STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2017-087
January 2017

AGENCY FOR STATE TECHNOLOGY

State Data Center Operations

Sherrill F. Norman, CPA
Auditor General

Executive Director of the Agency for State Technology

Section 20.61, Florida Statutes, creates the Agency for State Technology. The head of the Agency is the Executive Director and the State's Chief Information Officer who is appointed by the Governor, subject to confirmation by the Senate. Jason M. Allison served as Executive Director and Chief Information Officer during the period of our audit.

The team leader was Andrew Denny, CISA, and the audit was supervised by Brenda Shiner, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

This report and other reports prepared by the Auditor General are available at:

www.myflorida.com/audgen

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

AGENCY FOR STATE TECHNOLOGY

State Data Center Operations

SUMMARY

On July 1, 2014, the Agency for State Technology (AST) was established and the Northwood Shared Resource Center (NSRC) and the Southwood Shared Resource Center (SSRC) were transferred to the AST. This operational audit of the AST focused on evaluating selected information technology (IT) controls applicable to the State Data Center Operations. Our audit included a follow-up on related findings noted in our report Nos. 2013-182 for the NSRC and 2014-052 for the SSRC, as well as Finding No. 2014-021 noted for the NSRC in our report No. 2015-166. Our audit disclosed the following:

Finding 1: Administrative access privileges granted for some AST users and service accounts to selected mainframe, open systems, Windows server environments, and network domains did not promote an appropriate separation of duties and did not restrict users and service accounts to only those functions appropriate and necessary for assigned job duties or functions.

Finding 2: Some service accounts remained active when no longer needed and some service accounts inappropriately allowed interactive log-on increasing the risk that the confidentiality, integrity, and availability of AST data and IT resources may be compromised.

Finding 3: The AST did not perform quarterly reviews of user access privileges for the mainframe, open systems environments, and the network domains.

Finding 4: The inventory of IT resources at the State Data Center was not complete and, in some cases, was not accurate, increasing the risk that IT resources may not be appropriately monitored, tested, and evaluated to ensure the timely implementation of the latest security patches and other critical updates (e.g., service packs and hot fixes) from IT vendors.

Finding 5: Configuration management controls related to patch management for mainframe, network devices, and open systems environments continue to need improvement to ensure operating systems are appropriately secured and up-to-date.

Finding 6: Change management controls related to hardware and systems software changes continue to need improvement to ensure that only authorized, tested, and approved hardware and systems software changes are implemented into the production environment.

Finding 7: Contrary to State law,[1] four customer entities did not have signed service-level agreements (SLAs) with the State Data Center, increasing the risk that the effective, efficient, and secure operation of IT systems may be compromised for those customer entities.

Finding 8: Backup controls continue to need improvement to ensure that all IT resources that require back up are identified, backups are performed as required, and backups are periodically tested for recoverability.

[1] Section 282.201(2)(d), Florida Statutes.

Finding 9: State Data Center backup tape records were not up-to-date and some backup tapes could not be located and identified.

Finding 10: The State Data Center's business continuity and disaster recovery plans continue to need improvement to ensure that critical data center operations continue in the event of a disaster or other interruption of service.

Finding 11: The State Data Center's monitoring and reporting of the performance metrics of IT services provided to customer entities as defined in SLAs needs improvement to ensure that critical incidents effecting the performance of IT services are timely detected and, as applicable, resolved.

Finding 12: Certain State Data Center security controls related to user authentication, physical security, logging and monitoring, and protection of sensitive information, and vulnerability management for State Data Center IT resources need improvement to ensure the confidentiality, integrity, and availability of State Data Center customer entity data and related IT resources.

BACKGROUND

The Agency for State Technology (AST) was established on July 1, 2014, by the Legislature and the Executive Director of the AST is the State's Chief Information Officer. Pursuant to State law,[2] AST powers, duties, and functions include, among other things, developing and publishing information technology (IT) policy for the management of the State's IT resources, overseeing the State's essential technology projects, and managing the State Data Center. It was the Legislature's intent to create an entity that would provide utility data processing services to State agencies and to transfer the Northwood Shared Resource Center (NSRC) and Southwood Shared Resource Center (SSRC) into the State Data Center consisting of two physical locations, AST-North and AST-South.[3]

In March 2016, AST management became aware of mold and other environmental problems in the Northwood Centre where AST-North was located. Subsequently, proviso language in the 2016-17 General Appropriations Act[4] provided for the immediate relocation of the AST-North State Data Center and all of its staff, equipment, and operations by June 30, 2016; allowing only 3 months to plan and implement the move. As a result, AST consolidated the AST-North staff, equipment, and operations into the AST-South State Data Center facility as of June 30, 2016.

According to State law,[5] the State Data Center's duties are to:

- Offer, develop, and support services and applications defined in service-level agreements executed with its customer entities.
- Maintain performance of the data center by ensuring proper data backup, data backup recovery, disaster recovery, and appropriate security, power, cooling, fire suppression, and capacity.
- Develop and implement a business continuity plan and a disaster recovery plan, and beginning July 1, 2015, and annually thereafter, conduct a live exercise of the plan.

[2] Section 282.0051, Florida Statutes.

[3] Chapter 2014-221, Laws of Florida.

[4] Chapter 2016-66, Laws of Florida.

[5] Section 282.201, Florida Statutes.

- Enter into a service-level agreement with each customer entity to provide the required type and level of service or services.
- Be the custodian of resources and equipment located in and operated, supported, and managed by the State Data Center.
- Assume administrative access rights (privileges) to resources and equipment, including servers, network components, and other devices consolidated into the State Data Center.

As shown in ***EXHIBIT A*** to this report, as of March 28, 2016, the State Data Center provided IT services to 34 customer entities consisting of State agencies, municipal and county governments, a judicial branch entity, special districts, and other governmental entities as well as nonprofit entities that contract with the State Data Center for IT services. The State Data Center provides to its customer entities IT services covering a variety of services and computing environments, including data center facilities and operations, mainframe platforms, network platforms, open systems platforms, storage platforms, backup and recovery platforms, database platforms, Windows platforms, managed applications, and optional custom offerings.

