Secretary of State Audit Report

Kate Brown, Secretary of State

Gary Blackmer, Director, Audits Division

Department of Forestry: Computer Controls Need Attention

Summary

The mission of the Oregon Department of Forestry (department) is to serve the people of Oregon by protecting, managing, and promoting stewardship of Oregon's forests to enhance environmental, economic, and community sustainability. The department's programs provide fire protection and other services to manage private, state owned, urban, and community forests.

The purpose of this audit was to review and evaluate the effectiveness of key controls over the computing environment at the department. Although the department provides vital technical support for its computer systems, we identified areas where the department could improve.

We noted that the department's formal strategic plans were out of date and did not provide a clear vision for optimizing use of information technology. As a result, it is unlikely the department will timely address known information technology challenges or make other notable improvements to its current technology state.

In addition, management did not adequately organize important information technology functions such as planning, development and maintenance, security, and quality assurance to ensure they would be properly addressed.

Processes for selecting, acquiring, developing, implementing, and maintaining computer systems were also inadequate. Without these controls in place, it is unlikely the department will be able to keep pace with advancing technologies or take advantage of opportunities to gain efficiencies afforded by better use of technology.

We also found information security controls should be improved. We communicated details regarding these matters to department management in a separate confidential document, as provided in ORS 192.501 (23).

Agency Response

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

Background

The Oregon Department of Forestry (department) was established in 1911. Its stated mission is to serve the people of Oregon by protecting, managing, and promoting stewardship of Oregon's forests to enhance environmental, economic, and community sustainability. The department's programs provide fire protection and other services to manage private, state owned, urban, and community forests.

The department is divided into four major divisions. Three divisions are assigned operational programs, including Fire Protection, State Forests, and Private Forests. The fourth, Administrative Division, provides centralized services such as budgeting, accounting, facilities, procurement, and information technology. The department's central offices are located in Salem, but the department maintains regional and district offices in multiple locations throughout the state.

One of the department's most significant responsibilities is providing wildfire protection. According to department management, the goal of its Fire Protection Division is to devise and use environmentally sound and efficient strategies to minimize the total cost to protect Oregon's timber and other forest values from loss caused by fire. The department spent approximately $57 million during fiscal year 2012 providing fire protection for Oregon's forests.

The department has implemented various computer systems and databases to predict, document, track, manage, and record information relating to forest fire protection. Its systems also help manage information relating to costs, inventories, resources, contracts, and budgets needed to appropriately account for and manage the department's business functions.

The 1971 legislature enacted the Oregon Forest Practices Act to provide for timber harvest on private, state, and local government owned lands using techniques consistent with conservation and environmental protection. The department carries out the requirements of this law through its Private Forests Division. This program provides technical assistance, financial incentives, education, regulation, and other tools to help forest landowners manage their lands.

The Private Forests Division uses computer systems to track vital information relating to private forest operations, boundaries, streams and fish presence, and stewardship plans. In addition, the department tracks a variety of other program information such as data relating to compliance and civil penalties, contracts, and tax credits.

The department is also responsible for managing the 818,800 acres of state-owned forest land. The department's State Forest Division works to ensure timber harvests on these lands provide revenue for local governments and schools, while also protecting wildlife habitat and other

environmental values, and providing citizens opportunities for recreation and learning.

The State Forest Division utilizes various computer data systems to record and track program information such as tree stand mapping, boundaries, log brands, sale plans, log accountability, and invasive species.

The department shares responsibility for operating and maintaining its computer systems with Enterprise Technology Services (ETS) of the Department of Administrative Services. Some tasks are the sole responsibility of either the department or the ETS, while responsibilities for disaster recovery and security are shared between the organizations.

The department's budget for the 11-13 biennium is $292.5 million, which includes approximately $4.8 million for information technology needs. Approximately one-third of the information technology portion is allocated to supporting the Geographic Information System (GIS) capability that is used throughout the department.

Audit Results

We evaluated the Oregon Department of Forestry's (department) computing environment, including processes for using technology and planning for improvements, implementing and maintain systems, and protecting computer systems and data. For each of these areas, we found the department was providing technical support for its computer systems, but we also identified opportunities for improvement.

