New York State Office of the State Comptroller
Thomas P. DiNapoli

Division of State Government Accountability

Security and Effectiveness of Division of Criminal Justice Services' Core Systems

Office of Information Technology Services

Report 2014-S-24 February 2015

Executive Summary

Purpose

To determine whether the Division of Criminal Justice Services' (Division) selected core systems are secure, operating effectively, and available to continue processing in the event of a disaster or mishap that disables normal processing. This audit covers the period May 22, 2014 through October 22, 2014.

Background

The New York State Office of Information Technology Services (ITS) was established in November 2012 as part of a New York State IT transformation to consolidate and merge State agencies and streamline services. ITS is responsible for providing centralized information technology (IT) services to the State and its governmental agencies, and is headed by a Chief Information Officer. ITS's Enterprise Information Security Office (EISO) is responsible for oversight and coordination of security services. ITS organized approximately 40 executive State agencies into nine clusters based on the type of service provided. The Division is one of eight agencies that comprise the Public Safety Cluster. The Division's mission is to enhance public safety and improve criminal justice. During the transition to ITS Enterprise-developed policies and processes, ITS is charged with ensuring proper controls are in place to protect the vast amount of personal data stored in the Division's systems, maintain compliance with applicable standards, and ensure continuity of effective and efficient operations.

Key Findings

- ITS does not have an established monitoring and oversight process for user access management of Division systems and is not operating in compliance with State Cyber Security Policies.
- ITS does not have established policies and procedures for backup of key Division systems. Also, ITS does not have an active regional backup site, and Division systems are at risk for total data loss in the event of a regional disaster.
- ITS does not have an established monitoring and oversight process for software or operating systems and changes made to these systems.

Key Recommendations

- Adhere to the New York State IT Account Management/Access Control Standard, as issued by the EISO, by establishing a Cluster process for granting, modifying, removing, tracking, and monitoring access privileges.
- Establish a comprehensive process to inventory and monitor Division data, operating systems, and software assets as well as their associated versions. Remove unsupported systems and software or update them to vendor-supported levels.
- Establish Cluster-level backup and recovery policies. Coordinate with the Division to develop and regularly test a comprehensive disaster recovery plan.

Other Related Audits/Reports of Interest

Office for Technology: Procurement and Contracting Practices (2010-S-71)
Office of Information Technology Services: Procurement and Contracting Practices (2013-F-24)

State of New York
Office of the State Comptroller

Division of State Government Accountability

February 24, 2015

Ms. Margaret Miller
NYS Chief Information Officer
Office of Information Technology Services
State Capitol
Empire State Plaza
P.O. Box 2062
Albany, NY 12220

Dear Ms. Miller:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage government resources efficiently and effectively and, by so doing, providing accountability for tax dollars spent to support government-funded services and operations. The Comptroller oversees the fiscal affairs of State agencies, public authorities, and local government agencies, as well as their compliance with relevant statutes and their observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations. Audits can also identify strategies for reducing costs and strengthening controls that are intended to safeguard assets.

Following is a report of our audit entitled *Security and Effectiveness of Division of Criminal Justice Services' Core Systems*. This audit was performed pursuant to the State Comptroller's authority under Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

This audit's results and recommendations are resources for you to use in effectively managing your operations and in meeting the expectations of taxpayers. If you have any questions about this draft report, please feel free to contact us.

Respectfully submitted,

Office of the State Comptroller
Division of State Government Accountability

Table of Contents

State Government Accountability Contact Information:
Audit Director: John Buyce
Phone: (518) 474-3271
Email: StateGovernmentAccountability@osc.state.ny.us
Address:
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

This report is also available on our website at: www.osc.state.ny.us

Background

The Office of Information Technology Services (ITS) was established in November 2012 as part of a New York State IT transformation to consolidate and merge State agencies and streamline services. ITS is responsible for providing centralized information technology (IT) services to the State and its governmental agencies, combining talent and assets from various agencies to foster innovation, build skills, and promote development in order to meet customer needs. To achieve this, ITS organized the IT employees from approximately 40 executive branch agencies, accounting for more than 4,000 staff, into nine clusters based on type of services provided: Environment and Energy, Financial, Administrative and General Services, General Government, Health, Human Services, Disability and Aging, Public Safety, and Transportation and Economic Development. ITS's objectives include consolidating cluster infrastructure operations for each agency cluster and improving cluster effectiveness and integration.

