



**State of Florida
Agency for State Technology**


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

Rick Scott, Governor

Eric M. Larson
State CIO/Executive Director

MEMORANDUM

TO: Eric M. Larson, State Chief Information Officer/Executive Director
Eric Miller, Chief Inspector General, Executive Office of the Governor

FROM: Tabitha A. McNulty, Inspector General 

DATE: July 5, 2017

SUBJECT: Six-Month Follow-up Status to the State of Florida Auditor General Report Number 2017-087, *Agency for State Technology, State Data Center Operations*

Pursuant to section 20.055, Florida Statutes, attached is the six-month status of findings and recommendations included in the Auditor General Report Number 2017-087, *Agency for State Technology, State Data Center Operations*, published January 5, 2017.

The review found that sufficient corrective action has been undertaken to close four findings. The agency is making progress on the remaining findings and their associated long-term resolution efforts. The updates and status of the corrective actions are provided in the attached report under the sections Current Agency Status and Office of Inspector General (OIG) Assessment. The OIG will continue to follow-up on the open recommendations.

If further information is needed, please contact me at 850-412-6022.

TAM

Attachment

cc: Kathy DuBose, Coordinator
Joint Legislative Audit Committee (JLAC)
Sherrill F. Norman, CPA
State of Florida Auditor General
Robert Thompson, Chief Operations Officer
Curtis Unruh, Deputy Chief Operations Officer



Agency for State Technology Office of Inspector General

Eric M. Larson, State CIO/
Executive Director

Tabitha A. McNulty
Inspector General



Six-Month Follow-up Response to *Agency for State Technology, State Data Center Operations* Auditor General Report Number 2017-087 Internal Audit Project # A-1617-32

Overview

Section 20.055, Florida Statutes, requires the Inspector General to monitor and report to the Executive Director and the Chief Inspector General on the status of corrective action taken in response to reports issued by the Auditor General. In January 2017, the Auditor General published Report Number 2017-087, *Agency for State Technology, State Data Center Operations*. This audit focused on evaluating selected information technology controls applicable to the operations of the State Data Center (SDC) during the period July 2015 through June 2016.

Status Report

Finding Number: 1 Appropriateness of Access Privileges

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.

Original Report Response (December 2016): 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

Current Agency Status:

Privileged Identity Management (PIM) Deployment: The PIM pilot project to enhance the administrative controls of accounts based upon Least Privilege is in progress and on schedule. The design has been completed and the pilot was completed on June 16, 2017. The pilot validated the design on selected AST servers in the production environment and provided the framework for an expanded rollout. The next PIM project is scheduled to begin on July 1, which will continue to scale the solution to AST before bringing in SDC customers.

Security: The Security Group has finalized the policy surrounding service account provisioning (AST-ISO-P-0002) and has started the process to update the authentication procedures. The update is a result of the deployment of the new PIM tool and will include segregation of duties. The new policy should be completed by July 30, 2017.

Mainframe: On June 6, 2017, the user attribute "SYSTEM SPECIAL" was removed from the logical partitions (LPARS) for one customer noted within the Resource Access Control Facility (RACF). This change removed the customer staff's ability to have full control over the RACF-protected resources. The Cherwell Change number was 12756 and the Release number was 22778. The Mainframe group continues to work with the second customer using RACF to remove this feature from their employees. Additionally, Mainframe continues to meet with the customer on the Access Control Facility 2 (ACF2) to develop an implementation plan to correct the noted issues in the report. Mainframe expects to meet the original October 31, 2017, deadline set in the January response.

Office of Inspector General Assessment:

The Office of Inspector (OIG) agrees with the status of the recommendation and determines that the finding:

- will remain open and the OIG will follow-up in six months.
- is partially complete and will remain open. The OIG will follow-up in six months.
- is complete and the OIG will no longer follow-up on this.
- is not complete, but recommends that management accept any residual risk.

Finding Number: 2 Service Accounts

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

Original Report Response (December 2016): 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

Current Agency Status: AST has improved a number of controls surrounding privileged accounts in response to this finding.

