Secretary of State Audit Report

Jeanne P. Atkins, Secretary of State

Gary Blackmer, Director, Audits Division

State Data Center: First steps to address longstanding security risks, much more to do

Executive Summary

Over the last nine years, security weaknesses at the state data center have put confidential information at risk. These weaknesses continued because the state abandoned initial security plans, did not assign security roles and responsibilities, or provide sufficient security staff. The Governor, Legislature, and Chief Information Officer have taken the first steps to fix these problems, but the solutions will take time, resources, and cooperation from state agencies.

Critical security issues were never resolved at the data center

Data center management and staff are meeting day-to-day computing needs of state agencies relying on its services. However, critical security issues identified throughout the past nine years were never resolved.

Security problems affect multiple components of the data center's layered-defense strategy intended to make it more difficult for unauthorized users to compromise computer systems.

These weaknesses increase the risk that computer systems and data could be compromised, resulting in leaked confidential data such as Social Security numbers and medical records information.

Data Center Security Warnings Issued:

2006 Public Audit
2008 Public Audit
2008 Confidential Audit
2008 Consultant Report
2009 Public Audit
2009 Confidential Audit
2010 Public Audit
2010 Public Security Audit
2010 Confidential Audit
2012 Public Audit
2012 Confidential Audit

Data center was never fully configured for security

Management got a good start on security planning, but during data center consolidation management abandoned the plan, thinking they would complete some steps at a future time. Once the data center became operational, staff was overburdened and unable to make meaningful progress to resolve critical security issues or implement security systems they purchased.

These adverse conditions continued because management did not assign overall responsibility or authority to plan, design, and manage security. In addition, they did not provide the necessary staffing to implement and operate security systems.

First steps have been taken to resolve longstanding data center problems

The Govenor, Legislature and Director of the Department of Administrative Services took steps in the last six months to address data center staffing and organizational issues.

Two key steps that occurred were the state Chief Information Officer (CIO) became responsible for data center operations and the state Chief Information Security Officer was moved to the data center and tasked to oversee its overall security function.

These actions increased management's focus on security at the data center. However, it will take additional time, perseverance, significant resources, and cooperation to resolve all known weaknesses.

Some computer operations were stable but disaster recovery was only partially tested

Apart from security, data center staff provides important operational support to agencies, including routine backups and monitoring computer processing. Data center staff made significant strides to resolve prior disaster recovery weaknesses identified by earlier audits. Their innovative approach was to partner with the Montana State Data Center to establish an alternate site to store and process data. However, additional work needs to be done to ensure data at that site is secure, update recovery plans, and test the system.

Recommendations

We recommend agency management take steps to reconfigure data center security to provide the layered-defense strategy needed to protect state data systems. To accomplish this, management should clearly define security roles, responsibility, and authority to carry out the plans and provide sufficient staff.

We also recommend management update and fully test disaster recovery plans and ensure data is secure at the remote site.

Agency Response

The agency agreed with all of the audit findings and recommendations. The response includes specific plans to correct longstanding security weaknesses and improve overall security organization, plans and staffing. Their full response is attached at the end of the report.

Background

The Department of Administrative Services (DAS) is responsible for providing centralized computer services for state agencies through its Enterprise Technology Services' data center (data center). The data center is comprised of a complex and extensive inventory of computer operating system platforms, networks, and associated enterprise security infrastructure. Eleven state agencies use data center resources to operate hundreds of computer applications, including mission critical systems that often contain citizens' confidential information, such as personal income tax returns, Social Security numbers, driver's license information, and confidential medical records. In addition, the data center provides Internet service and networking for the majority of state agencies.

Security threats are severe and continue to worsen

The nature of risks to computer systems continues to worsen as obtaining and using hacking tools becomes easier and increases the sophistication and effectiveness of attacks.