ITS is headed by a Chief Information Officer. There is also an Enterprise Operations Group headed by the Chief Operating Officer, which is responsible for delivering centrally managed IT services to the agencies. The Enterprise Information Security Office (EISO) is responsible for oversight and coordination of security services. The EISO has assumed the functions, powers, and duties of the former Office of Cyber Security (OCS) and will begin creating and implementing functions such as enterprise risk management, secure systems engineering and architecture, and cluster security services. In addition, the EISO is responsible for setting statewide security policies and developing standards for use by all State agencies. The EISO is revising the Cyber Security Policies (Security Policy) currently in effect, issued by the former OCS, in order to establish baseline standards and policies with which all clusters' policies must align. ITS standards and policies will follow the framework of the National Institute of Standards and Technology.

The Division of Criminal Justice Services (Division) is one of eight agencies that comprise the Public Safety Cluster. The Division's mission is to enhance public safety and improve criminal justice. The Division relies heavily on information technology to accomplish its mission, and uses approximately 76 computer applications, including such core systems as the Enterprise Fingerprint Process, Domestic Incident Reporting, Criminal History, DNA Management, Sex Offender Management, and the Missing Person and Vulnerable Adult Alert and Wanted Person Systems.

During the transition to ITS Enterprise-developed policies and processes, ITS is charged with ensuring proper controls are in place to protect the vast amount of personal data stored in Division systems, maintain compliance with applicable security standards for systems under their control, and ensure continuity of effective and efficient operations for those systems.

Public Safety Cluster (Cluster) management issued a strategic plan outlining and prioritizing Cluster-wide initiatives. This plan also outlines the Cluster's planning and governance processes, summarizes the long-term vision and resource constraints, and describes the various investments planned. Division officials remain responsible for the administration of its business continuity planning.

Audit Findings and Recommendations

ITS is in its second year of transformation and many Enterprise policies, and resultant Cluster-level policies, are still under development. Prior to the transformation, ITS did not conduct an underlying risk assessment to identify potential policy conflicts or other procedural issues among agencies, which could thereby assist with a smooth transition. As a result, employees have had to rely on some of their former agency policies and procedures, jeopardizing operational effectiveness and increasing the risk that critical functions and procedures are not consistently handled among the Cluster agencies. It is imperative that ITS ensure appropriate processes and controls continue to be followed as State entities transition from agency-specific policies to Enterprise-developed policies to minimize the risk of weakened operations and disruption in quality of service.

To determine whether the Division's core systems are secure, operating effectively, and available to continue critical processing in the event of a disaster or mishap, we evaluated a range of system controls, including compliance with security standards, access management, change management, and system uptime. We identified several critical areas in need of improvement, including system availability, access controls, disaster recovery planning, business continuity planning, data classification, operating systems and software management, and change management. We also found that ITS has not always established adequate control over its processes and procedures during the transition.

User Access Management

Neither ITS nor the Division have sufficient controls in place to properly manage user access to Division systems and they are not operating in compliance with ITS's Account Management/Access Control Standard. This standard establishes the rules and processes for creating, maintaining, and controlling the access of a digital identity to New York State applications and resources to protect State entity systems and information. As a result, there is less assurance that all user access is accurate and reliable. To test for appropriate user access, we reviewed a sample of 22 generic user accounts, seven generic database administrator accounts, and 25 employee user accounts.

Monitoring User Access to Databases

Cluster officials failed to manage user access to six critical Division databases we reviewed. Although the Cluster follows the previously established Division process for requesting database access, they only recently, during the course of our audit, started to implement processes that would establish a six-month management review of user access. However, formal procedures for this process have not yet been drafted or documented, and the initial review was not yet complete as of the end of our audit. As a result, the audit team was unable to review the process to determine compliance.