The Security Group issued Policy AST-ISO-P-0002 that provides a policy definition for service accounts. In addition, the Windows Bureau has written their procedure AST-BWS-P-0005, *Service Account Configuration*, to enact the policy.

Additionally, AST has implemented an automated script for AST domains to enumerate all administrative and non-expired accounts. The results are provided to a Distribution List for review and tickets opened for any accounts that need remediation.

To prohibit anonymous logins, Active Directory Group Policy has been implemented to remove interactive login by Service Accounts.

As the PIM tool is expanded, it will log and provide reports on interactive account usage and activity. The PIM tool's reporting services can be utilized to identify non-essential or inactive accounts for removal and/or deactivation. During the PIM project, Platform groups will further review Service Accounts and validate that appropriate access levels are in place.

Office of Inspector General Assessment:

The policies and procedures noted above have been uploaded to FASTdocs. Additionally, Windows provided the Active Directory settings showing that service accounts are denied interactive logon and terminal service logon. The OIG agrees with the status of the recommendation and determines that the finding:

- will remain open and the OIG will follow-up in six months.
- is partially complete and will remain open. The OIG will follow-up in six months.
- is complete and the OIG will no longer follow-up on this.
- is not complete, but recommends that management accept any residual risk.

Finding Number: 3 Periodic Review of Access

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.

Original Report Response (December 2016): 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

Current Agency Status: Prior to the completion of the PIM project, remediation has been made in proportion to risk using available tools and manual review processes. There currently is an automated script running for the AST Active Directory domains for review of all administrative accounts. Windows has also created a script to run for Network to review their administrative accounts. The script results are provided to a Distribution List for review and tickets opened for any accounts that need remediation.

As the PIM project continues, AST User Accounts are placed within functional groups to control server and other resource access. The continued implementation of the PIM reporting tool will facilitate the ability to perform automated reviews of access privileges.

Open Systems is working to use Ansible/Puppet to automate user changes across the multiple systems. In the interim, Open Systems has run a custom script to inspect accounts and has reviewed the results for any accounts that need remediated.

Lastly, the Mainframe Platform Manager now conducts a manual quarterly inspection of each employee's access as a part of their routine responsibilities. Mainframe will continue this process even after the implementation of the PIM tool.

Defining the access review process that documents and ensures this periodic review, as well as a risk acceptance process that provides a process for AST and customers to document known risks and compensating controls for risk mitigation is expected by December 2017.

Office of Inspector General Assessment:

The OIG finds that the current measures in place to review access are in place and platforms have done reviews of access. However, with the PIM reporting tool will help facilitate reviews and procedures for the PIM tool not being complete, the OIG agrees with the status of the recommendation and determines that the finding:

- will remain open and the OIG will follow-up in six months.
- is partially complete and will remain open. The OIG will follow-up in six months.
- is complete and the OIG will no longer follow-up on this.
- is not complete, but recommends that management accept any residual risk.

Finding Number: 4 Inventory of IT Resources

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

Original Report Response (December 2016): 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 customers 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 ensure 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

Current Agency Status: AST has implemented a formal Configuration Item (CI) discrepancy reporting process within the CMS. The new process prompts for specific information related to the configuration item being added or modified and links the discrepancy to the configuration item. (See the CF007 – CI Discrepancy Process Work Detail document for more information.) In addition, a server decommission

process is currently being tested with an external agency prior to full rollout to customers. The server decommission process includes automatic task generation to the various teams including a task to the CMDB team to retire the server. A similar server build process is currently in the planning phase.

Example CI Discrepancy

AST also implemented a formal auditing process as detailed in the *IA005 – Audit Creation Work Detail* document. The auditing system within the Configuration Management System has been customized to complete CMDB audits. A CMDB Auditing dashboard has been built specifically to monitor and complete routine audits of configuration items. As items are reviewed within the dashboard and set to “audit complete,” they are linked to the primary audit record. A next audit due date is auto-generated for the configuration item. A draft *CF006 - Configuration Management Audit Procedures* document is currently being finalized.

