ALASKA STATE LEGISLATURE
LEGISLATIVE BUDGET AND AUDIT COMMITTEE
Division of Legislative Audit

P.O. Box 113300
Juneau, AK 9811-3300
(907) 465-3830
FAX (907)465-2347
legaudit@legis.state.ak.us

January 4, 2008

Members of the Legislative Budget
and Audit Committee:

In accordance with the provisions of Title 24 of the Alaska Statutes, the attached report is submitted for your review.

DEPARTMENT OF ADMINISTRATION
INFORMATION SYSTEM CONTROLS OVER
ALASKA DATA ENTERPRISE REPORTING (ALDER)

November 30, 2007

Audit Control Number

02-10005-08

We conducted this audit of information system controls over the State's new data warehouse – Alaska Data Enterprise Reporting (ALDER) – to determine whether the controls adequately manages risk to the confidentiality, integrity, and availability of the data. Report conclusions will be used to determine the degree of reliance we place on these controls in our financial and performance audits of the State of Alaska. As of the date our audit fieldwork ended, the system was in the field test environment.

Information system audits include a review of sensitive security data that, if disclosed, would not be considered in the best interests of the State of Alaska. Therefore, we are withholding security-related details from our publicly released report. Pertinent details have been communicated to agency leaders in a separate, confidential document.

We conducted this 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 objectives. Fieldwork procedures utilized in the course of developing the findings and recommendations, presented in this report, are discussed in the Objectives, Scope, and Methodology section.

Pat Davidson, CPA
Legislative Auditor

TABLE OF CONTENTS

	Page
Objectives, Scope, and Methodology	1
Organization and Function	5
Background Information	7
Report Conclusions	9
Findings and Recommendations	13
Glossary	27
Agency Response	
Department of Administration	31

OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with the provisions of Title 24 of the Alaska Statutes, we conducted this audit of information system controls over the State's new data warehouse Alaska Data Enterprise Reporting (ALDER) to determine whether risks are adequately managed to allow reliance on the data for financial and performance audit reporting.

Exhibit 1

Business Requirements For Information

Confidentiality: Concerns the protection of sensitive information from unauthorized disclosure.

Integrity: Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

Availability: Relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

Objective

The objective of our audit was to evaluate the effectiveness of controls over the State's new data warehouse and reporting system, ALDER. The effectiveness of information system controls is evaluated to determine whether controls adequately manage risk to the confidentiality, integrity, and availability of the ALDER data and system. See Exhibit 1.

Scope

The scope of our review encompassed:

1. General control areas impacting the ALDER system. These include data center controls, operating system controls, and change management controls. Data center controls protect the computer equipment from access, damage, and theft. Operating system controls are the policies, procedures, and practices that protect the application and data residing on the servers and being managed by the operating system. And lastly, change management controls protect program and data file integrity and availability from unauthorized changes.

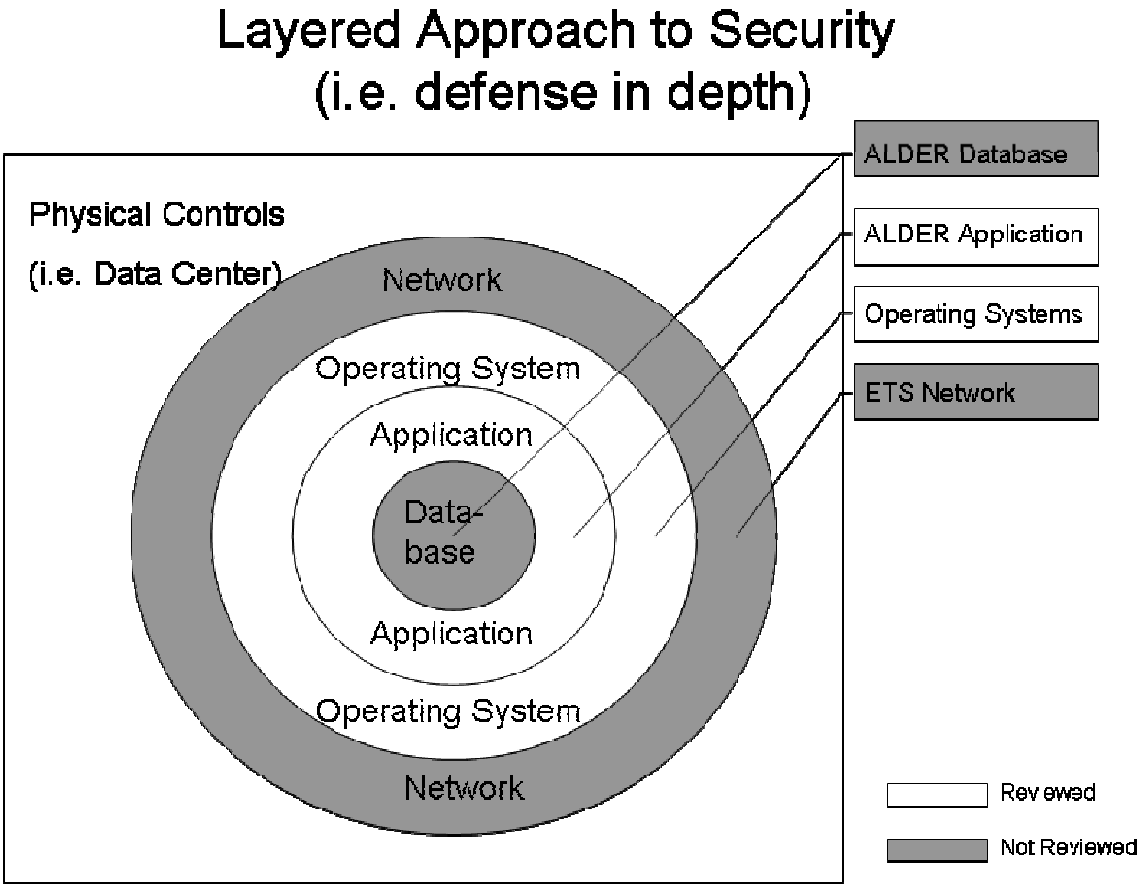
2. Controls specific to the ALDER application that help to ensure data integrity; data and system availability; and, data confidentiality.

3. Controls over the ALDER database and specific to the network on which ALDER resides were not reviewed. The Division of Finance was still making changes to the database at the time of our review; therefore, the database will be evaluated at a later time. Network controls were not reviewed as the ALDER system was not deploying any new networking components; thereby, introducing no new risk to the network environment.

Another way to view our scope is through what is termed a defense in-depth approach. The data warehouse consists of an application and database that run on servers with operating

systems. The servers are part of a network. And, the servers are housed in a data center which will have physical controls. See Exhibit 2 below.

Exhibit 2



Methodology

To meet our audit objective, we performed the following:

1. We collected and reviewed background information about data warehouses and about the ALDER data warehouse specifically.
2. Reviewed vendor-supplied reference manuals for the ALDER system.
3. Reviewed system documentation developed or published by the ALDER implementation team, Division of Finance (DOF), or Enterprise Technology Services (ETS).
4. Conducted interviews with Department of Administration employees involved with the ALDER system implementation, administration, security, and support.
5. Documented, analyzed, and tested controls at the Juneau data center where the ALDER servers reside. The data center and wiring closets were inspected. Items related to physical and environmental controls were evaluated. Physical access controls (including

access logs and procedures) were reviewed. Controls over the server racks housing the ALDER servers were evaluated for adequacy.

6. Documented, analyzed, and tested operating systems on servers where the ALDER application and database reside. This included review of the security and configuration of the operating systems.
7. Evaluated program change management controls and confidentiality measures.
8. Documented, analyzed, and tested application controls over the agencies' extract, transform, and load scripts. We reviewed agencies' procedures to ensure completeness and accuracy of the extract, transform, and load process.
9. We reviewed and evaluated agency controls over logical access to the data.