FINDINGS AND RECOMMENDATIONS

Finding 1: Appropriateness of Access Privileges

Effective access controls include measures that restrict user access privileges to data and IT resources to only those functions that promote an appropriate separation of duties and are necessary for the user's assigned job duties. Additionally, State law[6] requires the AST to assume administrative access rights (privileges) to resources and equipment, including servers, network components, and other devices, consolidated into the State Data Center. State law[7] also required State agencies to relinquish administrative rights to consolidated resources and equipment. Further, AST *Open Systems UNIX Procedures* (*AST Procedures*) require that system service accounts be restricted from having administrative authority to a server. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure.

Our audit procedures disclosed the existence of some inappropriate and unnecessary administrative access privileges to consolidated resources and equipment for selected mainframe, open systems, and Windows server environments and the interconnected network domains. Specifically, we noted that:

- Contrary to State law,[8] administrative access privileges to mainframe environments were assigned to both AST staff and State agency staff. Specifically:
  - For the Access Control Facility 2 (ACF2) mainframe security environment applicable to one State agency's logical partition (LPAR),[9] 23 of the 31 active accounts with one or more administrative access privileges that included the ability to establish user accounts, create or

[6] Section 282.201(2)(f), Florida Statutes.

[7] Section 282.201(2)(f)1., Florida Statutes.

[8] Section 282.201(2)(f), Florida Statutes.

[9] A logical partition, commonly called an LPAR, is a subset of a computer's hardware resources, virtualized as a separate computer. In effect, a physical machine can be partitioned into multiple logical partitions, each hosting a separate organizational environment if desired.

modify access rules to programs and files, and read or update any field within the LPAR were, as of May 11, 2016, assigned to the State agency's staff.

- For the Resource Access Control Facility (RACF) mainframe security environment applicable to five LPARs, 8 of the 44 active accounts with one or more of the administrative access privileges that included the ability to specify logging options, full access to all RACF-protected resources, and full control over all RACF user profiles were, as of April 15, 2016, assigned to State agency staff.

- For 23 of the 218 open systems servers within the Red Hat Enterprise Linux environment, as of March 28, 2016, 10 of the 29 active accounts with administrative access privileges were assigned to customer entities and allowed administrative authority on the customer entities' assigned servers, contrary to State law. Additionally, 1 of the 29 active accounts was an AST system service account with administrative authority to a server. This administrative authority assigned to the system service account was unnecessary and contrary to *AST Procedures*.
- Eight of 11 selected customer entities retained administrative access privileges to their respective Windows server environments as of April 13, 2016, contrary to State law.
- As of March 28, 2016, access privileges for two AST network domains,[10] were not always appropriate. Specifically:
  - For one network domain, 7 active accounts with domain administrator access privileges were assigned to State agency staff, contrary to State law.
  - For another network domain, two State Data Center employees were assigned domain administrator access privileges that were inappropriate based on their assigned job duties and one State Data Center employee was assigned administrator access privileges to network devices that were inappropriate based on his assigned job duties.

Additionally, we noted that certain IT security controls related to access need improvement. To avoid the possibility of compromising State Data Center customer entity data and related IT resources, we are not disclosing in this report the specific details of what we found. However, we have notified appropriate AST management of the specific issues.

Inappropriate or unnecessary access privileges to mainframe, open systems, and Windows server environments and the interconnected network domains increase the risk of unauthorized modification, loss, or disclosure of data and IT resources.

Recommendation: To promote compliance with State law and an appropriate separation of duties, we recommend that AST management appropriately restrict access privileges to mainframe, open systems, and Windows server environments and the interconnected network domains to only those functions necessary for the users' and accounts' assigned job duties and functions.

Finding 2: Service Accounts

Effective IT controls restrict access to sensitive system resources, such as service accounts (i.e., nonuser system accounts). Effective IT controls restricting access to service accounts ensure that service accounts are enabled to perform automated system processes based on least functionality, service accounts are deactivated when no longer needed, and the access capability of service accounts is

[10] A domain is a form of a computer network in which all user accounts, computers, printers and other security principles, are registered with a central database located on one or more clusters of central computers known as domain controllers.

restricted to prevent inappropriately allowing interactive log-on (i.e., allowing the service account to be used to log on to the system as an individual). Appropriately restricting the use and access capabilities of service accounts helps protect the confidentiality, integrity, and availability of data and IT resources.

Our audit procedures disclosed that IT controls related to service accounts need improvement. Specifically, as shown in Table 1, our review of active service accounts for six AST network domains disclosed service accounts that remained active but were no longer needed, inappropriately allowed interactive log-on, or both.

Table 1
Active Service Accounts

Characteristic	Network Domain					
	1	2	3	4	5	6
Number of service accounts that were no longer needed	1	-	-	-	-	-
Number of service accounts that inappropriately allowed interactive log-on	1	1	5	27	7	7
Number of service accounts that were no longer needed and inappropriately allowed interactive log-on	-	-	-	11	1	3

Allowing service accounts to remain active when the accounts are no longer needed and allowing the accounts to inappropriately have the capability of interactive log-on increases the risk that the confidentiality, integrity, and availability of AST data and IT resources may be compromised.

Recommendation: We recommend that AST management improve controls to ensure that service accounts are appropriately deactivated when no longer needed and that the capability of interactive log-on using service accounts is appropriately deactivated.

Finding 3: Periodic Review of Access

Effective access controls include periodic reviews of user access privileges based on risk, access account change activity, and error rate. Such reviews help ensure that only authorized users have access and that the access provided to each user remains appropriate.

AST procedures[11] require a quarterly review of access privileges granted for all users including employees, contractors, and volunteers with access to the mainframe, distributed processing (open systems) environments, and the network domains. However, our audit procedures disclosed that AST staff had not conducted any quarterly reviews of user access privileges since the AST was established on July 1, 2014. As such, management's assurance that user access privileges were authorized and appropriate is limited. We noted a similar finding in our report No. 2014-052 applicable to the SSRC.

Recommendation: We recommend that AST management conduct periodic reviews of user access privileges for the mainframe, open systems environments, and the network domains in accordance with AST procedures and to ensure that user access privileges are authorized and appropriate.

[11] Procedure IS120.3.7, Access Monitoring.