Example – Audit Ticket

Oracle databases, network devices, and storage devices have been reconciled with the appropriate teams by the configuration manager. AST is currently coordinating with the SQL team to automate the entry of SQL database configuration items and/or the associated attributes from the Solarwinds

monitoring tool. AST has initiated a formal project to design a process to synchronize data within the CMDB and AST data center tool, dcTrack.

As a part of the FY2017/18 Service Catalog effort, Service Level Agreement (SLA) language has been updated to document the customer's responsibility to maintain certain metadata within the CMDB. Specifically, the language states:

CUSTOMER MAINTENANCE OF SYSTEM METADATA.

In an effort to manage Customers' critical applications effectively, the Service Provider [AST] requires the Customer to complete and maintain certain system metadata within the Service Provider's CMDB through the Customer Portal. The metadata attributes include, but are not limited to, system name, purpose, application dependencies, business function and criticality, security and compliance requirements, data classification, primary user(s), and other contextual information to help the Service Provider to better address service issues. Specific CMDB fields required to be accurately maintained will be clearly indicated for editing in the Customer Portal and must be reviewed and updated at least bi-annually. If the agency metadata is not current or is absent, the Service Provider will not record the service interruption within the Service Provider's metrics to the extent the metadata was required to appropriately respond to the incident.

Office of Inspector General Assessment:

The Inspector General agrees that the CMDB is dynamic and will never be 100% accurate as changes are made daily. However, as stated in the original response, AST has defined the configuration item types that will be included within the CMDB. The list of these items may be found in document CF005 – *AST ITSM Configuration Management System Architecture*. Additionally, as noted in the updated response ITSM has made several process changes to review and audit the issues within the CMDB.

Therefore, the OIG agrees with the status of the recommendation and determines that the finding:

- will remain open and the OIG will follow-up in six months.
- is partially complete and will remain open. The OIG will follow-up in six months.
- is complete and the OIG will no longer follow-up on this.
- is not complete, but recommends that management accept any residual risk.

Finding Number: 5 Configuration Management

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.

Original Report Response (December 2016): 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 are 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

Current Agency Status:

Network – The Network Patch Management policy, AST-BCOS-POL-0005, was published to FASTdocs on May 25, 2017.

Mainframe – The Mainframe Software Maintenance Policy, AST-BCES-P-0001, was published to FASTdocs on June 23, 2017.

Open Systems – Continues to improve their patch management controls and work with customers that do not have established patch windows to remediate servers. Open Systems has remediated seven servers to their operating systems latest patch.

Additional processes are also being developed that will document risk acceptance by AST and/or customers for issues and risks created by installing unapplied patches, including any compensating controls implemented for risk mitigation due to these circumstances by December 2017.

Office of Inspector General Assessment:

The OIG has noted that the Network and Mainframe patch policies were uploaded to FASTdocs and will not follow-up on those items in the future. However, the OIG will continue to follow-up on the remediation of servers within Open System. The OIG agrees with the status of the recommendation and determines that the finding:

- will remain open and the OIG will follow-up in six months.
- is partially complete and will remain open. The OIG will follow-up in six months.
- is complete and the OIG will no longer follow-up on this.
- is not complete, but recommends that management accept any residual risk.

Finding Number: 6 Change Management Controls

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.

Original Report Response (December 2016): 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.

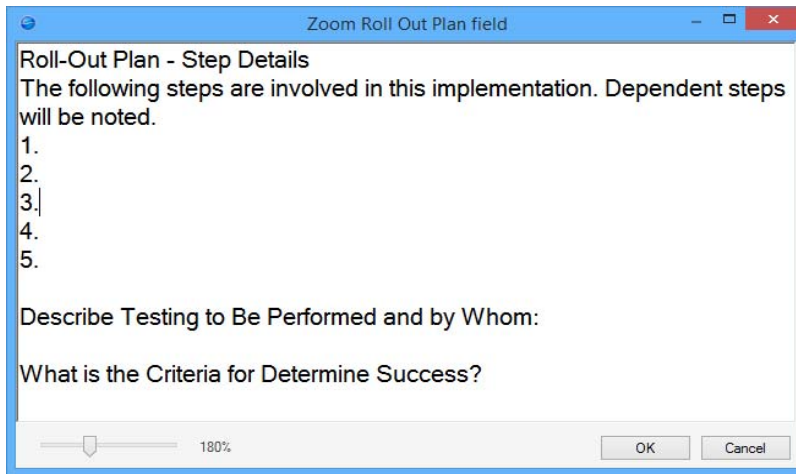
The AST change/release managers have performed 304 formal post implementation reviews (PIR) within the last 12 months. Reviews are completed on all changes classified as major or emergency, all changes resulting in an incident, and all unsuccessful changes (partially implemented/backed out). The PIRs 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