Specifically, we found that the department's:

- Strategic plans do not provide a clear vision for optimizing use of information technology.
- Information technology efforts are not well organized.
- Processes for acquiring, implementing, and maintaining technology solutions are inadequate.
- Security of information systems and data needs improvement.

These weaknesses limit the department's ability to protect department data or keep pace with technology advances that could enhance operations or take advantage of opportunities to gain efficiencies afforded by better use of technology.

Strategic Plans do not Provide a Clear Vision for Optimizing Use of Information Technology

Strategic planning for information technology helps organizations properly manage resources and realize optimum value from efforts and investments. To be effective, planning should take place at regular intervals and result in formal documentation describing required initiatives, resource requirements, and how efforts will be monitored and managed. Long and short-term strategic plans should provide a roadmap for allocating resources and prioritizing efforts by answering the basic questions of what, who, how, when, and why.

We found the department's formal strategic plans were out of date and did not provide a clear vision of how it would apply or enhance technology solutions to support its business objectives. The department's most current plan was for the eight year period ending in 2011. Although this document broadly addressed how the department would carry out its mission, it did not include important information regarding how it planned to use information technology.

We also found the department did not have ongoing processes for developing, updating, or implementing strategic plans for information technology. We noted that management led several efforts to gain insight regarding how it could improve business processes, including the use of information technology. Over several years, the department hired

consultants to model, identify and assess business processes, and identify challenges to implementing information technology. These projects identified weaknesses and opportunities to improve use of technology, but management did not effectively transform the recommendations included in the reports into actionable plans.

For example, the department hired a contractor in 2011 to help a work group analyze the results of previous consultants' reports to identify potential information technology projects that could address business challenges. The most significant product from this effort included a list of 15 information technology projects staff wanted to consider during the next three biennia. The work group, however, did not provide significant details regarding costs, feasibility, alternative solutions, timing, or how the projects could resolve some of the department's most challenging technology problems. Once the project was completed, the work group was disbanded and it was unclear how or if the list would be used.

Although the Chief Information Officer's position description identifies some responsibilities consistent with information technology planning, management has not formally assigned anyone to develop a process for regular strategic planning or to create, monitor and maintain related tactical plans.

Without formal strategic and tactical plans for information technology, it is unlikely the department will timely address known information technology challenges or make other notable improvements to its current technology state.

Information Technology Efforts Are Not Well Organized

Proper placement and organization of information technology personnel within an organization is necessary to provide adequate control and ensure services are properly aligned with business requirements. Management should ensure information technology functions have a sufficient number of competent staff and all personnel in the organization have and know their roles and responsibilities in relation to information systems.

Department management has taken a decentralized approach to managing information technology. As such, they did not provide adequate information technology policies, procedures, or standards to guide staff as they performed important tasks such as strategic planning, system development and maintenance, quality assurance, or security. In addition, management did not always clearly assign responsibility for ensuring important information technology tasks would be performed.

Management also provides significant flexibility and autonomy to division management relating to information technology. We noted the department has business critical systems supported by various combinations of Information Technology Program (IT) staff and division staff. Some of

these applications were written by division staff and cannot be supported by IT. Others were developed in cooperation with IT and now are supported by staff from both sources. One manager indicated this staffing model grew out of necessity because the central IT group does not always have the available resources to fulfill the growing needs of the agency.

As a result of the above issues, the department has not always kept up with changes in technology and progress to resolve technology challenges and weaknesses has been markedly slow. The department indicated that many of its computer applications were developed using technology that does not adequately support concurrent users, lacks the ability to interact with other department systems, or operates on obsolete and insecure platforms.

Processes for Acquiring, Implementing and Maintaining Technology are Inadequate

Organizations should define and implement information technology standards and adopt system development life cycle methodologies for developing, acquiring, implementing, and maintaining computerized systems. These methodologies should ensure applications provide the automated functions to effectively and efficiently support business processes and internal control.