Finding 4: Inventory of IT Resources

Effective IT inventory controls include the maintenance of a complete, accurate, and up-to-date inventory of IT systems (e.g., physical and virtual servers) to ensure that management is knowledgeable of all IT systems for which they are responsible and that the IT systems are configured as intended by management. Further, a complete, accurate, and up-to-date inventory is necessary for effective monitoring, testing, and evaluation of IT resources to ensure the timely implementation of the latest relevant security patches and other critical updates (e.g., service packs and hot fixes) from IT vendors.

The AST maintains an inventory of the State Data Center IT resources in a change management database (CMDB). Each inventory item is recorded as a configuration item (CI) in the CMDB. CIs include applications, databases, documents, network devices, storage items, applications, servers, and other IT infrastructure items. Additionally, a CI may contain information within the CMDB such as the operating system version, installed patches, system up-time, and maintenance notes.

Our audit procedures disclosed instances in which network devices, open systems servers, and databases were either not recorded as CIs in the CMDB or CIs contained incomplete or inaccurate information within the CMDB. Through our review, we determined that information was not recorded because the software agent used to communicate with the CMDB had not been installed on all the inventory items at the State Data Center. In response to our audit inquiry, AST management stated that they are actively working to install the software agent and correct inaccuracies on all inventory items that require tracking in the CMDB.

Maintaining a complete, accurate, and up-to-date inventory of all IT resources facilitates the monitoring, testing, and evaluation of IT resources to ensure the timely implementation of the latest relevant security patches and other critical updates from IT vendors. A similar finding was noted in our report No. 2013-182 applicable to the NSRC.

Recommendation: We recommend that AST management continue working to establish a complete, accurate, and up-to-date inventory of all State Data Center IT resources.

Finding 5: Configuration Management

Effective IT configuration management controls include patch management controls that ensure systems software is kept current by establishing effective procedures for patch management, virus protection, and other emerging threats. Patch management procedures help keep systems software current with the latest relevant security patches and critical software updates to ensure that systems software is not vulnerable to malicious code or other vulnerabilities resulting from emerging security threats or software flaws.

Our audit procedures disclosed that the AST had not established written patch management policies and procedures for the mainframe and network devices. Additionally, we tested 23 of the 218 Red Hat Enterprise Linux open systems servers to determine whether the server software was current and up-to-date as of March 28, 2016. For 20 of the 23 servers tested, we determined that the operating system software was not current and up-to-date. We noted a similar finding in our report No. 2013-182 applicable to the NSRC.

Without documented patch management procedures, IT resources may not be administered appropriately or effectively increasing the risk of unauthorized disclosure, modification, or loss of data and IT resources. Additionally, noncurrent and out-of-date operating system software increases the AST's vulnerability to malicious code or other emerging security threats or software flaws.

Recommendation: We recommend that AST management establish written policies and procedures for patch management for the mainframe and network devices and improve patch management controls for open systems servers to ensure that operating system software is current and up-to-date.

Finding 6: Change Management Controls

Effective change management controls over modifications to hardware and systems software ensure that only authorized, tested, and approved changes are implemented into the production environment. Further, the effectiveness of change management controls is enhanced through the maintenance of documentation supporting that hardware and systems software changes are appropriately tested and function as intended prior to being implemented into the production environment.

As part of our audit procedures, we reviewed 10 of 88 hardware and systems software change requests implemented during the period July 1, 2015, through April 6, 2016, to determine whether change requests were authorized, tested (as appropriate), and approved prior to being implemented into the production environment. We noted that for 1 of 4 hardware and systems software changes that required testing, AST records did not maintain documentation that the change was tested and functioned as intended prior to implementation into the production environment.

Effective change management controls ensure that all hardware and systems software changes are appropriately documented to evidence that changes are authorized, tested, and approved, and reduce the risk that erroneous or unauthorized hardware or systems software changes may be implemented into the production environment. A similar finding was noted in our report No. 2014-052 applicable to the SSRC.

Recommendation: We recommend that AST management improve change management controls to ensure that all hardware and systems software changes implemented into the production environment are appropriately documented.

Finding 7: Service-Level Agreements with Customer Entities

A service-level agreement (SLA) is a negotiated and signed agreement between two parties where one is the service provider and the other is the customer. State law[12] requires that the State Data Center enter into an SLA with each customer entity to define the required type and level of service or services to be provided by the State Data Center to the customer entity.

Our audit procedures disclosed that, as of March 28, 2016, the State Data Center was providing various IT services, such as server management and equipment hosting, to 34 customer entities. However, signed SLAs for 4 of the 34 customer entities did not exist. In response to our audit inquiry, AST

[12] Section 282.201(2)(d), Florida Statutes.

management stated they have been unable to obtain a signed SLA from 1 customer entity but were in the process of obtaining signed SLAs for the other 3 customer entities.

SLAs are necessary to, among other things, establish the services to be provided by the State Data Center, provide a billing methodology, and identify the roles and responsibilities of each party. Without SLAs, the AST cannot demonstrate compliance with State law and the effective, efficient, and secure operation of IT systems may be compromised. We noted a similar issue in our report No. 2014-052 applicable to the SSRC.

Recommendation: We recommend that AST management enter into mutually agreed-upon SLAs with all its customer entities as required by State law.

Finding 8: Backup Controls

State law[13] requires the State Data Center to ensure proper data backup and data recovery. Effective backup controls include written policies and procedures that provide guidance for an entity's backup process including the identification of IT resources requiring back up, the frequency of backups, and the periodic testing for recoverability to prevent or minimize the damage to automated operations that can occur from unexpected events. Furthermore, the State Data Center's SLAs with customer entities require the State Data Center to, at a minimum, perform incremental data backups daily and full data backups weekly.

Our review of backup procedures performed for 40 of the 2,387 production physical and virtual Windows and Red Hat Enterprise Linux open systems servers disclosed that AST backup controls need improvement. Specifically, we found that the State Data Center:

- Had not established written policies and procedures governing the backup processes, identifying all IT resources that require back up, and specifying the requirement for recoverability testing of backups.
- As of April 25, 2016, had not, backed up 7 of the 40 Windows and open systems servers we reviewed. Specifically, 3 Windows servers and 2 open systems servers had not been backed up because the servers were not included in the automated backup process. One Windows server had not been backed up since April 2, 2016, and one Windows server had not been backed up since April 8, 2016. A similar finding was noted in our report No. 2013-182 applicable to the NSRC.
- Did not periodically test backups to ensure recoverability.