Current Agency Status: The AST release form has been modified in the test environment to include specific instructions related to the roll-out process documentation. The roll-out plan field is pre-populated with rollout steps, a description of testing to be performed and by whom, and success criteria. The purpose is to provide guidance to technicians to ensure inclusion of testing parameters within the roll-out plan. The release closure notification to customers has been modified to include a request that testing be performed and to notify the AST Service Desk if testing is unsuccessful.

Example of Roll-out Plan Section



Office of Inspector General Assessment:

Release 22024 is scheduled to be released the second week of July and will implement the Roll-Out Step plan update. Therefore, the OIG agrees with the status of the recommendation and determines that the finding:

- will remain open and the OIG will follow-up in six months.
- is partially complete and will remain open. The OIG will follow-up in six months.
- is complete and the OIG will no longer follow-up on this.
- is not complete, but recommends that management accept any residual risk.

Finding Number: 7 Service Level Agreements with Customer Entities

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.

Original Report Response (December 2016): 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

Current Agency Status: As of the date of this report all customers have signed service level agreements.

Office of Inspector General Assessment:

Customers that required either a new or renewal to their SLA have signed. However, both DOT and HSMV have signed a Memorandum of Understanding that extends their last SLA that was at the time expired. The AST continues to work with both DOT and HSMV to execute a new SLA. The OIG agrees with the status of the recommendation and determines that the finding:

- will remain open and the OIG will follow-up in six months.
- is partially complete and will remain open. The OIG will follow-up in six months.
- is complete and the OIG will no longer follow-up on this.
- is not complete, but recommends that management accept any residual risk.

Finding Number: 8 Backup Controls

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.

Original Report Response (December 2016): 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

Current Agency Status: The Backup and Recovery Section established procedures to audit and test the backup and recovery of data.

AST has compiled and presented nine out of 29 customer audits. Eight customers have completed their review and approved the audits and one customer is pending. Additionally, three customers are in process and the remaining customers are pending scheduling of their annual audit. The audit process is labor intensive and will continue through a rolling progression.

AST Backup and Recovery also developed a standard process to test data recovery for each customer. The process includes requesting a single file be restored for a single customer system. The first of these individual tickets were created on April 4, 2017, and all customers have subsequently been completed successfully.

AST has also integrated the Backup and Recovery data into the customer portal that will allow customers to review individual servers to determine if their backup was success or not.

Office of Inspector General Assessment:

Backup and Recovery procedure AST-BCOS-I-0008 *Audit Process Documentation*, was uploaded to FASTdocs on June 28, 2017. The Backup and Recover Section also provided a list of customer tickets for the annual restore test that was conducted during March and April of 2017. The OIG was also provided a test account to a customer's ITSM system portal and reviewed that the backup availability information was added. The OIG also confirmed that this information is available in the CMDB.

The OIG agrees with the status of the recommendation and determines that the finding:

- will remain open and the OIG will follow-up in six months.
- is partially complete and will remain open. The OIG will follow-up in six months.
- is complete and the OIG will no longer follow-up on this.
- is not complete, but recommends that management accept any residual risk.

Finding Number: 9 Backup Tapes

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.

Original Report Response (December 2016): 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

Current Agency Status: The Backup and Recovery Section have worked with the offsite storage vendor to ensure the tape tracking system that is in place is in sync and remains in sync. When it is found to be out a sync, a ticket is generated with the tape track system manufacturer and/or the offsite storage vendor to resolve the issue. Backup and Recovery Section have also developed a procedure to work with the tape librarians to document media destruction and the policy and procedure (AST-BCOS-P-0003 and AST-BCOS-P-0004) can be found on the AST FASTdocs site. These procedures detail the steps taken by the Backup and Recovery Section when requesting media be destroyed.