According to the Cluster official who maintains user access requests, aside from being collected in a box, these documents are not filed systematically in an order that would allow for ease of retrieval and review. In fact, for 3 of the 22 (13.64%) generic accounts reviewed in our sample,

this Cluster official was unable to determine why they were used and who used them.

In addition, this Cluster official continued to perform database administrator duties and maintain control of these documents even after transferring to the data management unit and no longer an official database administrator. Our review also found one other former database administrator who retained privileged access for over a year – and continued to perform database administrator duties – after moving to the data management unit. In the data management unit, both employees worked with developers to create, model, and administer databases. Allowing employees to perform both functions and not maintaining adequate separation of duties violates the New York State Information Technology Policy and could jeopardize the integrity, confidentiality, and security of Division information assets. In response to our preliminary audit findings, Cluster officials condoned the lack of separation of duties, stating that "this access was by design" and was necessary as part of the Cluster transition process. They indicated one administrator's duties have been fully transitioned and access will be removed, while the other administrator's access was scheduled to be removed by the end of November 2014.

At the start of our review, according to Cluster officials, there was no process for deprovisioning user or database administrator access that was no longer warranted, thereby increasing the risk of improper access. As a result, we found that 52 percent (13 of 25) of employee users we tested retained access to databases they no longer worked with. One of the 13 had retired on May 30, 2014, yet retained active access for two months afterward. Access for this employee was terminated as a result of our inquiry. We also determined that 23 percent (5 of 22) of the generic user accounts and 29 percent (2 of 7) of the generic database administrator accounts in our samples were no longer needed, including one for a student intern who no longer needed access. Following presentation of our findings, these accounts were either terminated or locked with intention to terminate after allowing for testing for any potential problems.

Our review also revealed that three of the database administrators in our sample had a total of four other "testing" accounts that were no longer necessary; these were also deleted as a result of our audit inquiry. In addition, contrary to the New York State Information Account Management/Access Control Standard, we found a generic database administrator account that has been accessed and used by multiple database administrators without the password ever being changed. In response to our preliminary audit findings, Cluster officials stated that they will be placing a log-on trigger on this account that will disable unwarranted account access; however, no documentation to support this assertion was provided.

General User Access

Neither the Division nor the Cluster has a viable system to monitor account management activities as required by the Account Management/Access Control Standard. The Division relies on a newly established, incomplete, and non-automated Systems Repository to aid in the oversight and monitoring of user access. The repository is not complete or automated as required by the Standard. Further, the Cluster does not have the capability to address user access as required; however, in response to our preliminary audit findings, officials contend they will review the newly published ITS Standard on Account Management/Access Control to propose new procedures as

necessary for compliance.

The Division's Systems Repository, which is used to track and monitor user access, was recently developed (March 2014) as a result of a May 2013 internal audit. The internal audit recommended the Division consider creating an entitlement repository featuring "a database that tracks, by user, system access and privileges assigned to that individual. It also includes information regarding when the user account was established, user rights and privileges, and any changes to the account. The required approvals and dates of authorization would also be included in the repository."

Our review found that the repository created did not account for 44 percent (67 of the 153) of the applications used by Division employees, including applications ranked highly critical such as the Domestic Incident Reporting, Enterprise Fingerprint Process, and Missing Person and Vulnerable Adult Alert System. Further, for those applications that are listed in the repository, there is no information concerning user privileges, account establishment, approvals, or authorization. Without any of this pertinent information, the repository is unable to serve its original purpose: to aid in the oversight and monitoring of user access. Furthermore, the repository is a manual process administered by a training and development employee as an additional duty. This person is made aware of employee interdepartmental transfers, but does not change access or follow up to determine appropriate employee access needs unless a notification is received.

In response to our preliminary report, the Division stated they intend to track user access for all electronic systems once it becomes available. The Cluster is completing a roles-to-resources initiative that will combine two existing capabilities which enable the Cluster to map each individual user to specific roles and then map each role to specific systems and applications.

Change Management

Although the Cluster follows a change management process to address Division system changes, it is still the same process the Division developed and followed prior to the transformation and thus is no longer completely relevant. Furthermore, the Cluster is not adhering to this process, which requires a Change Manager, an Emergency Change Advisory Board, and a Board of Governance, none of which are currently in place.