Written policies and procedures governing the backup process help ensure that backups are performed as required to minimize the damage to automated operations from an unexpected event. Additionally, periodic recoverability testing of selected backups helps provide assurance that data is readily recoverable when needed in response to an unexpected event.

Recommendation: We recommend that AST Management establish policies and procedures governing the backup processes. Such policies and procedures should require that all IT resources requiring backup be identified, backups be timely performed, and backups be periodically tested for recoverability.

[13] Section 282.201(2)(b), Florida Statutes.

Finding 9: Backup Tapes

Effective backup controls include accurate records of the location and status of backup data which allow an entity to minimize the risk of data loss that may occur from unexpected events. Such actions maintain the entity's ability to restore data files that, if lost, may otherwise be impossible to recreate.

We reviewed the April 15, 2016, AST records for 6,554 backup tapes listed as located at an off-site storage facility to determine whether the tapes were recorded in the records of the off-site facility. Our audit procedures disclosed that 465 Windows and open systems tapes were listed on AST records as located at a particular off-site storage facility; however, the tapes were not recorded on the off-site storage facility's records. In response to audit inquiry, AST management stated that:

- 207 tapes had been destroyed due to tape expiration. However, our inspection of AST destruction records disclosed that evidence of destruction did not exist for 149 of the 207 tapes.
- 20 tapes were located at a different off-site storage facility.
- 151 tapes were located at the State Data Center; however, upon our inspection, 2 of 10 selected tapes could not be located.
- For 87 tapes, the location could not be determined as of July 6, 2016.

Inaccuracies in records for backup tapes may limit the State Data Center's ability to locate backup tapes and timely and completely recover information in the event of a loss of production data. We noted a similar finding in our report No. 2014-052 applicable to the SSRC.

Recommendation: We recommend that AST management improve backup controls to ensure the accuracy of AST backup tape location records and that all backup tapes can be appropriately identified.

Finding 10: Continuity of Operations and Disaster Recovery Planning

Continuity of operations and disaster recovery planning are intended to facilitate a timely and orderly resumption of critical operations in the event of a disaster or other interruption of service. State law[14] requires that disaster preparedness plans outline a comprehensive and effective program to ensure continuity of essential State functions under all circumstances. Additionally, State law[15] requires the State Data Center to develop and implement a business continuity of operations plan (COOP) and a disaster recovery (DR) plan and, beginning July 1, 2015, and annually thereafter, conduct a live exercise of each plan.

Our audit procedures disclosed that the State Data Center's COOP and DR planning need improvement. Specifically, we found that:

- While the State Data Center developed *Continuity of Operations Plan Operational Procedures* and had tested the notification components of the COOP, the AST had not tested the entire plan.
- A State Data Center DR plan had not been completed as of November 2, 2016.

[14] Section 252.365(3)(a), Florida Statutes.

[15] Section 282.201(2)(c), Florida Statutes.

Absent the development of a State Data Center DR plan and appropriate and timely COOP and DR plan testing, the risk is increased that critical State Data Center operations will not be timely and orderly resumed in the event of a disaster or other interruption of service. We noted a similar issue in our report No. 2013-182 applicable to the NSRC.

Recommendation: We recommend that, to ensure the recoverability of the State Data Center in the event of a disaster or other interruption of service, AST management develop and implement a State Data Center DR plan and annually conduct a live exercise of both the COOP and the DR plan as required by State law.

Finding 11: Performance Metrics

Effective IT performance management requires a monitoring process that includes defining relevant performance metrics and a systematic and timely reporting of performance in relation to the performance metrics. Additionally, State law[16] requires the State Data Center to establish in the SLAs with customer entities the metrics and processes by which the business standards for each service provided to the customer entities are to be objectively measured and reported.

Our audit procedures disclosed that the SLAs required Oracle database uptime to be a minimum of 99.5 percent of the scheduled availability for the respective database. As part of our audit procedures, we reviewed the performance metrics reported in the monitoring tool that measures Oracle database uptime for three selected customer entities for the month of January 2016. We found that the State Data Center did not meet its performance target for two of the selected customer entities (the Department of Children and Families and the Agency for Health Care Administration), as the Oracle database uptime was less than 99.5 percent of the scheduled availability. For the Department of Children and Families, the Oracle database uptime was not met for one database and for the Agency for Health Care Administration the uptime was not met for two Oracle databases. In response to our audit inquiry, AST management stated that they believe the performance uptime was met but, in these instances, the tool used to monitor the uptime did not accurately record the uptime.

We also noted that each customer entity's SLA defined the applicable performance metrics for mainframe services uptime. However, the State Data Center did not produce monthly performance metric reports for two customer entities as required in the SLAs. In addition, although the State Data Center met the monthly performance metrics and produced reports for one customer entity, the reports were not provided to the customer entity on a monthly basis as required in the SLA.

Effective IT performance monitoring, including relevant performance indicators and timely reporting to customers, is essential to the timely detection and resolution, as applicable, of critical incidents involving IT services.

Recommendation: We recommend that AST management ensure that State Data Center performance is properly measured and that the performance metrics outlined in the SLAs are consistently met. We also recommend that performance metrics reports are provided to each customer entity on a monthly basis.

[16] Section 282.201(2)(d)(5), Florida Statutes.

Finding 12: Security Controls – User Authentication, Physical Security, Logging and Monitoring, Protection of Sensitive Information, and Vulnerability Management

Security controls are intended to protect the confidentiality, integrity, and availability of data and related IT resources. Our audit procedures disclosed that certain security controls related to user authentication, physical security, logging and monitoring, protection of sensitive information, and vulnerability management need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising State Data Center customer entity data and related IT resources. However, we have notified appropriate AST management of the specific issues.

Without appropriate security controls related to user authentication, physical security, logging and monitoring, protection of sensitive information, and vulnerability management the risk is increased that the confidentiality, integrity, and availability of customer entity data and related IT resources may be compromised. A similar finding related to user authentication was communicated to NSRC management in connection with our report No. 2013-182 and SSRC management in connection with our report No. 2014-052.