Office of Inspector General Assessment:

The policy and procedure mentioned in the current agency status were uploaded to FASTdocs on May 2, 2017. The Section also provided a list of ITSM system tape requests for destruction and emails of issues with the tape tracking system. The movement of the tape backup write and restore process has not happened, however the Bureau Chief expects the tape libraries to move in July and then the offsite storage vendor should begin the process of writing the tapes.

The OIG agrees with the status of the recommendation and determines that the finding:

- will remain open and the OIG will follow-up in six months.
- is partially complete and will remain open. The OIG will follow-up in six months.
- is complete and the OIG will no longer follow-up on this.
- is not complete, but recommends that management accept any residual risk.

Finding Number: 10 Continuity of Operations and Disaster Recovery Planning

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.

Original Report Response (December 2016): 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

Current Agency Status:

COOP – AST's Continuity of Operations Plan (COOP) document was submitted on schedule to the Division of Emergency Management (DEM) on March 31, 2017. A live COOP test occurred on June 7, 2017, and exercised, among other things, out-of-band notification and alerting, and the ability of staff to work remotely. The test provided valuable information to improve the plan and next test.

Disaster Recovery – The AST Disaster Recovery (DR) plan, FASTdocs document AST-BCOS-P-0005, was finalized and tested between June 19-23, 2017. The test was successful and all applications targeted were restored during the test.

Office of Inspector General Assessment:

The OIG finds that the AST currently has both a DR plan and a COOP plan. Both plans were tested during the month of June successfully. Therefore, the OIG agrees with the status of the recommendation and determines that the finding:

- will remain open and the OIG will follow-up in six months.
- is partially complete and will remain open. The OIG will follow-up in six months.
- is complete and the OIG will no longer follow-up on this.
- is not complete, but recommends that management accept any residual risk.

Finding Number: 11 Performance Metrics

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.

Original Report Response (December 2016): 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.

Current Agency Status: A monthly availability reporting mechanism has been established in the agency's Configuration Management System (CMS) to report availability metrics for Network, Oracle Databases, Mainframe, Open Systems Managed Server, Windows Managed Server, and Backup and Recovery. The Cherwell team is currently working on completing the availability reporting mechanism for Network Load Balancing, SQL Database, and Facility-Scheduling, along with the three new services that will be offered on July 1.

Example of Performance Metrics

Mainframe Monthly Availability Sheet 4/2017

Report Date: 4/30/2017 4/2017

Enter the monthly availability percentage for each application. This sheet is visible to customers on the Availability Dashboard. Records that do not match a customer's agency are not displayed.

Created By: Stacy Newsome
Created On: 5/18/2017 5:33 AM
Last Modified By:
Last Mod By Date:

Application	Comments
DOT CICS Processing: 0.00 02 z/OS Processing: 0.00 05 Storage: 0.00 08 DB2 Processing: 0.00 10	
HSMV CICS Processing: 0.00 01 z/OS Processing: 0.00 04 Storage: 0.00 07	
FDC CICS Processing: 0.00 03 z/OS Processing: 0.00 06 Storage: 0.00 09 DB2 Processing: 0.00 11	
FSFN (DCF) DB2 Processing: 0.00 12 z/OS Processing: 0.00 13 Storage: 0.00 14	
FLORIDA (DCF) DB2 Processing: 0.00 15 IMS: 0.00 16 z/OS Processing: 0.00 17 Storage: 0.00 18	

As availability records are included in the CMS, a customer dashboard with drill-down capability is updated to include monthly availability records and trending charts.