The department has not adopted adequate system development life cycle methodologies. Rather, staff is left to perform these processes in isolation, having little direction to ensure their individualized solutions conform to an enterprise standard. As such, the list of databases, platforms, spreadsheets, and applications implemented over the years is numerous and disparate.

The department has invested considerable resources and efforts to properly maintain its Geographic Information System (GIS) capability. However, many of the department's other computer applications were built by staff using technology that is now outdated or inadequate for enterprise use. In addition, the department has some applications that run only on obsolete and insecure platforms. Some systems also cannot readily share information with other systems to avoid data duplication.

We also noted that some information technology projects languished. For example, it took four years to gather requirements and select a vendor for a project to customize and implement an important off-the-shelf business application. In addition, there have been few organized or concerted efforts to resolve information technology weaknesses identified by consultants. In most instances, nobody was formally assigned to develop solutions and manage the necessary changes.

Without a comprehensive and effective framework for acquiring, developing and maintaining information systems, it is unlikely the department will be able to keep pace with advancing technologies or take

advantage of opportunities to gain efficiencies afforded by better use of technology.

Security of Information Systems and Data Needs Improvement

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

We found that security measures were in place to protect department computer systems and data. However, we noted weaknesses that should be corrected by the department and the Department of Administrative Services' Enterprise Technology Services (ETS). In addition, we found that the department had not adequately defined its security requirements with the ETS or confirmed security expectations were met.

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

Recommendations

We recommend that department management:

- ensure effective strategic planning occurs for information technology at regular intervals, including development of tactical plans to allocate resources and prioritize efforts;
- provide information technology policies, procedures, and/or standards to guide staff as they perform important tasks such as strategic planning, system maintenance, quality assurance, or security;
- ensure sufficient numbers of competent staff are available and formally assigned to perform critical information technology tasks;
- formally adopt system development life cycle methodologies to better govern processes for selecting, acquiring, developing, and implementing computer systems; and
- resolve the security weaknesses we identified in our confidential management letter and work with the Department of Administrative Services' Enterprise Technology Services to ensure the department's security expectations are clearly established and fulfilled.

Objectives, Scope and Methodology

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

- the department's information technology is appropriately planned, organized and controlled;
- controls were in place to ensure successful acquisition, implementation and maintenance of technology solutions to meet the department's business users' needs; and
- the department provided adequate security for information technology assets.

We primarily focused on controls in effect on or after January 2012. We conducted interviews with department personnel and reviewed agency documentation.

To evaluate information technology governance and planning we:

- reviewed strategic planning documents;
- interviewed management and staff regarding the department's information strategic planning; and
- reviewed the department's roles and responsibilities for information technology functions.

To evaluate acquisition, implementation and maintenance of information technology solutions we:

- reviewed policies and procedures for system acquisition, including the use of feasibility studies and risk analyses prior to acquisition;
- reviewed the department's change management procedures and interviewed personnel responsible for managing changes; and
- reviewed policies, procedures and processes for training regarding systems and data standards.

To evaluate controls over the management of security for information technology assets we:

- reviewed the service level agreement with the ETS, including the division of responsibility;
- evaluated the department's monitoring of ETS provided services and systems, including network security, server management and patching and service cost charges;
- reviewed department security policies and procedures for user account maintenance; and
- determined whether access to systems is provided and reviewed in accordance with department policies and best practices.

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

We used the IT Governance Institute's publication, "Control Objectives for Information and Related Technology," (COBIT), and the United 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.

About the Secretary of State Audits Division

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

Audit Team

William K. Garber, CGFM, MPA, Deputy Director

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

Teresa Furnish, CISA, Senior Auditor

Shelby Hopkins, Staff Auditor

Matthew Owens, Staff Auditor

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

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

phone: 503-986-2255

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

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

Oregon
John A. Kitzhaber, MD, Governor

Department of Forestry
State Forester's Office
2600 State Street
Salem, OR 97310-1336
503-945-7200
FAX 503-945-7212
http:/ /www.odf.state.or.us

"STEWARDSHIP IN FORESTRY"

April 4, 2013

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

RE: Department of Forestry Information Technology Controls Audit

Dear Mr. Blackmer:

This letter is in response to the Oregon Department of Forestry's information technology controls audit report transmitted to us on March 18, 2013. We appreciate the professional and collaborative manner in which the Secretary of State staff performed this audit.