Recommendation: We recommend that AST management improve certain security controls related to user authentication, physical security, logging and monitoring, protection of sensitive information, and vulnerability management to ensure the confidentiality, integrity, and availability of State Data Center customer entity data and related IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the AST had taken corrective actions for the applicable findings included in our report Nos. 2013-182 and 2014-052 that are applicable to the scope of the audit and Finding No. 2014-021 disclosed in our report No. 2015-166.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from March 2016 through June 2016 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected AST IT controls applicable to State Data Center operations during the period July 2015 through June 2016 and selected actions subsequent thereto. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other

guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.

- To determine whether management has corrected, or is in the process of correcting, all deficiencies disclosed in our report Nos. 2013-182 and 2014-052 that are applicable to the scope of the audit and whether management has corrected, or is in the process of correcting, Finding No. 2014-021 disclosed in our report No. 2015-166.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the State Data Center controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the State Data Center controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the State Data Center controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of State Data Center controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed AST personnel and obtained an understanding of the organizational structure, statutory requirements, key policies, procedures, and operational processes for the AST State Data Center operations.
- Obtained an understanding of the IT infrastructure and architecture of the State Data Center, including hardware, software, and operating systems for the various server platforms and network components, and database management systems.
- Evaluated the AST's compliance with selected statutory and contractual requirements including performance monitoring and customer incident response. Specifically, we reviewed:

- The AST State Data Center customer entity list as of March 28, 2016, to determine whether all 34 customer entities had executed a service level agreement (SLA) with the AST as required by Section 282.201(2)(d), Florida Statutes.
- The SLAs for 5 AST State Data Center customer entities as of March 28, 2016, to evaluate whether the agreement components specified in Section 282.201(2)(d), Florida Statutes, were included.
- The monthly uptime performance reports for Oracle database for 3 customer entities for the month of January 2016 to evaluate whether AST met its monthly performance metric.
- The monthly uptime performance reporting system for Windows Managed Servers.
- The monthly uptime performance reporting system for the mainframe environment.
- The incidence response time frames reported for eight priority 1 incidents for 5 customer entities during the period July 1, 2015, through April 6, 2016, to evaluate whether the AST met its performance targets.

- Evaluated the effectiveness of AST procedures for vulnerability management and testing of the State Data Center's network and interconnected systems.
- Evaluated the adequacy of the State Data Center's IT resource inventory tracking procedures.
- Evaluated whether the AST's data loss prevention procedures were sufficient for the identification, usage, and monitoring of confidential and sensitive information.
- Evaluated the effectiveness of the State Data Center's software and IT infrastructure component change control process including hardware and system software changes, firewall changes, and patch management. Specifically, we reviewed:
  - Ten of 88 closed, nonminor, and medium or high risk change requests during the period July 1, 2015, through April 6, 2016, to determine whether hardware and systems software changes were appropriately authorized, tested, functioned as intended, and approved.
  - Forty of the 2,995 production and nonproduction physical and virtual Windows servers to evaluate whether, as of March 28, 2016, the State Data Center had timely installed vendor-supplied patches.
  - Twenty-three of the 218 Red Hat Enterprise Linux production and nonproduction open systems servers to evaluate whether, as of March 28, 2016, the State Data Center had timely installed vendor-supplied patches.
  - The seven mainframe production LPARs to evaluate whether the State Data Center installed vendor-supplied patches timely as of April 26, 2016.
  - Three selected network high-risk devices to evaluate whether the State Data Center installed vendor-supplied patches timely as of April 28, 2016.
- Evaluated the effectiveness of the State Data Center logging and monitoring controls.
- Evaluated the effectiveness of the State Data Center's process for authorizing, terminating, and reviewing physical access to sensitive areas of the State Data Center. Specifically, we evaluated the 38 key cards with access to the State Data Center as of March 30, 2016.
- Determined whether the AST had developed continuity of operations and disaster recovery plans and whether the State Data Center had conducted a live exercise of each plan as required by Section 282.201(2)(c), Florida Statutes.
- Evaluated the effectiveness of the State Data Center's backup processes, including backup procedures and off-site storage.

- Examined the backup reports for 40 of 2,387 production physical and virtual Windows and Red Hat Enterprise Linux open systems servers as of April 25, 2016, to determine whether required backups were performed.
- Examined State Data Center records for 6,554 Windows servers and open systems backup tapes and 84 mainframe backup tapes listed as being stored at an off-site storage facility as of April 15, 2016, to determine the completeness and accuracy of the records.
- Evaluated the logical design, authorization, administration, and periodic review procedures for logical access privileges to State Data Center IT resources and customer entity data. Specifically, we reviewed:
    - The appropriateness of administrative access privileges for the 6 network domains used for State Data Center services and operations as of March 28, 2016.
    - The appropriateness of access privileges for the 44 RACF administrative accounts with selected high-risk access privileges for 5 mainframe LPARs as of April 15, 2016.
    - The appropriateness of access privileges for the 31 ACF2 administrative accounts with selected high-risk access privileges for 1 mainframe LPAR as of May 11, 2016.
    - The appropriateness of access privileges for the 29 administrative accounts for 23 selected open systems servers as of March 28, 2016.
    - The appropriateness of access privileges for the 69 administrative accounts for 1 selected network device as of April 22, 2016.
    - The appropriateness of access privileges for 11 selected customers to their respective Windows server environments as of April 13, 2016.
- Evaluated the effectiveness of the State Data Center's IT infrastructure user authentication controls. Specifically, we reviewed:
    - RACF user authentication controls for 5 mainframe LPARs as of April 6, 2016, April 12, 2016, and May 9, 2016.
    - ACF2 user authentication controls for 1 mainframe LPAR as of May 3, 2016, and May 11, 2016.
    - User authentication controls for 6 selected network domains as of March 28, 2016.
    - User authentication controls for 23 selected open systems servers as of April 8, 2016, and April 26, 2016.
    - User authentication controls for the 17 accounts within two network groups with administrative access to State Data Center network devices as of April 22, 2016, and May 2, 2016.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.