Availability Overview Example

Availability Overview

Date Range: Within last 6 months

Server Availability

Server Name	Month	Year	Availability Percentage	Comments
█	November	2016	100.00	
█	December	2016	100.00	
█	November	2016	100.00	
█	December	2016	99.99	
█	November	2016	100.00	
█	December	2016	100.00	

Server Availability Trending

Network Availability

Agency	Month	Year	Avail. Percentage	Comments
AST	April	2017	99.99	
AST	April	2017	99.99	
AST	April	2017	99.99	
AST	April	2017	100.00	
AST	April	2017	99.99	
AST	April	2017	99.99	
AST	April	2017	99.99	
AST	April	2017	99.91	

Network Availability Trending

Oracle Database Availability

Name	Month	Year	Availability Percentage	Comments
█	April	2017	100.00	
█	April	2017	100.00	
█	April	2017	100.00	
█	April	2017	100.00	
█	April	2017	100.00	
█	April	2017	100.00	

Oracle Availability Trending

Mainframe Availability

Month	Y.	FSFN DB2 P.	FSFN z/OS P.	FSFN Stor.	FSFN Comments
April	2017	0.00	0.00	0.00	
March	2017	99.59	99.59	99.59	
February	2017	100.00	100.00	100.00	
January	2017	100.00	100.00	100.00	
December	2016	100.00	100.00	100.00	
November	2016	0.00	0.00	0.00	

Mainframe Availability Trending

Office of Inspector General Assessment:

Interviews with ITSM staff stated that this project is approximately 80 percent complete. The original date of July 1, 2017, will not be met, but they expect it to be completed within the next several weeks following the issuance of this report. The OIG agrees with the status of the recommendation and determines that the finding:

- will remain open and the OIG will follow-up in six months.
- is partially complete and will remain open. The OIG will follow-up in six months.
- is complete and the OIG will no longer follow-up on this.
- is not complete, but recommends that management accept any residual risk.

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

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.

Original Report Response (December 2016): AST agrees with the recommendation. AST will continue to work on implementing the necessary controls to correct the issues in the above-mentioned areas.

Current Agency Status: AST continues to work on correcting the issues with User Authentication, Logging and Monitoring and Vulnerability Management. AST had corrected the issue noted with Physical Security during the Auditor General's field work and implemented a new system since then. Lastly, AST issued a policy for the Protection of Sensitive Information, AST-ED-P-0038.

Office of Inspector General Assessment:

The OIG found that the correction of the physical security controls at the SDC were corrected immediately after the issue was found by the staff of the Auditor General. This issue was corrected months before the issuance of the audit report. In regards to the Protection of Sensitive Information, AST-ED-P-0038, Protection of Confidential and Sensitive Information Process Definition, was uploaded to released December of 2016 and uploaded to FASTdocs March 24, 2017. The OIG agrees with the status of the recommendation and determines that the finding:

- will remain open and the OIG will follow-up in six months.
- is partially complete and will remain open. The OIG will follow-up in six months.
- is complete and the OIG will no longer follow-up on this.

is not complete, but recommends that management accept any residual risk.

Objective, Scope, and Methodology

The objective of this follow-up report was to determine the status of action taken by agency management in response to the findings and recommendations made in the Auditor General Report Number 2017-087. The review focused on corrective actions taken since the report's publication on January 5, 2017.

Items reviewed include:

- Project management detail, plans, and updates related to the PIM pilot project,
- Updates to Mainframe security for user authentication,
- AST policies and procedures uploaded to FASTdocs,
- Documents and tickets concerning the periodic review of users and service accounts,
- Interviewing of employees involved in the remediation of audit issues.
- C MDB updates including server remediation and configuration item discrepancy,
- COOP plan and test results,
- DR plan and test results,
- Cherwell tickets including, change and release records, tape destruction, and incident reporting,
- Backup and recovery test and tape destruction documents
- Other security controls as noted in finding 12.

This work product was prepared pursuant to section 20.055, Florida Statutes, and is consistent with the applicable standards as defined in the Principles and Standards for Offices of Inspectors General (as published by the Association of Inspectors General) and International Standards for the Professional Practice of Internal Auditing (as published by The Institute of Internal Auditors, Inc.)

To promote accountability, integrity, and efficiency in government, the Office of Inspector General conducts audits and reviews of Agency for State Technology's programs, activities, and functions.

Other reports prepared by the Office of Inspector General of the Agency for State Technology may be obtained by telephone (850-412-6022), mail (2585 Shumard Oak Blvd, Tallahassee, FL 32399), or by emailing Tabitha.McNulty@AST.MyFlorida.com