Audit criteria used in the audit includes management policies, procedures, and control guidelines outlined in the Control Objectives for Information and Related Technology (COBIT) framework. The mission of COBIT is:

> *To research, develop, publicize, and promote an authoritative, up-to-date, internationally accepted* [information technology] *IT governance control framework for adoption by enterprises and day-to-day use of business, IT professionals, and assurance professionals.*

COBIT represents a consensus of experts and provides good practices and activities relevant to information technology.

Other criteria used in this audit includes policies and procedures produced by the State of Alaska's Security Office, security standards established by the National Institute of Standards and Technology, as well as best practices described by the vendors.

(Intentionally left blank)

ORGANIZATION AND FUNCTION

Department of Administration

Under the provisions of Title 44 of the Alaska Statutes, the Department of Administration (DOA) is empowered to provide support services to state agencies. These services include keeping general accounts; operating central purchasing and supply services; and, administering a statewide personnel program. In addition, the department is responsible for the operation/management of information system resources and activities of the executive branch of state government. DOA also provides information system services to the judicial and legislative branches as requested.

Division of Finance

The Division of Finance (DOF) maintains accounting records and reports, annually, on the financial activity and condition of the State of Alaska. To meet these responsibilities, the division operates and maintains statewide general accounting and payroll systems (AKSAS and AKPAY). DOF also implemented a new statewide reporting system called Alaska Data Enterprise Reporting (ALDER) which will integrate data from these systems, as well as the on-line recruitment system (Workplace Alaska), into a unified environment with a single toolset for user reporting.

Enterprise Technology Services Division

DOA has delegated to the Enterprise Technology Services (ETS) Division responsibility for providing information system services, in response to the needs of state government. ETS provides computer, network, and telecommunication services for the executive branch of state government as well as the judicial and legislative branches to the extent requested by those branches.

(Intentionally left blank)

BACKGROUND INFORMATION

The Division of Finance (DOF) began developing Alaska Data Enterprise Reporting (ALDER), a data warehouse system, in June 2006. The ALDER system is a web-based data warehouse and reporting solution for the State's accounting, payroll, and human resources data. It consists of a central data repository organized for query and reporting that will be updated nightly with copies of data from the state's accounting system (AKSAS), the state's payroll system (AKPAY), and the state's recruitment system (Workplace Alaska). The ALDER reporting tool is purchased software accessible with a web browser from the State of Alaska's intranet. ALDER will replace the current accounting system reporting tool (GENEVA), which is no longer vendor-supported.

The hardware, on which the ALDER primary production system will run, resides in the Enterprise Technology Services (ETS) Juneau data center. A redundant production system is planned for backup, should the primary system become unavailable. The hardware for the redundant system will be located in the ETS Anchorage data center.

ALDER implementation is broken down into four (4) phases. Each phase is designed to build upon the previous phases. Phase 1 involves developing the reporting tool and report templates for AKSAS and importing AKSAS data, from fiscal year 2001 to present, into the data repository. Phases 2 and 3 will integrate AKPAY and Workplace Alaska data and report templates. Phase 4 involves completion of the redundant system in Anchorage. The completion date of each phase has been extended beyond the original plan to accommodate changes in system architecture that will improve system performance and availability. As of November 30, 2007 – the end of our audit fieldwork – ALDER is still not classified as a production system but is available to approximately 450 users in a "field test"[1] mode.

The ALDER development and implementation team is comprised of individuals from the information technology service provider, CGI, and state employees from DOF and the Division of Personnel and Labor Relations. In addition, ETS, a division within the Department of Administration, has entered into a Service Level Agreement (Agreement) with DOF to provide server administration activities including server monitoring, maintenance, backup, and recovery.

[1] Field test is occurring on the production servers and is being called the field test environment (see glossary). Employees throughout the State continue to be trained on the system and after they complete training are given access to ALDER. Once the field test is completed, access will be open to other users depending on employees' need for reporting information.

(Intentionally left blank)

REPORT CONCLUSIONS

The primary objective of our audit was to evaluate the effectiveness of internal controls over the Alaska Data Enterprise Reporting (ALDER) system to ensure confidentiality, integrity, as well as availability of the system and data. The internal control deficiencies, identified during our review, are categorized as follows:

- Physical Controls
- Operating System Controls
- Application Controls
- Change Management Controls
- Privacy and Information Protection Controls
- Miscellaneous

We conclude that controls over ALDER's field test environment do not adequately manage risk to the confidentiality, integrity, and availability of the ALDER data and system. Although, physical access controls are sufficient – except for the weaknesses noted below – significant control deficiencies exist in the operating system, application, change management, and privacy categories that should be addressed.

Understanding potential ramifications of the risks, management may choose to accept these risks, where cost of implementing the control outweighs the benefit. However, in those instances, management should make a concerted effort to implement compensating controls, mitigating risks to an acceptable level.

Below are the specific deficiencies identified during our review.

Physical Control Deficiencies

Protection of computer equipment and personnel are important in providing and maintaining a suitable physical environment to protect information technology (IT) assets from access, damage, or theft. Generally, controls over the Juneau data center are sufficient to protect the ALDER servers; however, weaknesses exist in the areas of contractor access; management oversight of data center access; server rack security; and, the lack of complete, up-to-date policies and procedures for managing the Juneau data center. (See Recommendation No. 5)

Operating System Control Deficiencies

The operating system is software that controls the operation of the computer from the moment it is turned on or booted. It provides the primary means of managing the use and sharing of computer resources such as processors, memory, and input/output devices. Other software programs use standard protocols, dictated by the operating system, for displaying their own information or processing the output of other computer programs. Operating system controls are policies, procedures, and practices that protect the application and data being managed by the operating system.

Currently, controls over the operating system do not adequately manage risk over confidentiality, integrity, and availability of the ALDER application and data. Specifically, we noted the following:

- ALDER and Enterprise Technology Services (ETS) have not effectively secured the operating systems of ALDER servers. (See Recommendation No. 1)

- An operating system performance monitoring strategy has not been developed for ALDER servers. (See Recommendation No. 2)

- A backup and recovery strategy for ALDER operating systems has not been fully developed and documented. (See Recommendation No. 3)

- The Agreement between ETS and the Division of Finance for services relating to ALDER is not comprehensive. (See Recommendation No. 4)

Application Control Deficiencies

Data warehouse systems use an extract, transform, and load (ETL) process to transfer data from source systems to a central repository where reporting tools can be used to query the data. Application controls for a data warehouse are specific to the flow of data from source systems to the central repository; also, they are designed to ensure accurate and complete reporting of data.

Currently, application controls do not adequately manage risk over confidentiality, integrity, and availability of the ALDER system and data. Specifically, we identified the following weaknesses:

- Data transferred between source systems, and the data warehouse, are not being reconciled. (See Recommendation No. 6)

- The ALDER project team is not monitoring for application security patches to apply timely. (See Recommendation No. 7)

- The ALDER project team does not plan to load or stress test the ALDER system before it moves into production. (See Recommendation No. 8)

- The passwords for ALDER application system accounts are not adequately secured. (See Recommendation No. 9)

- Application security events are not being logged and monitored according to the State of Alaska (SOA) security policy. (See Recommendation No. 10)

- Metadata[2] is not well-documented or controlled. (See Recommendation No. 11)

- End-user and enterprise account[3] and password settings do not comply with SOA security policy. (See Recommendation Nos. 12 and 13)

Change Management Control Deficiencies

Change controls protect program and data file integrity and availability from unauthorized changes. In addition, change controls are designed to develop, implement, and track changes to ensure that program-, system-, and infrastructure-modifications are properly authorized, tested, documented, and monitored. The ALDER project team is not following a consistent, documented, or well-controlled, change management process. In addition, production programs and scripts are not secured from unauthorized changes. (See Recommendation Nos. 14 and 15)

Privacy and Information Protection Control Deficiencies

Privacy and information protection controls help to protect sensitive and confidential, data and information from being exposed to individuals without a need-to-know basis. The ALDER project team has identified and categorized confidential information, implementing controls to limit access to confidential and sensitive information. However, these controls do not completely prevent the exposure of such information to individuals without a need to know. Specifically, we found the control restricting access to AKSAS' confidential information is not working and other controls, that could further restrict access to AKPAY confidential information, are not being implemented due to cost. (See Recommendation No. 16)

[2] Metadata is generally defined as data about data.
[3] Enterprise accounts are those used by ALDER administrators to access the application. These accounts utilized the application software's built-in authentication mechanism.