Sherrill F. Norman, CPA
Auditor General

EXHIBIT A

LIST OF STATE DATA CENTER CUSTOMER ENTITIES

AS OF MARCH 28, 2016

	Entity Name
1	Auditor General
2	Agency for Health Care Administration
3	Agency for Persons with Disabilities
4	Chautauqua Offices of Psychotherapy and Evaluation, Inc.
5	Children's Home Society of Florida
6	Department of Business and Professional Regulation
7	Department of Children and Families
8	Department of Citrus
9	Department of Corrections
10	Department of Economic Opportunity
11	Department of Education
12	Department of Elder Affairs
13	Department of Emergency Management
14	Department of Environmental Protection
15	Department of Health
16	Department of Highway Safety and Motor Vehicles
17	Department of Juvenile Justice
18	Department of Lottery
19	Department of Management Services
20	Department of Military Affairs
21	Department of Revenue
22	Department of State
23	Department of Transportation
24	Department of Veterans' Affairs
25	Executive Office of the Governor
26	Florida Commission on Human Relations
27	Florida Fish and Wildlife Conservation Commission
28	Greater Orlando Aviation Authority
29	Justice Administrative Commission
30	Miami-Date Expressway Authority
31	Northwest Florida Water Management District
32	Public Employee Relations Commission
33	Public Service Commission
34	Santa Rosa County

MANAGEMENT'S RESPONSE

Rick Scott, Governor

State of Florida
Agency for State Technology

4050 Esplanade Way, Suite 115
Tallahassee, FL 32399-0950
Tel: 850-412-6050

Jason M. Allison
State CIO/Executive Director

December 21, 2016

Sherrill F. Norman, CPA
Auditor General
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Pursuant to section 11.45(4)(d), Florida Statutes, attached is the Agency for State Technology's (AST) response to the preliminary and tentative audit findings and recommendations for the information technology operational audit of the *State Data Center Operations.*

AST would like to provide some additional background and context related to the creation of the State Data Center (SDC) and the emergency evacuation of the Northwood Shared Resource Center (NSRC) not included in your report.

The report mentions follow-up on findings from previous Auditor General report numbers 2013-182, 2014-052, and 2015-166. These reports were completed on former state entities, the NSRC and the Southwood Shared Resource Center (SSRC). Though these entities had similar functions as the current SDC within state government, they maintained entirely separate management structures and were overseen by two distinct and independent Boards of Trustees. In addition, both entities operated under their own unique policies and procedures. The assets of these entities were transferred to AST in July 2014.

Omitting these historical details implies that AST has repeat findings which is not the case. Although we recognize the value of the findings, it is important to note that AST has combined two separate data center entities into a new state agency with a single cohesive team. AST also continues to create and update uniform policies, procedures, and processes for the SDC.

Secondly, in March 2016, AST was directed to vacate the staff and all data center equipment out of the Northwood Centre by June 30, 2016 allowing AST only three months to plan and implement the move (originally forecasted to take up to two years).

AST staff relocated their offices and the data center computer room equipment, which included a mainframe and more than 2,050 servers, 1,000 terabytes of data, and hundreds of supporting backup and network devices, to the Southwood location (now the SDC) on time and under budget. Prior to moving, each asset had to be disassembled, cleaned and decontaminated. When arriving at the Southwood facility, the equipment was reassembled and further cleaned.

While the move was occurring, daily operations could not be interrupted. Regular workloads could not be delayed although the workload increased given the overhead associated with the move's daily and weekly communications through email, planning conference calls, and extensive face-to-face meetings with agency stakeholders.

AST appreciates the patience, time and energy put forth by your staff to improve the operations of state government, and with the above statements, provides responses to the findings and recommendations.

If you have any questions concerning AST's response, please contact Tabitha McNulty, Inspector General, at 850-412-6022.

Sincerely,



Jason M. Allison
State CIO/Executive Director

JA:tam

Attachment

cc: Curtis Unruh, Deputy Executive Director
Danielle Alvarez, Chief Information Security Officer
Eric Larson, Chief Operations Officer
Robert Thompson, Deputy Chief Operations Officer
Tabitha McNulty, Inspector General

Corrective Action Plan
For
Agency for State Technology State Data Center Operations

Finding #	1
Finding Title	**Appropriateness of Access Privileges**
Finding Statement	Administrative access privileges granted for some AST users and service accounts to selected mainframe, open systems, Windows server environments, and network domains did not promote an appropriate separation of duties and did not restrict users and service accounts to only those functions appropriate and necessary for assigned job duties or functions.
Recommendation	To promote compliance with State law and an appropriate separation of duties, we recommend that AST management appropriately restrict access privileges to mainframe, open systems, and Windows server environments and the interconnected network domains to only those functions necessary for the users' and accounts' assigned job duties and functions.
Program Response	AST agrees with the recommendation. AST has purchased a Privileged Identity Management (PIM) tool to enhance the appropriate administrative control of accounts for both AST and customer agencies. Once implemented, the security group will create a process to restrict access privileges to ensure appropriate separation of duties. AST platform* groups will review all accounts against the new process. The PIM solution implementation is expected to be completed by June 30, 2017; however, the customer implementation process will take longer. It should be noted that section 282.201(2)(f)2, Florida Statutes, requires AST to provide customers with access to applications, servers, network components, and other devices necessary to perform business activities and functions, and this may require administrative access privileges. * Reviewing mainframe accounts will subject customer applications to an extremely high level of risk. Each individual application will require testing and cannot be tested before implementing the dataset profile changes into the production environment. Each of the thousands of application dataset profiles will have to be changed and will require customer agency cooperation. The testing and changes will begin in January 2017, and are anticipated to be completed by October 31, 2017, provided customer agencies can actively participate in the remediation.
Audit Evidence	List of remediated accounts and the PIM implementation plan

Finding #	2
Finding Title	**Service Accounts**
Finding Statement	Some service accounts remained active when no longer needed and some service accounts inappropriately allowed interactive log-on increasing the risk that the confidentiality, integrity, and availability of AST data and IT resources may be compromised.
Recommendation	We recommend that AST management improve controls to ensure that service accounts are appropriately deactivated when no longer needed and that the capability of interactive log-on using service accounts is appropriately deactivated.
Program Response	AST agrees with the recommendation. The security group will update the policy and platform groups will update the procedures to improve their controls around service accounts. AST platform groups will review all service accounts against the new policy and ensure that they have the appropriate access level. Remediation is anticipated to be completed by December 31, 2017.
Audit Evidence	Approved policy and procedures in FASTdocs.