In recent years, a number of high profile attacks have been reported, including:

- Federal system breach resulted in leaked confidential data of millions of federal employees, contractors, and other people.
- *Stuxnet* computer worm attacked machinery within Iran's nuclear program.
- Numerous retail attacks resulted in lost credit card numbers and reduced consumer confidence.

Verizon and a number of partners, including security firms and governmental agencies, compile and publish an annual Data Breach Investigation Report. The report evaluates security incidents and confirmed data breaches and examines common security patterns and threats. The Verizon report for 2014 indicates that the governmental sector continues to lead all other industry categories in the number of reported security incidents and confirmed data losses.

Oregon has much to lose

State agencies depend on computer systems to carry out their operations and to process, maintain, and report essential information. Virtually all state operations are supported by automated systems and electronic data. Security breaches in these systems can result in significant losses. For example:

- payments and collections, could be lost or stolen;
- computer systems and their data could be used for unauthorized purposes, including the launching of attacks on others;

- sensitive information, such as taxpayer data, Social Security records, medical records, and other personally identifiable information could be inappropriately added, deleted, read, copied, or disclosed;
- critical emergency services could be disrupted;
- data could be modified or destroyed for purposes of fraud or disruption; and
- state agency missions could be undermined by embarrassing incidents that result in diminished confidence of their ability to conduct business and fulfill their responsibilities.

Previous Reports and Assessments

- 2006 – Project plans did not address how critical security and disaster recovery services would be provided.
- 2008 – Data center had not yet provided a secure computing environment for clients
- 2008 – Confidential letter providing additional detail
- 2008 – Confidential consultant report confirms security concerns included in the previous audits
- 2009 – Department's legislatively mandated state security plan did not include details about data center security
- 2009 – Confidential letter that enterprise accounting and payroll computer programs at risk due to security problems at the data center
- 2010 – Previous security problems remain unresolved
- 2010 – Confidential letter providing additional detail
- 2010 – Governance structure not effective for improving security
- 2012 – Little meaningful progress in resolving the previously reported security problems
- 2012 – Confidential letter providing additional detail

Longstanding security warnings

We audited plans for the state data center just prior to its completion in 2006, and returned periodically to re-evaluate controls. During these audits we identified numerous security weaknesses that remained unresolved.

In September 2006, we issued an audit report titled Department of Administrative Services: Computing and Networking Infrastructure Consolidation Risk Assessment. We reported that project plans to create the state data center were incomplete in part because they did not sufficiently address how critical security and disaster recovery services would be provided.

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

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

In February 2009, we issued an audit report of the department's Enterprise Security Office. In that report we found that DAS's legislatively mandated state security plan did not contain details regarding how the data center would be secured, including how confidential information should be safely stored or transmitted.

In April 2009, we issued a confidential management letter to DAS management in conjunction with our annual audit of the state's Statewide Financial Management Application and Oregon State Payroll Application. That letter indicated that systems were at increased risk because of specific security weaknesses at the data center.

Our March 2010 audit found that the data center had not resolved most of the security weaknesses reported in the previous audit. We provided details in an accompanying confidential audit report. Because of the duration of these weaknesses, we expanded the audit work to determine why they were not resolved. We issued an additional report concluding that the governance structure was not effective for managing security at the data center.

In January 2012, we issued a confidential management letter in conjunction with our public management letter indicating that management had made little meaningful progress in resolving the security issues identified in prior audits.

Strong data center security should be multi-layered and collaborative

Proper security for a data center requires a coordinated use of multiple security components to protect the integrity of the computer systems and their data. The security industry refers to this methodology as defense in depth. Defense in depth is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier.

This security methodology minimizes the probability that hackers' efforts will succeed. In addition, it can help system administrators and security personnel identify people who attempt to compromise a computer system. If a hacker gains access to a computer system, defense in depth also minimizes the impact and provides time for staff to deploy new or updated countermeasures to prevent recurrence.