The Cluster has operated without a change management Board of Governance since January 2012 – a 2½-year gap in oversight of the Division's change management process. The three documented Emergency Change Advisory Board members no longer work in these roles, primarily as a result of employee separations and transformation changes. In addition, the Cluster has also been operating without a permanent Change Manager for a year, since November 2013, relying instead on an Acting Change Manager to assume these duties in addition to those of his primary position.

As a result of not having these key positions in place, the Cluster cannot ensure all changes obtain the appropriate approval and oversight prior to implementation. Furthermore, our review of the change management process found the process for approving, scheduling, and recording completion of changes is not being properly followed or documented.

To assess the integrity of the change management process, we reviewed 43 Request for Changes (RFCs) and 17 Emergency Request for Changes (ERFCs) as well as a sample of 39 changes documented on the change calendar. Among our findings:

- Hard-copy ERFCs are not being sent to the Acting Change Manager for verification as required.
- 71 percent (12 of 17) of ERFCs reviewed were not signed for approval by members of the Emergency Change Advisory Board existing at the time.
- 41 percent (7 of 17) of ERFCs reviewed either were not approved, or were approved improperly by one individual acting as both the original approver and a member of the Emergency Change Advisory Board.
- 14 percent (6 of 43) of RFCs reviewed either were requested and approved by the same employee or did not contain an approval.
- 49 percent (21 of 43) of RFCs and 35 percent (6 of 17) of ERFCs reviewed were approved and implemented despite not containing all required documentation, such as a back-out plan, testing plan, business impact, backup responsible party, or details/description of the change.
- 60 percent (26 of 43) of regular changes and 29 percent (5 of 17) of emergency changes reviewed were not documented on the change control calendar, or the calendar entry was not marked to reflect the status of change completion.
- 13 percent (5 of 39) of reviewed changes documented on the change calendar did not have the required supporting change request documentation showing the dates when appropriate approvals were obtained.

In response to our findings, Cluster officials noted the Cluster change management process is currently in a transition phase. In addition, the Cluster is working with Enterprise Operations to define and adopt a unified Enterprise solution for change management, and will create a full-time Change Manager role in accordance with the new process. However, officials did not provide any evidence of the process definition and time frame of implementation.

Operating Systems and Software Management

Despite the first goal of the Cluster's Strategic Plan to "maintain availability and performance of our information systems," neither the Cluster nor the Division maintains a complete inventory of Division software assets or operating systems and versions used. As a result, it is impossible to monitor assets as the New York State Technology Policy requires.

We reviewed the list of 47 software assets provided to us and found:

- 5 (11 percent) were no longer supported;
- 15 (32 percent) did not have sufficient information to determine whether they are supported; and
- 14 (30 percent) were at a version below what was currently offered by the vendor.

In response to our preliminary audit findings, Cluster officials stated that they plan to use the

tool Enterprise Elements, currently in a pilot phase, in tandem with their Information Technology Service Management System for more reliable software management and an improved picture of operating systems and software tracking.

Disaster Recovery

The Cluster is currently operating without a disaster recovery plan and does not have an adequate disaster recovery site. Currently, they rely on a high-availability configuration between two sites that are five miles apart. As a result, the Cluster and the Division face the possibility of complete data loss in the event of a regional disaster.

When we questioned officials about disaster recovery plans, Cluster officials provided us with a 2009 project proposal that identified a strategy to implement a disaster recovery plan. This five-year-old proposal refers to data centers and backup sites that no longer exist and makes no reference to the current data centers used by the Division and the Cluster. Cluster officials contend they are waiting for the completion of the ITS Disaster Recovery Site in Utica before completing a disaster recovery plan. However, during our visit to the new data center, Cluster officials informed us that, due to its size, the Utica site won't be able to physically accommodate the disaster recovery needs for all agencies, and it isn't known yet which agencies will be granted space. In addition, Cluster officials were unable to determine when the Utica site is scheduled to be operational.