Finding #	3
Finding Title	**Periodic Review of Access**
Finding Statement	The AST did not perform quarterly reviews of user access privileges for the mainframe, open systems environments, and the network domains.
Recommendation	We recommend that AST management conduct periodic reviews of user access privileges for the mainframe, open systems environments, and the network domains in accordance with AST procedures and to ensure that user access privileges are authorized and appropriate.
Program Response	AST agrees with the recommendation. AST is currently creating an access review process that ensures the periodic review. Total implementation of this process is anticipated to be completed by December 2017.
Audit Evidence	Information Technology Service Management (ITSM) system tickets.

Finding #	4
Finding Title	**Inventory of IT Resources**
Finding Statement	The inventory of IT resources at the State Data Center was not complete and, in some cases, was not accurate, increasing the risk that IT resources may not be appropriately monitored, tested, and evaluated to ensure the timely implementation of the latest security patches and other critical updates (e.g., service packs and hot fixes) from IT vendors.
Recommendation	We recommend that AST management continue working to establish a complete, accurate, and up-to-date inventory of all State Data Center IT resources.
Program Response	AST agrees with the recommendation. However, to an extent, all configuration management databases (CMDB) are dynamic, and therefore, are never complete. AST acknowledges deficiencies within the audited

	CMDB. Further AST is reliant on customer to provide the metadata to populate the CMDB and presently AST does not have the authority to compel customer participation. Additionally, AST will clarify for the future, the scope of IT assets that are expected to be in the CMDB. Some of the issues noted in the finding are a result of: • customer refusal to allow AST to install inventory products to their legacy systems, • devices and systems cannot run the standard inventory products, requiring manual updates to the CMDB, and • the merger of the two separate data center entities into one. AST has hired a dedicated CMDB resource to manage the discrepancies within the CMDB and to insure that missing elements are present. This individual is tasked with taking action on known and reported inaccuracies.
Audit Evidence	Process improvements and workflows to improve CMDB accuracy.

Finding #	**5**
Finding Title	**Configuration Management**
Finding Statement	Configuration management controls related to patch management for mainframe, network devices, and open systems environments continue to need improvement to ensure operating systems are appropriately secured and up-to-date.
Recommendation	We recommend that AST management establish written policies and procedures for patch management for the mainframe and network devices and improve patch management controls for open systems servers to ensure that operating system software is current and up-to-date.
Program Response	AST agrees with the recommendation. The mainframe and network teams will establish written policies and procedures for patch management. These will be completed by June 30, 2017. Additionally, open systems is working with customers to remediate servers with the current operating system software.
Audit Evidence	Approved policies and procedures in FASTdocs and a list of remediated servers from tickets in the ITSM system.

Finding #	**6**
Finding Title	**Change Management Controls**
Finding Statement	Change management controls related to hardware and systems software changes continue to need improvement to ensure that only authorized, tested, and approved hardware and systems software changes are implemented into the production environment.
Recommendation	We recommend that AST management improve change management controls to ensure that all hardware and systems software changes implemented into the production environment are appropriately documented.

Program Response	AST acknowledges that a test plan could not be produced for this one change. However, AST has developed a rigorous change/release process including thorough documentation of processes and procedures. In the last 12 months, AST personnel have completed 3,026 change records and 6,244 release records providing the change summary, rollout/back out plans, change type, justification, affected configuration items and customers, risk and classification details, and outcome. All scheduled change/releases are immediately available to customers via the AST customer portal, and notifications are automatically emailed to customer groups upon scheduling and closure. Change/release records are thoroughly reviewed/approved prior to implementation. All changes, except emergencies, are reviewed by the AST change manager. Major changes are reviewed and approved by the Change Control Board. Releases are approved by the appropriate platform manager(s) and emergencies are also approved by the applicable bureau chief. Within the last year, AST staff have submitted 24 continual service improvement (CSI) recommendations to further refine the agency's change/release process which includes items to ensure that testing is planned, performed, and documented. CSI implementations have resulted in improved change/release transparency to customers, additional review and functionality via the ITSM system mobile app, notification enhancements, and increased monitoring for timely notification and closure. The AST change/release managers have performed 304 formal post implementation reviews (PIR) within the last 12 months. Reviews are completed on all changes classified as major or emergency, all changes resulting in an incident, and all unsuccessful changes (partially implemented/backed out). The PIRs are reviewed in the weekly Change Control Board meetings. AST will communicate the necessity to record the test plan associated to the changes.
Audit Evidence	Change and release records with testing plans.

Finding #	**7**
Finding Title	**Service-Level Agreements with Customer Entities**
Finding Statement	Contrary to State law, four customer entities did not have signed service-level agreements (SLAs) with the State Data Center, increasing the risk that the effective, efficient, and secure operation of IT systems may be compromised for those customer entities.
Recommendation	We recommend that AST management enter into mutually agreed-upon SLAs with all its customer entities as required by State law.

Program Response	AST agrees with the recommendation and acknowledges that four customer agencies (Department of Highway Safety and Motor Vehicles, Department of Transportation, Florida Commission on Human Relations, and Greater Orlando Aviation Authority) do not have signed service level agreements (SLAs). However, AST cannot force customer agencies to sign and there are no repercussions for customer who do not sign an SLA. For each of the customers noted in the audit who have no signed SLA, the customer agencies have not furnished AST with an approved SLA. AST continues to follow-up with emails, phone calls, and hold customer meetings to assist with finalizing the SLAs. However, as services are still rendered and the customers are paying their bills, AST is honoring the last signed SLA as "current" to keep customers' systems operational. AST will continue to work with customers to finalize SLAs. This language for such a change has been proposed for the upcoming 2017 Legislative Session.
Audit Evidence	Signed SLAs with agencies.