Some common components of data center defense in depth include using antivirus software, firewalls, operating system updates, anti-spyware, system configuration management, and intrusion detection or prevention systems. In addition, physical protection of a data center site coupled with ongoing personnel training are both necessary to enhance security.

The data center has its responsibilities for security, but agencies in Oregon manage their own computer programs, which imposes equally important security requirements. Agencies must ensure that programs and their users do not provide hackers easy access to systems and data by allowing them to compromise computer code or bypass security mechanisms.

We will address the agency aspect of security in a future audit that evaluates how well state agencies carry out their security efforts. We will also re-evaluate security at the data center in a separate future audit.

Audit Results

Critical security issues have never been resolved

Data center management and staff continue to provide adequate controls to limit physical access to the building. However, they have not yet resolved most of the security weaknesses we identified during previous audits.

These unresolved weaknesses include significant components of defense in depth including:

- System configurations are not adequately managed.
- Monitoring and managing users with special access is inadequate.
- Critical network monitoring devices are not fully functional.
- Obsolete network equipment was not replaced.
- Obsolete operating system software is not always updated.
- Potential security incidents are not adequately tracked.

Collectively, these weaknesses can have costly and far reaching consequences, including a heightened risk that the security of computer programs hosted at the data center could be compromised.

System configurations are not adequately managed

A vital part of providing good security at a data center is controlling security configurations of operating systems and network control devices.

The data center staff has not maintained a complete inventory of authorized device configurations. In addition, they did not have processes to monitor systems to detect if configurations are inappropriately changed.

Without configuration management and monitoring, data center staff is less likely to detect unauthorized changes to critical security settings or identify systems that are not configured according to best security practices. Unauthorized changes to security settings could potentially allow a hacker to gain access to confidential agency information, including Social Security numbers and other information valuable to identity thieves.

These configurations control many vital security functions such as monitoring activities, automated operating system software updates, anti-virus updates, and access settings.

Security standards indicate that entities should establish standard configurations for each system. They should periodically monitor configurations to ensure unauthorized changes have not occurred, and also have processes and procedures for changing the standard configurations as needed.

Monitoring and managing users with special access is inadequate

Data center personnel responsible for maintaining systems and networks need powerful access to perform their job functions. This privileged access allows these users to view or alter everything on a system, including system data.

Best practices for security indicate that all privileged users should be authorized and their actions closely monitored. Data center management has not developed or implemented adequate processes for ensuring privileged users remain authorized. In addition, they do not have processes to routinely monitor the changes each privileged user makes to systems to ensure they are appropriate.

We noted that data center systems create transaction records that could identify the actions of privileged users. However, data center staff indicated that they did not routinely monitor these records. As a result, data center staff is less likely to detect unauthorized changes to systems and data, including those affecting confidential information contained in systems.

Critical network monitoring devices are not fully functional

Deployment of intrusion detection and prevention systems is an important element of a layered-defense security strategy. These security devices monitor network traffic for telltale signs of attacks, which can then be quickly and appropriately contained and resolved. However, the huge volume of traffic on the state's network requires an automated system to effectively analyze the gathered network and system information.

The department purchased intrusion detection and prevention devices when it created the data center but did not fully implement them. The data center replaced these systems with new devices that have enhanced capability, but have not yet fully configured them for all customer networks.

In order for these network security devices to effectively detect unusual events, information they collect must be aggregated and correlated with information collected by other systems. The data center purchased a system to manage this aggregation and correlation within the first year of operation but they never configured it to provide the anticipated benefit. In December 2014, data center management acquired a replacement system to collect and manage network and system information, but this system is also not yet fully configured or functional.

These deficiencies greatly diminish the state's ability to provide a secure operating environment. Without effective network monitoring, dangerous network traffic or attacks may not be quickly detected and their adverse effects may not be appropriately mitigated.

Obsolete network equipment was not replaced

To ensure ongoing technical support is available, network hardware needs to be replaced when it is no longer supported by its vendor. Vendors provide updates to repair known vulnerabilities in their hardware for only a short time after determining it is obsolete.