In the course of our audit, Cluster officials stated they were unaware of a regional backup plan or regular testing performed. However, in response to our preliminary audit findings, the Cluster referenced a "robust backup plan," including a document not previously supplied to the audit team – "Backup and Recovery Services for Block Storage." The document calls for off-site backups to be sent to the Utica Disaster Recovery Site, even though the new site isn't operational yet and the Division may not be assigned to it once it is. When asked about the origins of the document, ITS officials informed us it was created for use in their response to our preliminary audit findings.

Business Continuity

We found the Division's Business Continuity Plan is also outdated, not completely relevant to the current transformation, and not entirely followed. Without a reliable plan, the Division could suffer a prolonged service outage, potentially disabling operations and impairing its ability to function as a government entity.

The Division was unable to provide evidence that officials have performed a comprehensive review and analysis of their mission-critical systems or a risk assessment, including recovery time objectives or recovery point objectives, evaluating the criticality of Division systems used in information processing. Further, the Division also lacks a formal agency-wide communications plan, and has not secured an alternate facility for use in the event the primary facility becomes uninhabitable. Finally, the Division has not provided employees with business continuity training, drills, exercises, or response capability assessments in more than two years.

The Division concurred with our preliminary audit findings regarding the completion of a risk analysis of mission-critical systems and a Division impact analysis. However, the Division noted that the outdated plan that is currently followed does contain elements of an agency communication plan. Specifically, each program area has a communication plan, but there is not a Division-wide, comprehensive communication plan. They also noted that they are working to secure an alternate facility and that a training plan has been developed that will soon be available to all employees. However, once again, they did not provide information as to when these items would be complete.

Data Classification and Service Level Agreements

The Security Policy indicates that all agency information should be classified on an ongoing basis based on its confidentiality, integrity, and availability. Further, Standard PS08-001, Information Classification and Control, notes that an information asset must be classified based on its highest level necessitated by its individual data elements.

According to the draft Service Level Agreement (SLA) provided to the audit team, the Cluster will coordinate with the Division to classify data so that appropriate security controls can be established. However, a data classification of Division information has not been performed, nor does the Division have a written or electronic inventory of all its assets. Without an inventory and classification of information, the Division is in violation of the New York State Information Classification Standard, and information entrusted to the Division may not be adequately protected.

The Division originally responded in agreement with our recommendations that a data classification process should be implemented. However, a month and a half later, officials revised their position and indicated that, based on assertions made by the Cluster, the Division participated in a joint analysis of data sets owned by various criminal justice agencies. This analysis found that data requiring high levels of confidentiality, integrity, and availability resided on a majority of the participating agencies' systems. Therefore, it was decided that the best approach to data classification was to protect all data at the highest classification level. Officials also noted the Cluster initiated the rollout of the Secure Systems Development Life Cycle to ensure any new systems meet standard security requirements and that existing or new data sets are classified and include the appropriate controls. Finally, Division officials stated they will continue to work with ITS to ensure that controls already established are appropriate for each data classification. However, Division officials did not provide any documentation supporting the previously performed data classification.

We also noted that, according to ITS's website, the SLA "between CIO/OFT (ITS) and the Cluster defines our mutual expectations, roles and responsibilities, service level outcomes, and financial commitments." In their response to our preliminary audit findings, officials stated that the SLA provided to the audit team was a draft, and since providing it to the audit team, ITS has decided not to execute SLAs with agencies but is instead pursuing other arrangements. In contrast, in response to our preliminary findings from another audit, ITS officials noted they are working with the Cluster agencies toward a complete and detailed SLA.

Uptime

The Cluster does not monitor the availability and performance of Division information systems, even though the Cluster's 2013-14 Strategic Plan lists the first organizational goal as "Maintaining availability and performance of our information systems," one component of which is to "monitor and measure systems availability and performance measures." In response to our preliminary audit findings, however, Cluster officials indicated that ITS's Enterprise Architecture will be monitoring system availability and has started an ongoing system availability and response time initiative to document key business scenarios by importance and usage. They reported that Enterprise Architecture has now initiated daily and weekly reports on system response times, which were scheduled to begin in September 2014. No further information was provided to indicate if all Division systems would be included in this effort.