Finding #	**8**
Finding Title	**Backup Controls**
Finding Statement	Backup controls continue to need improvement to ensure that all IT resources that require back up are identified, backups are performed as required, and backups are periodically tested for recoverability.
Recommendation	We recommend that AST Management establish policies and procedures governing the backup processes. Such policies and procedures should require that all IT resources requiring backup be identified, backups be timely performed, and backups be periodically tested for recoverability.
Program Response	AST agrees with the recommendation. The Backup and Recovery Section has developed policies governing backup procedures and standards. These documents provide the processes in which the AST Backup and Recovery Section protects systems and how every backup client is notated with its current status. The notation is directly related to AST's ticketing system and CMDB. This allows the section to quickly compare a client's notated status and verify if they should be in any automated backup policies. In addition, the Backup and Recovery Section conducts routine customer-wide audits and presents the results of the audit to the customer for review, approval, and sign-off. Daily backup result reports are also delivered to each customer via email. AST expects to supplement this email reporting by integrating server level backup data directly into customers' ITSM system portal for additional customer insight and analysis. This is expected to be completed by March 30, 2017. It should be noted that the Backup and Recovery Section completes restores from backups routinely and on a daily basis. Successful restorations ensure that the backup system and recovery process are working as designed. However, to address the audit finding, AST will additionally ensure that each customer is represented with a restore request at least annually.

Audit Evidence	Approved policies and procedures in FASTdocs; evidential restore requests from all agencies at least annually from ITSM system.

Finding #	**9**
Finding Title	**Backup Tapes**
Finding Statement	State Data Center backup tape records were not up-to-date and some backup tapes could not be located and identified.
Recommendation	We recommend that AST management improve backup controls to ensure the accuracy of AST backup tape location records and that all backup tapes can be appropriately identified.
Program Response	AST agrees with the recommendation; however, during the time of this review, AST was in the process of changing offsite tape storage vendors, moving the Northwood Shared Resource Center, and updating three different tape tracking systems. Responsibility for tape media management belongs to both the Backup and Recovery Section and the tape librarians. The Backup and Recovery Section is responsible for writing the data to the tapes, and the librarians ship and receive the tapes to the offsite storage vendor and record when tapes are destroyed. With the expedited data center move and tape storage vendor transition complete, a complete inventory of tapes has been completed and the tape tracking software is up to date. Additionally, the following actions are being implemented to ensure accurate records are kept: • Controls are being put in place to ensure the tape tracking system is fully operational and remains working through monitoring and routine maintenance. The system is identical to the offsite storage vendor's system and the two systems automatically sync - allowing events in either system to be updated to the peer. This notifies the vendor that tapes are being shipped and allows AST to verify when the tapes arrive and vice-versa. • Destruction of backup tapes will be captured in the AST ITSM system through the issuance of a ticket and the tape tracking software will also be updated. • Lastly, the Backup and Recovery Section is working to move all tape backup write and restore operations to the offsite storage vendor's location, eliminating some of the overhead associated with tape shipment.
Audit Evidence	Tickets from the ITSM system of tape request and destruction; documentation of tape destruction; review of tape management software

Finding #	10
Finding Title	**Continuity of Operations and Disaster Recovery Planning**
Finding Statement	The State Data Center's business continuity and disaster recovery plans continue to need improvement to ensure that critical data center operations continue in the event of a disaster or other interruption of service.
Recommendation	We recommend that, to ensure the recoverability of the State Data Center in the event of a disaster or other interruption of service, AST management develop and implement a State Data Center DR plan and annually conduct a live exercise of both the COOP and the DR plan as required by State law.
Program Response	AST agrees the recommendation. The Disaster Recovery Section is in the process of finalizing AST's disaster recovery (DR) plan for approval. The plan outlines the services necessary for AST to provide continuing operations to its customers. The AST DR plan will be finalized by June 30, 2017, though effecting that plan will be dependent on the technical DR foundation and infrastructure currently being developed. At the same time, the Continuity of Operations (COOP) Coordinator is updating the COOP plan with current information. Once both plans are completed and approved, AST will conduct live exercises annually as required by State law, contingent upon continued funding. It should be noted that AST's in progress activities to construct the new infrastructure will provide the foundation and a base level of DR for all customers as long as they are hosted within our shared enterprise environment.
Audit Evidence	Approved DR and COOP plans and evidence of live exercise results.

Finding #	11
Finding Title	**Performance Metrics**
Finding Statement	The State Data Center's monitoring and reporting of the performance metrics of IT services provided to customer entities as defined in SLAs needs improvement to ensure that critical incidents effecting the performance of IT services are timely detected and, as applicable, resolved.
Recommendation	We recommend that AST management ensure that State Data Center performance is properly measured and that the performance metrics outlined in the SLAs are consistently met. We also recommend that performance metrics reports are provided to each customer entity on a monthly basis.
Program Response	AST agrees with the recommendation. While the majority of AST services have automated performance metrics to assess availability, some services lack metrics or the metrics are produced through manual processes. AST recently appointed an Availability Manager who has met with all platforms sections to gather information related to availability monitoring and reporting. AST is currently re-validating or documenting the availability requirements for each platform including how availability targets are calculated, the monitoring tools used, and the monitoring schedules.

	The goal is to add availability data to the ITSM system either through direct entry or automated data imports and provide availability to customers via monitoring dashboards that display the success/failure rates for all performance metrics. Planned implementation is for July 1, 2017.
Audit Evidence	Documented performance metric availability targets, calculation methods, monitoring tools, and schedules for all services; availability data to satisfy SLA requirements posted to the ITSM system for agency access at any time.

Finding #	**12**
Finding Title	**Security Controls – User Authentication, Physical Security, Logging and Monitoring, Protection of Sensitive Information, and Vulnerability Management**
Finding Statement	Certain State Data Center security controls related to user authentication, physical security, logging and monitoring, and protection of sensitive information, and vulnerability management for State Data Center IT resources need improvement to ensure the confidentiality, integrity, and availability of State Data Center customer entity data and related IT resources.
Recommendation	We recommend that AST management improve certain security controls related to user authentication, physical security, logging and monitoring, protection of sensitive information, and vulnerability management to ensure the confidentiality, integrity, and availability of State Data Center customer entity data and related IT resources.
Program Response	AST agrees with the recommendation. AST will continue to work on implementing the necessary controls to correct the issues in the above-mentioned areas.