In April 2011, data center managers were aware that approximately 20% of a certain type of network device was obsolete and had critical security vulnerabilities. Some of these devices were already past their useful life in 2006.

In 2014, the department requested and received additional funds from the Legislature to replace the hardware and other computing equipment. Management indicated that they are hiring contracted staff to accelerate the replacement of the obsolete equipment, but the project will continue well through 2016.

Continuing to rely on obsolete network equipment exposes state computer systems to various forms of network based attacks.

Obsolete operating system software is not always updated

Security standards indicate organizations should have strategies for ensuring operating system software is appropriately updated to reduce the risk that known weaknesses could be used to compromise computer systems.

Many of the state's enterprise computer programs are hosted on the state's mainframe computer. However, an increasing number of computer programs run on approximately 2,000 servers using various versions of Linux and Microsoft Windows operating system software. Some computer programs can only function on servers with specific operating system versions.

As vendors become aware of security vulnerabilities in their software products, they distribute updates, or patches. However, vendors generally do not support their products forever and routinely announce when they stop providing these updates for older versions of their software products.

The data center has approximately 175 servers that have operating systems that are no longer supported by their vendors. Using these servers increases the risk that computer programs and data residing on them could be hacked. This risk of compromise may extend beyond these servers, allowing intruders access to other computer systems attached to them.

The risks posed by the obsolete operating systems could be reduced by applying a solution, such as isolating the affected servers by moving them to a network not connected to other systems. However, the data center has not taken steps to do so.

Potential security incidents are not adequately tracked

Security standards indicate that responsibilities and procedures should be in place to handle information security incidents once they have been identified and reported to management.

We noted that the data center was not tracking or evaluating potential security incidents identified by staff during routine network monitoring.

The data center works with the department's Enterprise Security Office to investigate potential security incidents. However, that office may not investigate a potential security incident if it affects only the data center or a single agency. The data center also does not have a security incident plan or procedures for potential incidents that do not involve multiple agencies and does not have forensic capabilities.

Data center staff are less likely to notice patterns of on-going or persistent attacks without a process for tracking or evaluating them. The lack of procedures and incident plan weakens the data center's ability to understand and respond to threats and attacks.

Data center was never fully configured for security

Three key ingredients to proper management of information technology security functions is that they must be properly planned, organized and appropriately staffed to accomplish strategic goals and objectives. The security weaknesses at the data center remain unresolved because the department did not follow through on the key components in the initial security plan, which described how security would be provided, assigning security roles and responsibilities, and calling for sufficient staff to implement and maintain security systems.

A good start on security planning was abandoned

During the initial planning phase for creating the state's data center, consultants and technology professionals from state agencies created the Information Security Capability Architecture Plan in 2005 (2005 plan). This comprehensive 105 page document defined the security program and architecture for the data center.

The 2005 plan is a well crafted document based on best practices for security. Its creation was a necessary first step in establishing a security program. However, it was only a first step because it did not provide all the necessary detail to bring its requirements and concepts to fruition.

Data center consolidation and implementation of critical security components did not follow that plan. Rather, state agency equipment was moved to the new data center in their existing state, anticipating that the necessary changes would occur at a later time.

During this time, data center management abandoned many of the planned security measures. Key components were never installed or were only partially implemented. One of the most significant security flaws occurred when the data center abandoned the 2005 plan that called for segregating systems with more confidential data or systems with more security vulnerabilities.

In each of our data center audits, we found that management made little progress in planning for and implementing critical security systems or in resolving identified security weaknesses. In several instances the data center made an effort to address some problems by purchasing security hardware. However, they did not fully implement these systems, abandoning them before benefit could be achieved.

Security function never established at the data center

When developing the data center, planners stressed the importance of establishing specific security functions, roles, and responsibilities within the data center. However, this did not occur as planned.