The report's findings and recommendations provide insight into the challenges the department faces in the management and control of its information technology assets. We are grateful for the information provided and believe that it validates our position that changes are needed in the overall management and funding of technology at the Oregon Department of Forestry.

In summary, we generally concur with the audit findings and agree with the recommendations. Please see the enclosed agency response and corrective action plan for each finding and recommendation.

We look forward to our continued working relationship with the Audits Division. Please don't hesitate to contact me if you have any questions regarding our response.

Sincerely,

Doug Decker
Oregon State Forester

Encl: Department of Forestry's Response to the Information Technology Controls Audit Findings and Recommendations

cc: Neal E. Weatherspoon, CPA, CISA, CISSP
Teresa Furnish, CISA
ODF Executive Team

Department of Forestry's Response to the Information Technology Controls Audit Findings and Recommendations

Audit Finding 1: Strategic plans do not provide a clear vision for optimizing use of information technology.

Audit Recommendation: Ensure effective strategic planning occurs for information technology at regular intervals, including development of tactical plans to allocate resources and prioritize efforts.

Agency's Response: Management agrees with this recommendation. The Oregon Department of Forestry (ODF) is currently developing an agency-wide strategic plan, with annual operating plans for each of its divisions. In alignment with these plans, the Information Technology Program will develop strategic and tactical plans by the fall of 2013. These plans will set clear direction for the program on how it supports and provides services to the agency, including specific tactical actions one to two years out.

Audit Finding 2: Information technology efforts are not well organized.

Audit Recommendations: Provide information technology policies, procedures, and/or standards to guide staff as they perform important tasks such as strategic planning, system maintenance, quality assurance, or security.

Ensure sufficient numbers of competent staff are available and formally assigned to perform critical information technology tasks.

Agency's Response: Management agrees with these recommendations. Taken together, this finding's components point clearly to the need for an information technology governance model to coordinate responses to all of the concerns raised. This will be a major undertaking, given ODF's unique mission which requires 24-7 fire response, geographic spread and remoteness of offices and operations, and its diverse and complex funding model.

The department has started to develop an information technology governance model and to build internal understanding of the need for such a model. We expect to implement the model, with the full support of the executive team, in the fall of 2013. The model will be applied immediately to address the specific items identified in the audit report.

The oversight committee will need to carefully evaluate the organization and funding of information technology services throughout the agency. Although addressing the audit report findings will require considerable effort, we believe that a governance model with full executive team support will position ODF for dramatic improvements in short- and long-range IT planning and execution.

The Governor's Balanced Budget for the agency for 2013-15 recommends additional IT staffing. The Legislature is currently considering this budget proposal. Approval of the proposal would provide the capacity to help address the audit report's specific recommendation regarding staffing.

Audit Finding 3: Processes for acquiring, implementing, and maintaining technology solutions are inadequate.

Audit Recommendation: Formally adopt system development lifecycle methodologies to better govern processes for selecting, acquiring, developing, and implementing computer systems.

Agency's Response: Management agrees with this recommendation. The agency needs documented standards and lifecycle approaches for developing, acquiring, implementing and maintaining computer systems and applications. ODF has lacked sufficient IT staff to achieve these goals. While development standards have already been set, documentation and processes still need to be completed. With our limited IT resources, there currently is no timeline for this.

Once formed, the IT governance committee will be tasked with fully understanding the importance of a lifecycle methodology for systems and applications, and will work on a plan to obtain the necessary resources.

Audit Finding 4: Security of information systems and data needs improvement.

Audit Recommendation: Resolve the security weaknesses we identified in our confidential management letter and work with the Department of Administrative Services' Enterprise Technology Services to ensure the department's security expectations are clearly established and fulfilled.

Agency's Response: Please refer to the confidential response letter hand-delivered to the Audits Division.