the state to conduct day-to-day business
- Consolidating a vast computing infrastructure to avoid ever increasing technology costs
- Improving the day-to-day operations

Finally, some of the vulnerabilities identified have significant impact on customer-agencies' operations and require their continued involvement and governance to resolve.

Specific responses to auditors' recommendations

- **Audits Division recommendation:**

  We recommend that DAS management revise the shared services governance structure to facilitate timely resolution of security issues. SDC governance should ensure that customers'

needs are appropriately considered without encumbering the SDC staffs ability to implement timely solutions or carry out their security responsibilities.

DAS' Response:

Management disagrees with this recommendation. The governance structure has been carefully balancing these timelines and implementations to ensure that critical business functions are not interrupted and security issues are resolved or adequately mitigated. The customer-agencies and SDC are very serious about the security of the information technology resources required to do business. Although the objective of the audit did not include a determination of risk, materiality and business impact, the current SDC governance is structured to meet this responsibility.

"Governance," as defined by the Control Objectives for Information and Related Technologies (COBIT), is "a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes." This type of partnering with our customers is what has achieved the balance of risk and IT value as required by the business. The daily defense and incident management that are part of the SDC operation are all aggressive actions that have protected the state from serious attacks. These types of daily decisions and 24/7 operations are not managed by a governance structure.

- **Audits Division recommendation:**

We also recommend that SDC management:

Formally assign an individual to be responsible for assuring both physical and logical access of SDC information assets. This individual should be accountable to senior management and have the authority and resources to implement security measures according to the enterprise security plan and its associated standards.

DAS' Response:

Management agrees with this recommendation. In October 2009, the SDC hired just such a person to lead the security program for the SDC. This person acts independently of the technical team, which is responsible for implementing technical security. The person in this position reports directly to the manager of Plans and Controls with regular interaction with the administrator and deputy administrator. The position's key responsibilities include the following:

- Monitoring and tracking the security posture of the SDC
- Tracking and reporting progress on remediating identified vulnerabilities
- Managing the continued development of the SDC security plans, procedures and standards
- Conducting liaison with the DAS Enterprise Security Office

- **Audits Division recommendation:**

  Develop and implement an SDC security plan with associated standards and procedures in accordance with the proposed Information Security Plan for the State of Oregon and the associated Statewide Information Security Standards document.

  DAS' Response:

  Management agrees with this recommendation. Our current strategic plan includes a focus on security, as well as standards, procedures and architecture for each technical domain. In place today is a well executed incident response procedure and layers of security protection that help fend off thousands of attempted attacks and intrusions daily.

  Consistent with the auditors' recommendation, the next phase in the SDC maturity will be development of a consolidated SDC security plan. This plan will incorporate and align individual plans developed by each technical domain to create one unified plan. The plan will use as its base the proposed security plan and standards for the State of Oregon. We anticipate completion of the consolidated plan by the end of this calendar year.

- **Audits Division recommendation:**

  Take aggressive action to implement the recommendations included in our confidential security reports and the Pacific Northwest National Laboratory's (PNNL) security vulnerability assessment.

  DAS' Response:

  Management partially agrees with this recommendation. The SDC has resolved many of the vulnerabilities highlighted in the PNNL assessment—particularly those that lie exclusively within the SDC's purview. The remaining unresolved vulnerabilities require significant interaction with customer-agency personnel. The SDC must approach resolution of these vulnerabilities in a way that does not risk interrupting or causing critical business systems to fail. Balancing the available resources, both at the SDC and its customer-agencies, is a critical factor in setting remediation priorities and timelines.

  The SDC and DAS management continue to take appropriate action to address all known security vulnerabilities. The SDC evaluates each perceived vulnerability for its risk to the state's information assets. Based on that evaluation, the SDC develops an approach to mitigate that risk. Every solution must preserve the delicate balance between solving the problem and increasing the risk of system failure or disruption of business flow by using an overly aggressive tactic.

  The SDC strategic plan aggressively seeks to achieve the following:

  - Generate cost savings and implement solutions that avoid future costs.

- Accommodate the increasing technology growth required that agencies require to do their business.
- Answer the need for new technology services to the state.
- Manage and improve the day-to-day operations.
- Consolidate the state's vast array of computing resources and architecture.

The strategic plan contains a focus area dedicated to security. Each focus area's plan outcomes are used in development of inter-related and dependent projects that we prioritize with input from customer-agency directors and chief information officers. The security focus area describes planned and expected outcomes over a five-year period. When the SDC receives findings such as those from PNNL, we consider whether they require adjustments to current plans.

The SDC has taken steps to remediate previous findings of vulnerabilities identified by PNNL and the Secretary of State's auditors. We will address remaining vulnerabilities in accordance with the SDC strategic plan. Our security plan takes into account the materiality of the vulnerability, the risk of disrupting business flow, and the availability of resources to support the fix.

Closing

We appreciate your audit team's diligent effort over the past year to address security vulnerabilities and highlight opportunities for improvement at the SDC. Since the team completed its field work in June 2009, we have endeavored to implement many of its recommendations and will continue to make progress as described above.

If you have any questions about this response, please don't hesitate to contact either John Koreski, SDC Administrator at 503-378-6430 or Julie Bozzi, SDC Deputy Administrator at 503-378-4578.

Thank you again for the recommendations and helpful insight that your audit has afforded us.

Sincerely,

Scott L. Harra, Director
Oregon Department of Administrative Services

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
Deputy Director: William K. Garber, MPA, CGFM
Audit Manager: Neal E. Weatherspoon, CPA, CISA, CISSP
Principal Auditor: Mark A. Winter, CPA, CISA
Staff Auditor: Teresa L. Furnish

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 Department of Administrative Services during the course of this audit were commendable and sincerely appreciated.