Recommendations

1. Adhere to the New York State IT Account Management/Access Control Standard, as issued by the EISO, by establishing a Cluster process for granting, modifying, removing, tracking, and monitoring access privileges.

2. Appoint a permanent Change Manager and create a unified, Cluster-wide change management process.

3. Establish a comprehensive process to inventory and monitor Division data, operating systems, and software assets as well as their associated versions. Remove unsupported systems and software or update them to vendor-supported levels.

4. Establish Cluster-level backup and recovery policies. Coordinate with the Division to develop and regularly test a comprehensive disaster recovery plan.

5. Coordinate with the Division to perform a comprehensive risk analysis of mission-critical systems and a Division impact analysis, and to update the Business Continuity Plan to include proper training and the identification of an alternate facility.

6. Formalize and complete the process of classifying Division data.

7. Develop and implement a current Service Level Agreement or similar arrangement that defines mutual expectations, roles and responsibilities, etc. for ITS, the Cluster, and the Division.

8. Implement a process to monitor the availability and performance of Division systems.

Audit Scope and Methodology

We audited the security, effectiveness, and long-term sustainability of core Division IT systems at ITS for the period May 22, 2014 through October 22, 2014. The objective of our audit was to determine whether the Division's core systems are secure, operating effectively, and available to continue processing in the event of a disaster or mishap that disables normal processing.

To accomplish our objective, we interviewed selected ITS and Division officials to obtain an understanding of ITS Enterprise, Cluster, and Division policies and procedures, as well as internal controls relevant to security and effectiveness of the Division's computer systems. To complete our audit work, we reviewed supporting documentation for user access, business continuity, disaster recovery, change management, security, and system availability in order to determine compliance with established policies. We reviewed user access for a judgmental sample of 6 of the 76 Division databases. We then selected a random sample of 25 employees, 21 database administrators, and 22 generic user accounts from the population of 108 users with access to these six databases. We also visited the State data center.

We conducted our performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions, and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our opinion, these functions do not affect our ability to conduct independent audits of program performance.

Authority

The audit was performed pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

Reporting Requirements

We provided a draft copy of this report to ITS officials for their review and comment. We considered their comments in preparing this report and have included them in their entirety at the end of it. ITS officials generally concurred with our report's recommendations and indicated that certain actions have been and will be taken to address them. Our rejoinders to certain ITS

comments are included in the report's State Comptroller's Comments.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Chief Information Officer shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and if the recommendations were not implemented, the reasons why.

Contributors to This Report

John Buyce, CPA, CIA, CFE, CGFM, Audit Director
Brian Reilly, CFE, CGFM, Audit Manager
Nadine Morrell, CISM, CIA, CGAP, Audit Supervisor
Holly Thornton, Examiner-in-Charge
Rachael Hurd, Staff Examiner
Patrick Lance, Staff Examiner
Marzie McCoy, Senior Editor

Division of State Government Accountability

Andrew A. SanFilippo, Executive Deputy Comptroller
518-474-4593, asanfilippo@osc.state.ny.us

Tina Kim, Deputy Comptroller
518-473-3596, tkim@osc.state.ny.us

Brian Mason, Assistant Comptroller
518-473-0334, bmason@osc.state.ny.us

Vision

A team of accountability experts respected for providing information that decision makers value.

Mission

To improve government operations by conducting independent audits, reviews and evaluations of New York State and New York City taxpayer financed programs.

Agency Comments

ANDREW M. CUOMO
Governor

Empire State Plaza
P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

MARGARET MILLER
NYS Chief Information Officer
Director, Office of IT Services

Mr. John Buyce
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

Re: Audit Report 2014-S-24

Dear Mr. Buyce:

In regards to your Draft Audit Report 2014-S-24 issued by the Office of the State Comptroller (OSC), which covers the results of your audit on the Security and Effectiveness of the Division of Criminal Justice Services' Core Systems, please find our written response from ITS's viewpoint for your consideration. Please feel free to contact me for any questions or clarifications.