Miscellaneous

The last two recommendations pertain to weaknesses identified during the audit that do not fit into one of the categories, listed on the previous pages, but still present a risk to the confidentiality, integrity, and availability of the system. Specifically, login warning banners at the application and operating system level were incomplete and nonexistent respectively. (See Recommendation No. 17)

Lastly, the Agreement for Professional Services with CGI should, but does not, contain nondisclosure and confidentiality language to protect the ALDER system and the state's networking infrastructure. (See Recommendation No. 18)

FINDINGS AND RECOMMENDATIONS

Recommendation No. 1

The Alaska Data Enterprise Reporting (ALDER) project manager and the Enterprise Technology Services' (ETS) mid-tier manager should implement controls to secure the ALDER operating systems.

Operating system controls are deficient in many areas including configuration baselines, user account management, patch management, and security-event monitoring. As a result, ALDER cannot ensure that applications and data residing on the servers are protected from unauthorized modification, loss, or disclosure. The absence of controls is due to the lack of documented procedures; the absence of agreed upon and documented configuration baselines or checklists; implementation team members not following established security policy and standards; and, no enforcement of existing security policies and standards.

1. Configuration Baselines.[4] The ALDER project team did not apply basic operating system security configurations to the ALDER servers. As a result, authorized and unauthorized individuals could exploit the vulnerabilities resulting from these configuration weaknesses, to render the server and the ALDER system unavailable. Although a server vulnerability assessment is conducted by ETS' Security Office on some of the servers, it is done after the system is connected to the state's network and only determines whether vulnerable ports are open.

   The Control Objectives for Information and Related Technology (COBIT) framework[5] states that effective system security includes testing and monitoring information technology (IT) systems for compliance with an approved security baseline. This implies that organizations have an approved security baseline to begin with.

   We recommend ETS develop a detailed, server security configuration baseline or checklist for each type of operating system and, in conjunction with ALDER Project management, configure the ALDER servers to comply with the baseline. In addition, ETS should periodically compare hosted systems configuration to the baselines, as part of their security monitoring activities referred to in the Service Level Agreement (Agreement). The server configuration baselines should comply with State of Alaska

[4] According to Gartner, one of the leading information technology research and advisory companies, "*Sixty-five percent of attacks exploit misconfigured systems…*"

[5] COBIT's framework embodies good practices that ensure an enterprise's information technology supports the business objectives; while satisfying the quality, fiduciary, and security requirements for the information. COBIT's good practices represent a consensus of experts. COBIT was designed and created by the IT Governance Institute (ITGI) as an educational resource. ITGI was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology.

(SOA) security policies and any exceptions should be presented to the Security Office for review.

2. User Account Management. Neither ALDER's project team nor ETS' mid-tier group have implemented procedures for user account management of operating system users, groups, and access rights. Further, neither area has a formal approval process whereby data or system owners approve the access privileges requested. Lastly, neither has procedures describing how password changes and locked accounts are handled. ETS does not feel it is necessary to formalize operating system access because operating system users have access as part of their jobs in being operating system administrators. However, unauthorized individuals could access the ALDER system and retain access without being detected.

   COBIT states that effective security management includes user account management procedures that address requesting, establishing, issuing, suspending, modifying, reviewing, and closing user accounts and related user privileges with a set of user account management procedures. Included is an approval procedure outlining the data or system owner granting the access privileges. These procedures apply to all users, including administrators. Just as important, management should ensure that all users and their activity on IT systems are uniquely identifiable in order to trace the activity to a responsible party.

   Given the importance of ensuring the confidentiality of the state's payroll system (AKPAY), the state's recruitment system (Workplace Alaska) data, and the availability of the ALDER system; we recommend that ETS and the Division of Finance (DOF) develop comprehensive user account management procedures for all system access, including procedures for password resets and account lockouts.

3. Patch Management. ETS is not consistently applying all operating system security patches in a timely manner and has not developed and documented patch management procedures for the ALDER servers. As a result, some servers are vulnerable to attack by unauthorized individuals exploiting holes in the operating system. According to ETS, they are responsible under the Agreement for applying operating system security patches. However, the ALDER project team stated they had not asked ETS to do so.

   The current SOA security policy requires that all security updates or fixes be installed as quickly as possible on all systems and devices and shall not exceed the following time frame by classification:

   Critical = 3 Days
   Important = 5 Days
   Moderate = 10 Days

In addition, COBIT recommends putting preventive, detective, and corrective measures in place, especially up-to-date security patches and virus control, across the organization to protect information systems and technology.

Given that according to CERT,[6] 95 percent of security breaches could be prevented by keeping systems up-to-date with appropriate patches; we recommend that ETS develop patch management procedures so that patches are applied to meet the stated requirements. ETS should also update all ALDER servers with applicable security patches.

4. Security Event Monitoring. Event logging is enabled on some, but not all, ALDER servers. When event logging is enabled, the captured events do not comply with SOA security policy and no one is monitoring the logs. This is primarily due to a lack of an established process for the various types of servers. As a result, log records of various system events are not reviewed and analyzed to detect system violations.

   SOA security policy requires that all servers and server applications support the minimum requirements for server and application event logging. Within these requirements is a list of events the Security Office requires to be logged. Monitoring the log records is a detective control which COBIT suggests using, along with preventive controls, to protect information systems.

   We recommend ETS enable logging-on to all ALDER servers meeting the SOA's minimum requirements. We also recommend that ETS develop and implement a log monitoring strategy as part of their Agreement to provide security monitoring.

Recommendation No. 2

ALDER project management should develop an operating system performance monitoring strategy for the ALDER servers.

ETS is not monitoring the ALDER servers for indications of performance problems. The Agreement indicates that hosted servers are monitored by software to simplify the management of servers. The software features test to identify and notify administrators when defined events occur to facilitate proactive problem resolution and prevent critical outages. In addition to the standard monitoring, ETS offers tailored monitoring to meet an agency's specific needs.

---

[6] CERT is an organization devoted to ensuring that appropriate technology and systems management practices are used to resist attacks on networked systems, limiting damage, and ensuring continuity of critical services in spite of successful attacks, accidents, or failures. CERT is located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

However, servers are being monitored very minimally because the ALDER project team has not worked with ETS to develop and customize performance monitoring to meet their needs. Without adequate performance monitoring, the project team may not have the correct performance metrics in place to identify potential system outages before they occur. This is especially important for servers not running antivirus software or an intrusion prevention system, as this provides another way to identify possible server attacks. COBIT recommends that management should implement a process to ensure the performance of IT resources is continuously monitored and exceptions are reported in a timely manner.

We recommend ALDER's project management work with ETS to develop and implement a performance monitoring strategy for the ALDER servers.

Recommendation No. 3

The ETS mid-tier manager should develop host operating system backup and recovery procedures and backup ALDER operating systems to meet DOF's needs.

Neither the ALDER project team nor ETS have complete documentation of the backup and recovery strategy and procedures specific to the ALDER operating systems. In addition, ETS is not backing up an operating system regularly. The Agreement indicates that ETS is responsible for backup and recovery of managed hosts; however, they were not doing so unless requested by the project team.

Without documented backup and recovery procedures, it is unclear to agencies what is being backed up, how it is being backed up, and the frequency with which it is backed-up. Without restore procedures, the on-call administrator has to recall from memory the recovery steps necessary to timely restore a server in the event of failure. Further, without frequent system backups, it may not be possible to restore a server to its pre-failure condition. COBIT recommends that management implement a backup and recovery strategy which includes a review of business requirements as well as the development, implementation, testing, and documentation of the recovery plan. Procedures should be set up to ensure backups are satisfying these requirements and the usability of backups is regularly verified.

We recommend ETS document their operating system backup and recovery procedures, confirm with the ALDER project manager that the strategy meets their needs, and backup the operating system according to the strategy.