The 2005 plan intended for the security function within the data center to work in cooperation with the DAS Enterprise Security Office. This office had no authority over the data center to direct the design or implementation of security controls. In addition, DAS placed the state Chief Information Officer and the state Chief Information Security Officer in the ESO and a security function was never established at the data center.

Data center managers did not hire a technical security professional to assume the role of security architect until 2009. However, this individual did not have the necessary staff, support or authority from management to resolve the known security weaknesses or to develop a security plan. Management eliminated the position in 2012 after the individual transferred to another state agency, again leaving nobody responsible for overall security at the data center.

In earlier audits, we found that management did not resolve security weaknesses because they did not clearly define or communicate security standards, or assign overall responsibility for managing the security function. Many identified security weaknesses continued to exist simply because nobody had the authority or responsibility to resolve them.

Data center security work exceeded staff resources

The 2005 plan for the data center indicated that at least eight full time staff should be dedicated to design and manage security systems. In addition, operational staff would have specific security assignments related to their particular service domains.

Since its development, the data center has not had the human resources necessary to carry out critical security functions. Managers generally assigned already burdened operational staff to install security systems. However, dedicated staffing was not assigned to respond to alerts or other system outputs.

With nobody assigned to manage overall security and insufficient staff to implement and operate security components, the slow and unsatisfactory progress to resolve identified security weaknesses was predictable.

First steps taken to resolve longstanding data center problems

During this audit, the Director of the Department of Administrative Services, Governor, and Legislature took action to address data center issues.

In February 2015, the DAS Director assigned overall responsibility for the data center to the state Chief Information Officer (CIO). In addition, the CIO now answers directly to the Governor.

To better address security concerns, the state CIO moved the state Chief Information Security Officer to the data center to begin managing the overall security function.

Legislative testimony indicated that the Governor directed the state CIO "to take charge of the ETS [Enterprise Technology Services] unit, managing its daily operations and services for the foreseeable future…… and continue to work closely with the Legislature to address how I.T. resources should be structured and funded in the future to ensure transparency and public access to information as well as secure, cost-effective service delivery."

The 2015 Legislature passed HB3099 to formalize the state CIO's responsibility for information technology throughout the state, including the data center.

These actions were necessary and appropriate advances toward resolving organizational issues at the data center, and helping to focus management attention on security. With these changes, managers have also started to develop the security function within the data center.

However, there are many longstanding security weaknesses and resolving them will require significant resources, time, perseverance, and the cooperation of other state agencies. Some problems will likely require the state CIO to exercise the authority to impose changes on those state agencies.

Day-to-day computing was stable but disaster recovery was only partially tested

We also evaluated the data center's ability to meet the day-to-day needs of state agencies relying on its services. Specifically, data center management and staff continued to:

- monitor and control the physical environment to limit physical access and protect computing resources from environmental hazards, such as excessive heat and humidity;
- provide routine back-ups for agency computer programs;
- monitor computer processing to ensure production problems and incidents are appropriately investigated and resolved; and
- allocate operating costs in compliance with federal guidelines and according to the agreed-upon cost recovery model.

Disaster recovery strategies are only partially tested

Restoring data center operations after a disaster or serious disruption requires significant advance planning, coordination, and testing. In addition, data backups stored off-site should be protected against loss or inappropriate disclosure.

As part of its disaster recovery strategy, data center management entered into a unique and innovative inter-governmental agreement with the state of Montana. The agreement allows the data center to replicate its computing environment and data inside the Montana State Data Center. However, management has not fully ensured that data at the remote site is secure.

Data center staff also had not updated recovery procedures to fully reflect the current strategy. In addition, work remains to ensure all systems are replicated at the off-site location. As a result, data center staff could not test all systems.

Without fully updated and tested plans, the state may not be able to quickly recover some critical technology infrastructure in the event of a disaster, especially if experienced data center staff is unavailable.