Sincerely,

Theresa Papa
Director of Administration

Introduction

Please allow this letter to respond to the Draft Audit Report 2014-S-24 issued by the Office of the State Comptroller (OSC) concerning the security and effectiveness of Division of Criminal Justice Services' (DCJS) Core Systems (the Draft Report). This letter will also serve to offer some clarifications of and corrections to certain statements and representations in the Draft Report. These clarifications in no way diminish the appreciation of ITS in the Draft Report's findings and recommendations. The IT Transformation is large, complex and in progress, however, we believe that these responses provide a more accurate reflection of how the IT Transformation is progressing and its relation to DCJS systems specifically. Accordingly, ITS seeks to make the following clarifications to the descriptions of its organization in the Draft Report.

Clarification of ITS Organization (Background):

As indicated in the Draft Report, the Office of Information Technology Services (ITS) was established as part of a New York State IT transformation to streamline and modernize the delivery of information technology (IT) by the State. This was effected on November 22, 2012 when IT professionals from approximately 40 executive branch agencies were transferred to ITS. In addition to the transference of personnel, ITS also assumed responsibility for the processes which were then in effect for those 40 executive branch agencies.

ITS is headed by the NYS Chief Information Officer. Within ITS there are two types of service delivery organizations: centrally managed IT services, such as infrastructure services, directed by a Chief Operating Officer (COO); and cluster-based IT services, which are directed by a Cluster Chief Information Officer (CIO). The COO and the Cluster CIOs all ultimately report to the NYS CIO. Each cluster is made up of IT professionals who support a group of agencies. Agencies are grouped into clusters based on similarities between their core missions. The clusters are: Environment and Energy, Financial, Administrative and General Services, General Government, Health, Human Services, Disability and Aging (formerly known as "Behavioral Health"), Public Safety, and Transportation and Economic Development. DCJS is an executive agency within the Public Safety Cluster.

The Draft Report mentions DCJS continued responsibility for the administration of its Business Continuity planning. DCJS also continues to be responsible for data classification and management and setting priorities of, and dedicating funding for, DCJS-related IT projects.

Within ITS exists the Enterprise Information Security Office (EISO), whose responsibilities include protecting the NYS government's cyber security infrastructure and providing statewide coordination of policies, standards, and programs relating to cyber security. The Draft Report states that "The

EISO is revising Cyber Security Policies (Security Policy) currently in effect, issued by the former OCS in order to establish baseline standards and policies with which all clusters' policies must align. ITS standards and policies will follow the framework of the National Institute of Standards and Technology." The goal of the coordination effort with regard to policies and standards is for all clusters to adhere to EISO promulgated enterprise policies and standards which are aligned with ISO/IEC Information Security Management Systems (ISMS) standards 27001 & 27002, and based on NIST standards to the extent practicable. Additionally, in the Draft Report OSC states that ITS EISO assumed the powers and functions of the former Office of Cyber Security (OCS). While that is correct, the Draft Report indicates that OCS was performing certain enterprise-grade security functions that it was not. More specifically, OCS did not perform enterprise risk management (outside of the annual policy compliance assessment), secure systems engineering and architecture, or cluster security services. Because EISO did not absorb these functions from OCS, EISO is now creating and implementing these functions.

* Comment 1

Audit Findings and Recommendations:

ITS takes the security and effectiveness of all of the systems it operates, including DCJS's, very seriously and welcomes the insight, input and recommendations offered by the auditors. While this Draft Report focuses on DCJS alone, it is worth noting that on November 22, 2012, ITS instantly became responsible for the operation, security, deployment, patching and management of the legacy products, systems and applications that have historically been developed over the decades in the 40+ different agencies and their varied environments under different processes, some of which may now be considered outdated. The point of IT Transformation is for ITS to harmonize these disparate management processes and policies that flourished in these 40+ agencies and establish a consistent set of best practices to be leveraged across all of them. The Draft Report does not adequately describe the enormity of this task when it states that "Prior to the transformation, ITS did not conduct an underlying risk assessment to identify potential policy conflicts or other procedural issues among agencies, which could thereby assist with a smooth transition. As a result, employees have had to rely on some of their former agency policies and procedures, jeopardizing operational effectiveness and increasing the risk that critical functions and procedures are not consistently handled among the Cluster agencies.