Recommendation No. 4

The ALDER project manager and the ETS mid-tier manager should develop a comprehensive Service Level Agreement (Agreement) that details the responsibilities and activities of each party.

The Agreement is a standard agreement template drafted by ETS and used for all hosted arrangements. As such, details are excluded as they may differ for each hosting arrangement. However, COBIT recommends having an Agreement that explains how the services will be technically delivered in an optimal manner. Even the Agreement states that its purpose and objective is to define the parameters of the service, for the benefit of the provider and the customer/agency. Following are some examples where explanations and parameters are excluded from the Agreement:

1. The Agreement includes a provision that ETS will provide tape backup of the managed hosts disk, but it does not indicate the frequency of the backups (daily, weekly, monthly, etc.); the type of backups (incremental, full, etc.); nor, the tools used to perform the backups.

2. The Agreement contains a provision that ETS will provide security configuration and monitoring, but does not describe the extent of either.

3. The Agreement contains a provision that ETS will provide maintenance support for hardware and operating system software, but includes no specifics about what this includes or how often it is done.

Without well-defined parameters of the services performed, DOF may not fully understand the services ETS provides and to which they agreed. For example, the Agreement states that ETS will provide security configuration and monitoring. According to ETS, antivirus software and an intrusion prevention system are the security monitoring tools they use for this task. However, they are not part of the configuration baseline for some of the servers discussed in Recommendation No. 1. As a result, ETS is not monitoring the security on some of the ALDER servers as agreed to in the Agreement. As such, malicious activities could jeopardize the system's availability without any advance warning or detection.

We recommend ETS develop either a comprehensive, service level agreement or an operating level agreement that details how services will be technically delivered, as well as metrics for measuring the services provided. We also recommend ETS and DOF implement some form of security monitoring, for those servers without security monitoring, until a suitable antivirus and intrusion prevention system can be installed.

Recommendation No. 5

The ETS data center manager should strengthen controls over the Juneau data center.

Generally, controls over the data center are sufficient to protect the ALDER servers; however, deficiencies exist in the areas of physical access controls, server rack security, and policies and procedures. Changes in data center management and the lack of clear, up-to-date, policies and procedures have led to ambiguity over strong data center controls.

Physical access control weaknesses at the data center include:

- lack of adequate review of requests for data center access;
- issuances of access cards to groups of contractors, including the janitorial staff;
- lack of periodic review of names of those who have access to the data center, to verify access is still necessary;
- inadequate login and logout processes;
- failure to review the visitor log book for unusual activity; and
- lack of display of ETS badges in the data center.

These weaknesses can compromise the security at the data center.

Another identified concern deals with server rack security. Doors to the server racks, within the data center, are not locked. As a result, anyone with access to the data center could intentionally or inadvertently tamper with the devices in the racks causing them to become unavailable. We recommend that the ETS data center require server racks be locked.

Finally, ETS does not have:

- complete and up-to-date data center policies and procedures for managing the Juneau data center;
- written procedures for granting, changing, revoking, and periodically reviewing data center access for the different categories of users;
- an up-to-date list of position control numbers, attached to their administrative procedure, which requires certain ETS employees to pass a background investigation;
- documented procedures for maintaining the environmental controls in the data enter; and
- documented procedures describing what to do in the event of a security incident within the data center.

COBIT recommends that the data center manager define and implement procedures to grant, limit, and revoke access to IT facilities according to business need. Further, access should be justified, authorized, logged, and monitored. This should apply to all persons entering the premises including temporary staff, vendors, visitors, or any other third-party.

We recommend management also implement physical security measures capable of preventing, detecting, and mitigating risks of theft, vandalism, and environmental hazards to IT facilities.

Recommendation No. 6

The ALDER project manager should reconcile data transferred from the source systems to the ALDER data warehouse. In the meantime, DOF should advise departments that reconciliations have not been completed.

Currently, the ALDER data warehouse contains AKSAS data from FY 01 to current. However, no reconciliations have been done to ensure the data transferred from AKSAS matches the data in the ALDER data warehouse.

As a result 450 end-users, with access to the ALDER field test environment, may be making significant business decisions with inaccurate or incomplete data. COBIT recommends verifying that all data expected for processing are received and processed completely, accurately, and in a timely manner. Although the project team has developed some reconciliation routines to ensure that data does not change during internal ALDER transformation processes, they have not developed reconciliation procedures to reconcile the ALDER data being queried to the source system.

We recommend the ALDER project team develop and implement procedures for reconciling data in the ALDER data warehouse to its source systems. Further, due to the large number of individuals who may now be relying on information in ALDER, we recommend that DOF continue to maintain an ongoing dialog with finance officers and share strategies on how users can validate the data.

Recommendation No. 7

The ALDER project manager should monitor for application security patches so they can be applied within the required time frame.

SOA security policy requires security patches, updates, or fixes be installed as quickly as possible on all IT systems. The ALDER project team receives monthly email notifications of security patches from the application software vendor. Even though this information is updated weekly on the vendor's website, the project team chose to receive monthly notifications to allow the vendor time to receive feedback from others about problems encountered when installing the patch.

Exhibit 3

Security Policy
Time Frame by Classification

- Critical = 3 Days
- Important = 5 Days
- Moderate = 10 Days

As a result, security patches for critical vulnerabilities could be available for up to a month before ALDER staff is notified. This exceeds the 3- to 10-day installation window required by policy; thus, increasing the exposure to a system compromise (see Exhibit 3).

We recommend that the ALDER project team develop a process for identifying newly released security patches so they can be evaluated and, where applicable, applied within the required time frames.

Recommendation No. 8

The ALDER project manager should conduct load and stress testing of the ALDER system.

The ALDER project team does not plan to perform load and stress testing until after the first phase of the project moves into production. This is because the project team wants to use the redundant site for this testing, but the redundant site will not be available until after Phase 1 is in production.

As a result, the ALDER system may fail if all potential users access it simultaneously. COBIT recommends that load and stress testing be performed before the system is in production. Without such testing, the project team will not know how the system will behave if 1,200 potential users access it simultaneously.

We recommend the ALDER project team conduct and evaluate the results of load and stress testing of the ALDER system before Phase 1 is in production.

Recommendation No. 9

The ALDER project manager should improve controls over application accounts.

The individuals administering the ALDER application use a shared user account. This account is the default administrator account that came with the software and has extensive system privileges. The project team is sharing this account because they have been unable to duplicate the permissions for individual accounts.

As a result, inappropriate and unauthorized changes may be made to the ALDER application and, even if detected, may not be traceable to the individual responsible. Further, passwords to application system accounts and file transfer protocol (FTP) accounts are known by ALDER developers and individuals outside the project team. COBIT recommends implementing identity management solutions to ensure that all users and their activity on IT systems are uniquely identifiable.

We recommend ALDER's project manager assign owners to the FTP and application system accounts; secure the passwords for all accounts; and, assign each administrator a unique user account.

Recommendation No. 10

The ALDER project manager should log and monitor application security events.

The audit reports, currently available in ALDER, do not satisfy the SOA minimum requirements for server and application event logging which are included in the SOA security policies. Further, procedures do not exist for reviewing or monitoring the events that can be logged. As a result, system events cannot be reviewed and analyzed to detect system violations and reconstruct user activities, if unusual or suspicious activities are identified. To date, event logging and reporting has not been a priority of the project team but is something they plan to do.

COBIT recommends that violation and security activity be logged, reported, reviewed, and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity. Further, the SOA security policies require all server applications to support the minimum logging requirements as defined. We recommend ALDER capture, report, and review application security events as required by SOA policy.

Recommendation No. 11

The ALDER project manager should develop, implement, and document a metadata model.

The ALDER project team has not developed a metadata model for the ALDER system that specifies the required metadata elements and how they will be managed. The key objectives of metadata is to provide users with information about the data, such as, how to find the data, what the data means, what the source of the data is, how the data was collected and transformed, and how the data is formatted.

Although, the ALDER project team has some metadata documented, it is neither complete nor available in a format that end-users can access and easily understand. Also, the ALDER reporting application comes with an encyclopedia function for explaining metadata and giving additional contextual information about reports; however, the project team has opted not to use it because it would be maintenance intensive.