Recommendations

To correct the unresolved security weaknesses, we recommend management:

- develop and maintain a complete inventory of system device configurations and processes for monitoring systems to detect unauthorized changes;
- develop and implement processes to ensure privileged users remain authorized and that changes these powerful users make are appropriate;
- fully implement newly acquired network monitoring devices and systems to collect and analyze network and system security data;
- replace network equipment that is no longer supported by vendors;
- replace obsolete operating systems or provide other mitigating controls for them, such as increasing monitoring or isolating them from other state computing resources; and
- create and implement a plan with associated procedures to track and evaluate potential security incidents.

To better configure the data center for security, we recommend management:

- create and implement a comprehensive security plan to appropriately configure security, implement critical security systems, and resolve identified security weaknesses;
- clearly define and assign data center security roles, responsibility, and authority; and
- provide sufficient human resources to carry out critical security functions.

To ensure that the state's computing infrastructure, computer programs, and data could be restored after a disaster, we recommend management update and fully test disaster recovery plans and ensure data is secure at the remote site.

Objectives, Scope and Methodology

Our audit objectives were to:

- Determine if Enterprise Technology Services provides adequate security controls to protect agency and enterprise computer programs and data.
- Determine if Enterprise Technology Services provides a controlled and stable operating environment for agency and enterprise computer programs.

We focused our efforts on determining the status of previous audit findings and controls in place during calendar year 2014 and the first quarter of 2015.

To address our audit objectives, we:

- reviewed policies and procedures,
- observed physical controls,
- reviewed various project and recovery plans,
- reviewed network drawings, inventory records, and system reports,
- reviewed rate setting and adjustment processes,
- verified rate setting calculations, and
- interviewed data center management and staff.

Because of the sensitive nature of the security issues, we communicated some details of security findings in a confidential meeting with management in accordance with ORS 192.501 (23). We did not issue a separate confidential report.

We used the IT Governance Institute's publication, "Control Objectives for Information and Related Technology" (COBIT), the United States' Government Accountability Office's publication "Federal Information System Controls Audit Manual" (FISCAM), and International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002 to identify generally accepted controls 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 objective. We believe that the evidence obtained and reported provides a reasonable basis to achieve our audit objective.

Oregon

Kate Brown, Governor

Department of Administrative Services
Chief Information Office
155 Cottage St NE, 4th Floor
Salem, OR 97301
PHONE: 503-378-3175
FAX: 503-378-3795

August 20, 2015

Oregon Secretary of State
900 Court Street NE, Rm 136
Salem, OR 97301

RE: ETS Response to Audit Results

Security Changes at the Data Center

Under HB 3099, the State Chief Information Officer (CIO) is now responsible for security at the State Data Center (SDC). The State (CIO) and State Chief Information Security Officer (CISO) have reviewed the results of this audit and generally concur with the findings.

To improve accountability and overall execution effectiveness, roughly 10% of existing SDC staff and all security operating budget is being moved to the Enterprise Security Office (ESO) led by the State CISO. The State CISO is now fully accountable for the security at the State Data Center.

Key transition activities are underway to set the SDC up for security success, all of which are scheduled for implementation by the end of 2015:

- Formation of a Security Operations Center with staff dedicated to monitoring and response for security events
- Investment in additional staff to accelerate the transition of outdated infrastructure
- Putting a security program manager in place to drive all security projects to completion, countering the history of partial complete projects
- Review and update of all SDC security policies and procedures, with specific focus on monitoring, incident response, privileged access, configuration management, compliance and risk management
- Security risk assessment conducted by an external third-party to better align priorities to those that will make the most significant risk reductions

Responses to Audit Results

We agree with the findings and recommendations made by the Secretary of State auditors. Below are some specifics on activities either planned or already underway to address each recommendation highlighted in this report.