The primary reason for implementing the data warehouse is to simplify access to data from various sources. Metadata is the key to this simplification because it provides for quality data in a usable and understandable format. Further, without reliable metadata, users may not have confidence in the data. We recommend the ALDER project team develop and implement a metadata model that defines the metadata elements and describes how the metadata will be maintained and secured from unauthorized modification.

Recommendation No. 12

The ETS manager should evaluate whether State of Alaska employee identification account and password settings can be strengthened.

End-users of ALDER logon to the system using their State of Alaska employee identification (LDAP[7]) and password. However, two LDAP account and password settings do not comply with SOA security policy. First, the LDAP password complexity setting created by ETS is "strong;" however, it does not comply with the SOA policy requiring both a number and special character. It requires passwords to be comprised of any three of the following four attributes: uppercase, lowercase, symbol, and/or number.

Also, LDAP allows more than the five invalid logon attempts required by SOA security policy. ETS intentionally set this lockout threshold higher, due to the number of applications using LDAP for authentication. Some of these applications attempt to authenticate a user two or three times, against the LDAP server, before notifying the user that an attempt has failed. So what is perceived by the user as a single logon attempt is recorded in LDAP as two or three attempts; thereby, potentially locking out a user after what he or she perceives as two invalid logons.

Allowing weak account and password settings provides unauthorized individuals a greater opportunity to compromise passwords and gain access to personal and confidential information. We recommend ETS reevaluate these settings to determine whether they can be strengthened.

Recommendation No. 13

The ALDER project manager should strengthen account and password controls.

Enterprise account and password settings do not comply with SOA security policy. In addition, the ALDER team has not developed procedures for regularly reviewing administrator and end-user accounts and privileges.

While end-users gain access to ALDER using their LDAP ID and password, ALDER system administrators gain access using the authentication mechanism that came with the software. Accounts established using the software's authentication mechanism are referred to as enterprise accounts. These enterprise accounts have weak account and password settings.

SOA security policy requires passwords be a minimum length of eight characters; passwords expire every 90 days; five passwords be retained in history; and, accounts lock after five invalid logon attempts. These stronger settings help to prevent unauthorized individuals from

[7] State of Alaska employee ID accounts use the Lightweight Directory Access Protocol (LDAP). LDAP is an application protocol for directory services used to access, query, and modify a directory listing.

easily compromising passwords, using them to make unapproved system changes, or view confidential and sensitive information. We recommend that the ALDER project team implement enterprise account and password settings that comply with SOA security policy.

In addition, ALDER system administrators have not developed procedures for regularly reviewing all ALDER accounts and privileges to ensure access is still appropriate. Without regularly reviewing accounts and privileges, individuals who no longer need access may still have the ability to make unauthorized system changes or view sensitive information. We recommend that the ALDER project team develop and implement procedures for regularly reviewing all accounts and related privileges.

Recommendation No. 14

The ALDER project manager should develop, document, and implement a comprehensive, consistent, well-controlled change management process.

The ALDER team is not following a well-controlled change management process when introducing new and changed application components to the ALDER system. The project team was unable to implement some change controls because they did not always have an available and properly configured testing environment. Having a well-controlled change management process is vital for ensuring the phases being deployed remain available and are not changed negligently.

COBIT recommends that a formal change management procedure be established to handle, in a standardized manner, all requests for change to applications and systems. These changes should be evaluated for impact on the system as well as categorized, prioritized, authorized, tested, and implemented as planned. In addition, a change tracking and reporting system should be established to document and communicate the change status. Further, a process should be established for defining, prioritizing, testing, documenting, assessing, and authorizing emergency changes that do not follow the established change process. Lastly, the respective environments should be segregated and properly protected.

We recommend the ALDER project manager develop, document, and implement a change management process that includes items recommended by COBIT.

Recommendation No. 15

The ALDER project manager should secure production programs and scripts.

The ALDER production programs and scripts on the servers are not adequately secured. The project team is using the development environment for storing production code, because it has the version control software installed. Additional weaknesses result from the lack of well-defined account and change management controls.

Maintaining production schemas and scripts on a development server, where user access is less restrictive than production, could result in developers intentionally or inadvertently changing production schemas and scripts without proper approval and testing. Currently, any developer can check out the production scripts on the development server, change them, and check them back in. In addition, comingling development and production versions on the same server makes it difficult to track and identify the version approved for use in production. Further, giving developers the ability to change production programs and data could result in them making unauthorized and untested changes directly to the production environment without going through a formal change management process. Lastly, using obsolete version control software could put programs at risk because support, fixes, and patches are no longer provided.

We recommend that all production programs, schemas, and scripts be secured so they cannot be deleted or modified without proper approval and to avoid production programs from being accidently interchanged with development programs. We also recommend the project team implement current version control software.

Recommendation No. 16

The ALDER project manager should restrict access to confidential and sensitive information to only those users with a need-to-know basis.

The ALDER project team is developing a data classification scheme in which they are identifying and categorizing every data type from all sources based on the sensitivity level of the information. End-users will request ALDER system access by completing an ALDER User Affidavit (Affidavit) where they will indicate the level of access required, based on the sensitivity level of the data fields they need to access. The Affidavit must be approved by the Department's Appointing Authority.

For AKSAS data, the ALDER team has determined that only two data categories are necessary, public and confidential. The only data element categorized confidential is the Employer Identification Number (EIN) because it can be a social security number. However, the ALDER team has not yet implemented the necessary security features to limit EIN viewing to only those individuals that requested access to confidential data. All 450 ALDER users can view EIN whether they need to or not.

Originally, the ALDER project team considered limiting access to AKPAY data by department, as well as sensitivity level (see Exhibit 4 on the following page). This would have resulted in individuals being able to view payroll data for only individuals within the same department (the exception being for departments dealing with employees in all departments such as Division of Personnel, Retirement and Benefits, etc.). However, according to the ALDER project manager, due to the costs involved in developing and

maintaining departmental access restrictions, they have decided not to limit access by department – only by sensitivity level.

During the data classification process, the ALDER team consulted with the Department of Law who opined that the State should continue to maintain data stewardship. However, good data stewardship includes granting access to confidential information on a need-to-know basis. In addition, because of the rise in identity theft, privacy legislation is pending at both the state and federal levels that would impose penalties for the disclosure of personally identifiable information.

Exhibit 4

Data Sensitivity Levels

Data Categories of AKPAY Data
(1) unclassified
(2) controlled
(3) restricted
(4) personal
(5) sensitive

Four and five reference data that contains personally identifiable information that could be used to commit identity theft.

Lastly, not only does COBIT recommend access be granted based on the individual's demonstrated need; COBIT also recommends all personnel be trained and educated in system security principles, including periodic updates.

We recommend the ALDER project manager implement field-level security for AKSAS and AKPAY data as planned. If DOF does not implement departmental access restrictions to AKPAY data, due to cost constraints, we recommend that DOF consider implementing compensating controls to further protect AKPAY data. These could include annual security awareness training for all users, requiring ALDER users to sign an annual confidentiality statement, and regularly reviewing end-user access privileges (as suggested in Recommendation No. 13).

Recommendation No. 17

The ALDER team should implement login banners at all entry points into ALDER and ensure that all login banners display the necessary information.

Users are not presented with a login banner (i.e. system use notification message) before entering credentials to log into the ALDER server operating systems. Login banners provide notice of the obligations and responsibilities related to using the computer system. Thus, users of the computer system cannot claim ignorance of their actions if they were presented with these login banner warnings. Further, lack of proper legal caption may make it difficult or impossible to prosecute someone who accesses the system without authorization. Login banners are not installed on the operating systems because ETS does not have standard hardening guidelines requiring them.

In addition, although ALDER end-users are presented with a login warning banner, it does not contain the elements recommended by NIST.[8] For example, it does not contain a direct statement alerting that access is strictly limited to state employees. Further, it does not contain a warning about unauthorized access and consequences for unauthorized access. The login banner also offers more information than is necessary such as the name of the software package and the web portal.

We recommend that the ALDER project team collaborate with ETS' mid-tier group and the ETS Security Office to develop and deploy a login warning message at all entry points into the ALDER system that conforms to best practices. NIST's publication 800-53 lists the elements that should be considered in a warning banner.

Recommendation No. 18

The chief procurement officer should develop and incorporate nondisclosure and confidentiality language into the Standard Agreement Form for Professional Services.

The agreement for professional services between DOF and CGI does not include a nondisclosure clause requiring contractors to: (1) maintain the confidentiality of the SOA's technology infrastructure, architecture, operating systems, security tools, IP addresses, etc.: and, (2) completely remove any confidential information from their systems at the conclusion of the contract. The project team did include a clause requiring that CGI maintain the confidentiality of state payroll information; however, no further confidentiality language was included because it was not part of the State's standard contract language.

Because CGI has been involved in implementing and configuring operating systems and application software, they have gained in-depth knowledge about the State's computing environment and they know passwords for system IDs with elevated privileges. This information could be used to harm, or assist in harming, the State's computing environment. Without a nondisclosure agreement, the contractor is free to share information about the State's technical infrastructure and security posture without any consequences for disclosing such information.

COBIT recommends, with regard to relationships with third-party service providers, that management should ensure that security agreements (e.g., nondisclosure agreements) are identified, explicitly stated and agreed to, and conform to universal business standards in accordance with legal and regulatory requirements, including liabilities.

We recommend the chief procurement officer develop and incorporate standard nondisclosure language into all applicable professional services agreement templates so as to prevent omission of important nondisclosure provisions in the future.

[8] National Institute of Standards and Technology

GLOSSARY

access controls: Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.

Alaska Data Enterprise Reporting (ALDER): A new statewide reporting solution which will integrate data from the statewide general accounting and payroll systems, as well as the on-line recruitment system, into a unified environment with a single toolset for user reporting.

antivirus software: A term used to describe a computer program that attempts to identify, neutralize, or eliminate malicious software. This type of software is so-named because the earliest examples were designed exclusively to combat computer virus; however, most modern antivirus software is now designed to combat a wide range of threats, including computer worms, phishing attacks, root kit, Trojan horses, and other malware.

application software: Computer software that employs the capabilities of a computer directly and thoroughly to a task that the user wishes to perform.

backup and recovery strategy: Backup refers to making copies of data so that these additional copies may be used to restore the original after a data loss event. These additional copies are typically called "backups." Backups are useful for two purposes. The first is to restore a computer to an operational state following a disaster. The second is to restore small numbers of files after they have been accidently deleted or corrupted. Backups are typically the last line of defense against data loss and, consequently, the least granular and the least convenient to use.

booted: In computing, boot is a bootstrapping process that starts operating systems when the user turns on a computer system. A boot sequence is the set of operations the computer performs, when it is switched on, that loads an operating system.

change controls: Change controls protect program and data file integrity and availability from unauthorized changes. Change controls are designed to develop, implement, and track changes to ensure that program-, system-, and infrastructure-modifications are properly authorized, tested, documented, and monitored.

configuration baseline: A term used in information system configuration management. A baseline marks an approved state of a system. Numerous configuration items can be associated with a given baseline.

Control Objectives for Information and Related Technology (COBIT) framework: COBIT is a set of best practices for information technology management, created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI), in 1992. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes, and best practices – to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

data element: A combination of characters or bytes referring to one separate item of information, such as, but not limited to: name, address, age, or social security number.

data warehouse: A computer system that collects, stores, and manages large amounts of data to be used for business analysis and reporting.

end-user: The end-user is a concept, in software engineering, referring to an abstraction of the group of persons who will ultimately operate a piece of software.

field test environment: A field test is to try out a product under conditions of actual operation or use. A test system is one that is being tested before being used for production work. In computer sciences, the environment is the entire set of conditions under which one operates a computer, as it relates to the hardware, operating platform, or operating system.

intranet: A privately maintained computer network that can be accessed only by authorized persons, especially members or employees of the organization that owns it.

intrusion prevention system: An intrusion prevention system is a computer security device that exercises access control to protect computers from exploitation.

Lightweight Directory Access Protocol (LDAP): LDAP is an application protocol for directory services used to access, query, and modify a directory listing. A directory is a set of objects with similar attributes organized in a logical and hierarchical manner. A protocol is a set of guidelines or rules that help in governing an operation on the internet and communications over it.

load test: Load testing generally refers to the practice of simulating multiple users accessing the program's services concurrently. When the load placed on the system is raised beyond normal usage patterns, it is known as stress testing.

metadata: Metadata is data about data. The metadata elements provide standardized data definitions and explain the nature of data transformations from source systems.

operating system: An operating system is the software that manages the sharing of the resources of a computer and provides programmers with an interface used to access those resources. An operating system processes system data and user input. It responds by

allocating and managing tasks and internal system resources as a service to users and programs of the system.

patch: A fix for a software program where the actual binary executable and related files are modified. Often this is used to repair a software bug or a security vulnerability.

performance monitoring: With respect to system software, a program that tracks and records the speed, reliability, and other service levels delivered by a computer system.

script: A script is a sequence of instructions that is interpreted or carried out by another program rather than by the computer processor.

schema: A schema defines the tables, the fields in each table, and the relationships between fields and tables in a relational database.

stress testing: Stress testing involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results.

web-based: A web application that is accessed with a web browser over a network such as an internet or intranet. The ability to update and maintain web applications without distributing and installing software on potentially thousands of client computers is a key reason for their popularity.

web browser: Browsers for the World Wide Web (WWW) enabling one to hook up with network servers to obtain HTML documents and Web pages. It provides a linkage among pages and documents. The server may physically be on the Internet or a private network. The browser may contain "help" applications for special files.

(Intentionally left blank)

STATE OF ALASKA

DEPARTMENT OF ADMINISTRATION

ANNETTE KREITZER, COMMISSIONER

SARAH PALIN, GOVERNOR

P.O. BOX 110200
JUNEAU, ALASKA 99811-0200
PHONE: (907) 465-2200
FAX: (907) 465-2135

RECEIVED
FEB 29 2008
LEGISLATIVE AUDIT

February 28, 2008

Ms. Pat Davidson
Legislative Auditor
Division of Legislative Audit
P. O. Box 113300
Juneau, Alaska, 99811-3300

Dear Ms. Davidson:

RE: Preliminary Audit Response to Information Systems Controls over Alaska Data Enterprise Reporting (ALDER), November 30, 2007

Thank you for the opportunity to respond to the preliminary audit report for the ALDER project issued on January 29, 2008. The Department of Administration has found the outside review beneficial to identifying areas of improvement to ALDER's security and internal processes.

Overall, we concur with the auditor's conclusion that controls over the field test environment were not adequate when the audit fieldwork ended. As reflected in the responses that follow, most of the identified deficiencies have been corrected or will soon be resolved.

Recommendation No. 1

The ALDER project manager and the Enterprise Technology Services' (ETS) mid-tier manager should implement controls to secure the ALDER operating systems.

Many improvements have been made in this area.

1. Configuration Baselines
We concur with the auditor recommendations and have completed corrections to address the majority of the recommendations for the server environments, and the rest will be compliant with the auditor

recommendations prior to operational status. Some of the recommendations, such as the Server Build Standards, will require ALDER and ETS collaboration.

2. User Account Management
Most of the recommendations identified by the auditors have been implemented or corrected, with others pending a standard from ETS. Upon a standard being available, individual user accounts will be established and maintained to conform to State of Alaska (SOA) security policy.

Further, the ALDER project manager will perform a comprehensive audit of application and user accounts, identify a clear purpose for each account, establish procedures for password reset, verify SOA security policy compliance, and document and implement procedures for all environments.

3. Patch Management
The operating system security patches are routinely applied by ETS during the servers' weekly roll using a predefined time schedule to accommodate the server power off/on sequencing and availability of particular application services during start up.

The redundant site servers will be added to Big Brother and the weekly application of operating system security patches immediately upon availability.