Develop and maintain a complete inventory of system device configurations and processes for monitoring systems to detect unauthorized changes

System baseline configurations and standards have been developed at ETS, but the definitions are not in place for every type of system in use at ETS. Further, a regular process of review and monitoring of these settings is currently ad hoc. ETS is going to address this by identifying and completing documentation of baselines where they are absent, out-of-date or otherwise inadequate. This work is being started now and targeted for completion in the first half of 2016 at the latest.

Once documented baselines are in place, ETS will work in partnership with agencies to evaluate existing systems for deviations from secure baselines and address identified issues on a case-by-case basis. This process will leverage tools already in place at ETS in most cases. Where tools are found lacking, we will look to acquire adequate tools wherever possible. The intention is to automate this so that it is easily and quickly repeatable.

After baselines are established and work is underway to address deviations, work to create repeatable periodic procedures to monitor for deviations will be put in place, with a target to complete in the first half of next year. To ensure the process is repeated regularly, focus will be on ensuring processes are automated as much as possible to ensure regular execution.

Develop and implement processes to ensure privileged users remain authorized and that changes these powerful users make are appropriate
ESO continually works to improve our privileged access management at the State Data Center. We are specifically looking at tools, policies and procedures that can help us identify and act on status changes that might affect level of privileged access granted to individuals in systems we manage and maintain, to provide complete lifecycle management over privileged access grants. Today automatic account expiration and manual account removal on exit are in place, but more improvements can be made, especially around internal role changes and automation of account removal on exit.

ESO is also looking at best methods to consistently detect insecure configuration through active real-time integrity monitoring and regular vulnerability scanning at the both the network and server layers. We have started to deploy security incident and event monitoring (SIEM) at ETS, but are still in the early phases. Leveraging this system for monitoring of unauthorized or anomalous system changes will be addressed in later phases of that deployment.

We have deployed vulnerability management capabilities at both the system and network layers, but intend to take those deployments and leverage them more consistently on a schedule with full support for vulnerability remediation.

Fully implement newly acquired network monitoring devices and systems to collect and analyze network and system security data
In the mid-2015, ETS completed acquisition and initial deployment of security incident and event monitoring (SIEM). SIEM projects are very complex and require a great deal of time and effort to get right, so SIEM is being implemented in phases, focusing on highest priority assets and event sources first.

In addition to a phased approach for implementing improved monitoring capabilities, monitoring and response of these new capabilities is being addressed through formation of a dedicated Security Operations Center (SOC) with the sole purpose of monitoring for and responding to security incidents in real-time. While these functions have existed at ETS in the past, the team was distributed throughout ETS without specific accountability and ownership. Formation of the SOC under the State CISO will ensure accountability and consistent monitoring, analysis and response to security events. The SOC will be up by the end of this year.

Replace network equipment that is no longer supported by vendors
ETS is in the process of removing obsolete network equipment. It is a multi-year process that involves changes to every agency in the State. Excellent progress has been made in moving agencies to supported equipment, but until every user of a piece of equipment is migrated, the legacy device cannot be removed from service.

To accelerate migration from old equipment, additional staff are being hired on a short term basis to ensure this gets dedicated focus and is not slowed by day-to-day security operations and other ETS customer demands. With increased staffing levels, we expect to be able to complete infrastructure replacements by the end of 2016.

Replace obsolete operating systems or isolate them from other state computing resources
ETS and ESO are actively working with customer agencies to address obsolete operating systems that support each agency's functions. This issue must be worked in partnership with the agencies as many of these systems support custom applications that were only built on these obsolete operating systems; operating systems upgrade cannot take place without first updating application code. These custom applications provide vital State services that cannot be taken offline while application upgrades are taking place.

By standard operating procedures at ETS, servers are only connected to other assets explicitly, based on specific connectivity needed to implement their function (least privilege). As a result, further isolation can often not be implemented without stopping the function of the applications the system supports.

Identification of obsolete operating systems through regular vulnerability scanning is being implemented. Where obsolete operating systems are identified in the environment, risk assessment will be completed around each identified obsolete system in partnership with client agencies and additional mitigations put in place where possible and practical until migration of applications to supported operating systems can take place.

This will be an on-going process, working in partnership with agencies to determine risks, mitigations and plans for upgrade in a way that does not degrade critical State services. Completion is heavily dependent on agency participation, but we expect the majority of the instances can be addressed by the end of next year.

Create and implement a plan with associated procedures to track and evaluate potential security incidents
Security incident handling policy has already been documented, reviewed and put in place at the State Data Center, directly owned by the State CISO. We are currently working to document procedures that support that policy and reflect the undocumented response procedures already in

place. Formation of the centralized Security Operations Center will clarify and specifically staff security incident identification and response as a primary data center function, with clear line of accountability to the State CISO and State CIO.

Create and implement a comprehensive security plan to appropriately configure security, implement critical security systems, and resolve identified security weaknesses
With the recent moving of ETS security operations under the Enterprise Security Office, the State CISO is in the process of writing a new comprehensive Enterprise Security Plan which will include specific plans for security operations at ETS. It is expected that this plan will be published by the first quarter of 2016.

Clearly define and assign data center security roles, responsibility, and authority
The new Enterprise Security Plan currently being written will address roles, responsibilities, authority and accountability for all enterprise security functions, including those specifically at the State Data Center.

Provide sufficient human resources to carry out critical security functions
We have recognized the need for dedicated human resources to carry out critical security functions and as a result moved nearly 10% of current ETS staff to the Enterprise Security Office under the direction of the State CISO. Through this transition, we will also be evaluating what critical staffing needs still exist and bringing those forward for review with Legislature. In addition to regular staffing, we are also applying incremental contract resources to address specific gaps identified in this report.

To ensure that the state's computing infrastructure, computer programs, and data could be restored after a disaster, we recommend management update and fully test disaster recovery plans and ensure data is secure at the remote site
The State Data Center has made great progress in designing and implementing an innovative disaster recovery capability, leveraging relationships with the State of Montana. This project is a large multi-year undertaking being completed in phases. Infrastructure is now in place at State of Montana to facilitate operation of some critical systems and recovery of critical data in the event of disaster and testing of capabilities in key areas has already been completed.

Subsequent phases are underway to complete installation, transition of data and configurations to the infrastructure in Montana to make all infrastructure in place effective for disaster recovery. Further training of staff and testing of capabilities will be completed as more capabilities are put in place. This is targeted for completion for full infrastructure capability to be online with tests completed in mid-2016.

Work has also recently been started with agencies to further identify additional critical State infrastructure and data that needs to be addressed above the basic infrastructure level, as well as identify recovery goals for each agency. This activity will be on-going with requirements still to be defined. As requirements still need to be collected from each agency, it is difficult to estimate completion at this time. Testing with agencies to determine effectiveness will take place ETS builds out plans with each agency.

Security of data and systems at the Montana Data Center is being maintained at the same levels and standards of care in place in at Oregon's State Data Center. Montana Data Center physical security is held to the same federal compliance standards as Oregon (CJIS, PCI, HIPAA, IRS Publication 1075, etc.), including oversight and audit by FBI, IRS and other federal entities. Oregon security personnel conduct periodic audits at the Montana facility as well, as required by various regulations. At the system and data level, the same security protections, policies and procedures used in the Oregon State Data Center are applied to Montana, managed completely by ETS personnel.

Sincerely,

Alex Z. Pettit, Ph.D.
State Chief Information Officer

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 other agencies within 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 Garber, CGFM, MPA, Deputy Director

Neal Weatherspoon, CPA, CISA, CISSP, Audit Manager

Teresa Furnish, CISA, Senior Auditor

Amy Mettler, CPA, CGFM, CISA, Staff Auditor

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

website: sos.oregon.gov/audits

phone: 503-986-2255

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

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