We concur that the intent of applying operating system patches to the servers within the allocated SOA security policy timeframe must be implemented prior to operational status.

4. Security Event Monitoring
We concur with the recommendation that ALDER meet the SOA security policy event logging standards and will work with the State Security Office (SSO) to properly configure the ALDER solution.

Recommendation No. 2

ALDER project management should develop an operating system performance monitoring strategy for the ALDER servers.

We concur with the recommendation and have implemented a number of metrics on Big Brother to monitor real time the performance of the ALDER servers.

The Big Brother monitoring will be expanded to include the redundant site servers when they become operational while the specific metrics will be continually adjusted and expanded as operational conditions demand.

Recommendation No. 3

The ETS mid-tier manager should develop host operating system backup and recovery procedures and backup ALDER operating systems to meet Division of Finance's (DOF) needs.

ETS has designed a solution for backup and recovery of the operating system and is currently working with the ALDER project manager to implement across all ALDER servers.

ETS will document the operating system backup and recovery procedures.

In addition, ETS recognizes that periodic testing of backup and restore procedures should be implemented to ensure that backups are valid and that staff are trained on the restore process. ETS will review this further and consider adopting a policy and cycle for testing and restoring data backups.

Recommendation No. 4

The ALDER project manager and the ETS mid-tier manager should develop a comprehensive Service Level Agreement (SLA) that details the responsibilities and activities of each party.

ETS agrees with this recommendation and will be developing SLAs for each of ETS' services. SLAs for similar services are developed to provide services in accordance with the ETS federally approved cost allocation plan. These principles ensure a fair and equitable sharing of the costs to provide those services.

By design ETS SLAs have not been specific. This allows some flexibility to serve customer needs and continue to adhere to federal cost principles. The current chargeback methodology as determined by the division's federally approved cost allocation plan for mid-tier services is covered by the computer services Enterprise Productivity Rate (CS EPR). Therefore an SLA for the EPR should be consistent and provide similar services at the same level. However, services funded from the CS EPR may vary from the demands of others in the mid-tier group. For example, myAlaska requires continuous administrative attention

example, myAlaska requires continuous administrative attention whereas other hosted servers can best be described as monitored but not needing intervention.

ETS has developed a Request for Proposal to replace its chargeback software. The new system will incorporate the mid-tier environment and will enable ETS to more effectively associate cost with services from the mid-tier section. Once deployed, ETS will consider revising their federally approved cost allocation plan to one that associates costs more closely with each of the services under the CS EPR, enabling ETS to be more responsive to their customers and more specific in the SLAs.

ETS is developing a division-wide standard SLA template. Once this template is finalized, ETS will work towards developing SLAs for each service, with the goal to have them complete during FY09.

Recommendation No. 5

The ETS data center manager should strengthen controls over the Juneau data center.

The management letter noted instances where the manager does not appear to have adequate control over access to the data center necessary to ensure the security of the data storage. Specifically, the auditor noted that the data center manager:

1. Does not review requests for data center access.
Access is requested through the Unicenter Service Desk (USD) via an electronic Millennium access form. The ETS data center manager receives an email for every access request entered in USD. The reason for needing access to the raised floor is entered on this form by the individual along with their immediate supervisor's name and phone number. Copies of the electronic Millennium access request form generated in USD are available.

2. Allows the issuance of access cards to groups of contractors, including the janitorial staff.
Current policy for access to the raised floor is to require a background check and fingerprints. This is coordinated and approved through the SSO. The Department of Public Safety sends this access clearance information to the State security officer who then sends the request to the ETS data center manager to grant access through the Millennium card system.

Janitorial staff has been assigned one card that is kept in Operations and is signed out to janitorial staff only. Janitorial staff are required to complete a background check and be fingerprinted by their employer. Air conditioning contractor staff have a card that is kept in Operations and it is only signed out to that contractor.

3. Does not regularly review the individuals with access to the data center to determine whether access is still necessary.
The ETS data center manager receives names of contractors and vendors from the SSO who no longer have a valid business reason for access and the cards are deactivated. A Millennium USD is created for each individual for documentation.

When an ETS employee terminates, the ETS administrative manager sends their employee access card to Operations to be deactivated. This is documented in the USD.

The ETS data center manager will run quarterly reports of those who have access to the raised floor to verify valid business needs.

4. Cannot determine who is in the data center at any one point in time.
The ETS data center manager will regularly remind ETS staff they are accountable for their visitors. A policy reminder will be placed in the visitor sign-in log book to remind ETS staff that all fields must be filled in at entry and exit.

5. Does not regularly review the visitor log book for unusual activity.
Recommended additional fields will be added to the visitor sign-in log book.

6. Does not mandate that all individuals inside the data center visibly display the ETS badge.
Door signs indicating that badges are to be visibly worn at all times will be posted. Color-coded lanyards will be purchased to represent different categories of access such as visitor, contractor, ETS staff and client department staff.

The management letter identified concerns regarding server rack security within the data center. ETS is currently assessing why the server racks are not locked and will take appropriate action based on that assessment. ETS will also review Control Objectives for Information and Related Technologies framework recommendations to assess and update policies and procedures for managing access to the Juneau data center and physical security measures.

Recommendation No. 6

The ALDER project manager should reconcile data transferred from the source systems to the ALDER data warehouse. In the meantime, DOF should advise departments that reconciliations have not been completed.

We concur with the recommendation to reconcile data transferred from source systems to ALDER. As the auditors state, even during field tests we have reconciled transaction counts between source systems and ALDER. We are in the process of implementing a reconciliation of amounts for AKSAS source system nightly loads to ALDER, similar to that performed for the GENEVA reporting system. This will be in place before ALDER is moved into production status.

We have not specifically advised finance officers about the integrity of the data beyond our steady warnings that field test is not production. Users are advised to report data anomalies they see in ALDER for resolution by the project team.

Recommendation No. 7

The ALDER project manager should monitor for application security patches so they can be applied within the required time frame.

The recommendation to timely apply application security patches within the period specified by the SSO is based on the Security Patch Management (SP-009) of the Enterprise Security Policy. Although this policy and tight implementation timeframe is intended for operating system level patches, we concur that the general principles and intent should extend to the application software. The only difference being an extended implementation period to allow for adequate change analysis, baseline, source customization, unit/integration testing, acceptance testing, and production migration. The extended period is necessary in order to maintain a reliable and predictable production environment.

The two application components for ALDER are a database and reporting software. Analysis of various types of application releases is conducted and a decision to proceed with implementation is determined. Factors that play into this analysis are:

Database

- Only quarterly patch releases that apply to the ALDER hardware platform shall be applied.

- Quarterly patch releases that are applied will typically be completed within 30 days of vendor availability.
- Major release or version upgrades are projects requiring a specialized timeframe and implementation schedule.

Reporting Software

- Every Service Pack (SP) will be applied and typically be completed within 30 days of vendor availability.
- All Fix Packs released between SP releases will be evaluated for ALDER required functionality and significant security fixes that are applicable to our environment. Only those that rise to a level of necessity will be applied and typically completed within 30 days of vendor availability.

On the rare occasion that a security fix contained within an application patch warrants an ALDER emergency condition, then all timeframes will be expedited to minimize exposure to the security risk.

Recommendation No. 8

The ALDER project manager should conduct load and stress testing of the ALDER system.

We concur with the best practice approach of performing stress testing and analysis of a system prior to placing into a production status. The current due dates for this activity and written deliverable are February and March 2008, respectively. Analysis during stress testing includes adjustments to the system to maximize load capacity and throughput. The ALDER system will not be declared a production system until after stress testing has occurred and recommended adjustments have been completed.

Recommendation No. 9

The ALDER project manager should improve controls over application accounts.

Control over application accounts that comprise the ALDER solution is indeed an ongoing concern and we concur that improved controls over the application accounts were required. We have taken many steps to limit exposure to any intentional or inadvertent alterations to source system data to the shortest time period possible.

A number of default system accounts were being used by ALDER developers during the initial and early creation of the environment. We concur that this practice is unacceptable going forward and steps have been taken to establish unique accounts for accountability and tracking of changes to the system. The application does require that certain master accounts be utilized for the ALDER solution and in those cases only team members with a need to know have access to the password.

We concur that the ALDER project manager should perform a comprehensive audit of application and user accounts, identify a clear purpose for each account, establish procedures for password reset, verify SOA security policy compliance, document and implement procedures. This audit will be completed prior to ALDER moving to operational status.

Recommendation No. 10

The ALDER project manager should log and monitor application security events.

We concur that the SOA security policy requirement for server and application event logging is required for the ALDER solution. All application activity related to write/update transactions is now being logged and is performed by either the daily ETL process or through activity associated with a specific migration. The ALDER project manager intends to continue improving the reporting to facilitate proactive review of security events, as required by policy, through utilization and performance metric monitoring in later increments.

Recommendation No. 11

The ALDER project manager should develop, implement, and document a metadata model.

We concur that a complete metadata model must be available to users so that accurate and useful information is extracted from the ALDER data warehouse. Each of the database environments maintains a metadata repository to control the reliability and recoverability of each database. Although users do not access this metadata repository directly it is available to support staff to trace data lineage.

An analysis of the Commercial-Off-The-Shelf Encyclopedia module and functionality provided with the application demonstrated little to no

benefit to explaining metadata. A number of significant issues were identified:

- Changes to Encyclopedia are enterprise wide with no department specific customization allowed.
- All Encyclopedia entries (terms, business question, and storyline) are performed manually.
- Only the title and short description entry in the Encyclopedia is available for a copied report. Since this is the typical user action the usefulness of Encyclopedia will continually decline as no automatic mechanism is available to enforce proper entries (terms, business question, and storyline).
- Encyclopedia entry updates must be performed by a user with developer access (i.e. agency advocate).

As an alternative, an InfoView and DOF web site link is available to ALDER users that provides glossary terms related to both the application and source systems. The ALDER project manager expects the contents of this link to continually grow and mature during the life-cycle of the ALDER solution.

Recommendation No. 12

The ETS manager should evaluate whether State of Alaska employee identification account and password settings can be strengthened.

ETS agrees that the Lightweight Directory Access Protocol (LDAP) does not comply with SOA security policy and is reviewing steps necessary to become compliant.

A second issue developed under this finding is that LDAP is not following the SOA security policy that requires accounts to lock after a limited number of invalid logon attempts. LDAP is a general purpose background service used by a wide variety of different systems including many different client applications such as email, web browsers and custom applications that are connected to a variety of servers. Both applications and servers may authenticate, and another intermediate service may be necessary to authenticate to LDAP. In some cases each piece may ping LDAP. If validation fails, LDAP counts each ping as an attempt, although the end user has only made one attempt.

When the lockout policy was adopted in October 2005, ETS implemented the current policy. This had a great impact on agency help desks and resulted in numerous complaints. As a result, the State security officer

reviewed the process and agreed that LDAP pings were not the same as end-user login attempts. Based on this recommendation, the security officer will consider addressing this with a formal policy.

Recommendation No. 13

The ALDER project manager should strengthen account and password controls.

The recommendation to implement enterprise account and password settings that comply with the SOA security policy has been completed since audit fieldwork ended. Further we concur that the ALDER project manager should develop and implement procedures for regularly reviewing all accounts and related privileges.

Recommendation No. 14

The ALDER project manager should develop, document, and implement a comprehensive, consistent, well-controlled change management process.

We concur that a well-controlled change management process is vital, not only for effective development, but is required for ALDER to move to production status. Each of the weaknesses identified by the auditors has been addressed.

Segregation of duties is an important component of the change management process, and we have taken steps to implement practical changes to our process as recommended by auditors. However, we recognize that we will always be challenged with segregation of duties given the small size of the support staff.

We concur that similar yet distinct environments are mandatory for successful development and controlled migration of approved system changes. The ALDER solution currently has three distinct environments, with a redundant environment available in the near future, for a highly controlled change management process. Although this has always been the desired environment configuration, technical difficulties have delayed progress.

We also concur that a strict and defined migration path between the different environments is essential. The ALDER team has developed written Migration Packet Process documentation that provides specific direction to team members for this critical aspect of building and maintaining ALDER.

The availability of multiple identical environments, as outlined above, provides an opportunity for emergency application corrections to be validated prior to applying to the production environment. This is particularly important when the application correction involves data within the database as miscues or impromptu changes can cause significant damage and lengthy recovery time given the volume of data contained in ALDER. We intend that emergency application correction would simply be fast tracked through the regular migration process allowing for appropriate levels of verification, validation, and refinement of steps required to implement a change in the production environment.

Recommendation No. 15

The ALDER project manager should secure production programs and scripts.

We concur that consistent and reliable version control methodology should be implemented that allows for cross platform migration. The ALDER project manager intends to continue the development of the ALDER Migration Packet Process documentation to specify server, directory, retention, and naming conventions associated with script changes, as well as method of implementation in the various environments that comprise the migration path.

Recommendation No. 16

The ALDER project manager should restrict access to confidential and sensitive information to only those users with a need to know.

The ALDER team has carefully considered the confidentiality requirements of the data available for reporting. As the auditors state, the data classification process was based on consultation with the Department of Law.

The personal information in AKPAY has complex security requirements, as demonstrated by the five planned data classifications. These will be designed into Increment 2, in which AKPAY data will become available for reporting.

It is true that security will not limit access by department. This option was considered during the design phase, but rejected at that time for two reasons. First, such security would be difficult to establish and labor-intensive to maintain. Second, the State of Alaska is a single employer,

and reporting needs often legitimately cross departmental organization lines. The ALDER team has chosen to treat our employee information as a single database and establish security based on the confidentiality of the data contained within each field.

All users of ALDER with access to data beyond the unclassified level will sign a user affidavit affirming their understanding of their responsibility with regard to confidential data.

Recommendation No. 17

The ALDER team should implement login banners at all entry points into ALDER and ensure that all login banners display the necessary information.

The ALDER team will evaluate the points of entry into the server operating systems for placement of login banners. The team will work with ETS staff to determine where banners should be located, and the appropriate language where they are applicable.

The login warning banner that is presented to users was developed in conjunction with Department of Law and was therefore regarded as acceptable. The auditors point out some elements recommended by NIST that the current banner lacks. These will be referred to the Department of Law for consideration of amending the current end-user login banner.

Recommendation No. 18

The chief procurement officer should develop and incorporate nondisclosure and confidentiality language into the Standard Agreement Form for Professional Services.

The department agrees with the recommendation that the chief procurement officer (CPO) should develop nondisclosure and confidentiality language for information technology (IT) contracts.

Division of General Services (DGS) staff have reviewed nondisclosure and confidentiality clauses developed for large IT projects and have worked with the security officer located in ETS to draft such a clause. That draft is under review in the Attorney General's Office. Once the draft is finalized, DGS will revise the Request For Proposals (RFP) and Invitation To Bid (ITB) shells to include this language. We anticipate that this will be accomplished within the next few weeks. However, rather than incorporating this clause into the Standard Agreement Form for

Professional Services, which is required for all professional services contracts (not just IT contracts), the CPO believes it would be more appropriate to include the clause in the standard solicitation documents (RFP & ITB). The terms and conditions of a solicitation are included in resulting IT contracts by reference, and any firm responding to a formal (over $50,000) solicitation would have to agree to this clause, or risk being declared nonresponsive and eliminated from consideration. DGS also plans to issue a Procurement Information Message informing procurement personnel state-wide of this change, and requiring agencies to include the clause in all IT contracts that are established via small procurements ($50,000 and less) and alternate procurements such as single source and exempt procurements.

Thank you again for the opportunity to comment and for the professional review conducted by the auditors. Their review of ALDER during its development and field test phases will contribute to its integrity and durability once it is moved into full production.

Sincerely,

Annette Kreitzer

cc: Scot Arehart, ALDER Project Manager, Division of Finance
Anand Dubey, Director, Enterprise Technology Services
Kim Garnero, Director, Division of Finance
Vern Jones, Director, Division of General Services

(Intentionally left blank)