Recommendation

1. Adhere to the New York State IT Account Management/Access Control Standard, as issued by the EISO, by establishing a Cluster process for granting, modifying, removing, tracking, and monitoring access privileges.

   ITS Response:

* See State Comptroller's Comments, page 24.

Based on the EISO Standard on IT Account Management/Access Control, published on August 15, 2014, ITS will propose new supporting procedures, if necessary, for compliance. If funding is required to implement these procedures, ITS will review with DCJS and the Cluster Executive Board (CEB). ITS is currently in the process of linking systems to produce timely reports for proactive management review.

Recommendation

2. Appoint a permanent Change Manager and create a unified, Cluster-wide change management process.

   ITS Response:

   The ITS management team has been engaged with the Enterprise Operations team in both defining, and ultimately adopting a unified Change Management Process. ITS has identified a full time resource for the Public Safety Cluster Change Manager. Initially, the Change Manager will be responsible for implementing the existing DCJS Change Management Process. As the new Enterprise Change and/or Configuration Management policies are rolled out, the Change Manager will be tasked with reviewing these new policies and implementing appropriate procedures within PSC to comply with the policies. The full time Change Manager will be in the new role by mid-December 2014.

Recommendation

3. Establish a comprehensive process to inventory and monitor Division data, operating systems, and software assets as well as their associated versions. Remove unsupported systems and software or update them to vendor-supported levels.

   ITS Response:

   ITS has begun to use State-wide Enterprise Elements software to inventory the entire enterprise's applications. Additionally, ITS is in the process of implementing a discovery and dependency mapping tool, ADDM. This information will help identify unsupported systems and software. As for the recommendation to inventory Division data, Division data management is the responsibility of DCJS. Finally, removing or updating unsupported systems and software is a complex endeavor that generally requires significant time to procure, plan, test, and migrate as well as funding. Any such efforts to remove or update unsupported systems and software is prioritized and funded by DCJS based on DCJS business needs using the IT project governance process.

Recommendation

4. Establish Cluster-level backup and recovery policies. Coordinate with the Division to develop and regularly test a comprehensive disaster recovery plan.

ITS Response:

The first sentence of this recommendation was based on the cited conditions that Cluster Officials were unable to provide a backup and recovery schedule followed by the Cluster during the audit discovery period but the Cluster did provide and confirm that it follows the Backup and Recovery services outlined with the ITS Data Center Block Storage Service offering (see Appendix A). The Draft Report on Page 9 indicates that ITS officials informed the OSC auditors that the ITS Data Center Block Storage Service offering document was created in response to OSC preliminary audit findings. This is not accurate. The document was previously developed and was to be included in the Service Catalog when published.

* Comment 2

Regarding the development and testing of a comprehensive disaster recovery plan, once the Public Safety Cluster transitions to the statewide data center and disaster recovery processes are implemented, ITS will work with the Division to develop and regularly test a comprehensive disaster recovery plan.

Recommendation

5. Coordinate with the Division to perform a comprehensive risk analysis of mission-critical systems and a Division impact analysis, and to update the Business Continuity Plan to include proper training and the identification of an alternate facility.

   DCJS Response:

   The Division of Criminal Justice Services concurs with this recommendation and will work with ITS to conduct a risk analysis on all mission critical systems.

Recommendation

6. Formalize and complete the process of classifying Division data.

   DCJS Response:

   All data elements are currently classified as confidential and subject to the highest level of security. The Division will take steps to formally document the data elements as such.

Recommendation

7. Develop and implement a current Service Level Agreement, or similar arrangement that defines mutual expectations, roles and responsibilities, etc. for ITS, the Cluster, and the Division.

   ITS Response:

   ITS continues to work with the public safety agencies to accurately capture the service levels in the appropriate service level documents.

Recommendation

8. Implement a process to monitor the availability and performance of Division systems.

   ITS Response:

   Daily and weekly response time reports were initiated in October 2014 for the highest priority systems based on key business scenarios and usage. As part of a larger initiative, performance and availability monitoring will be planned out and implemented beginning in 2015 including the implementation of Continuous Diagnostic Monitoring and Security Information and Event Management (SIEM) tools.

Thank you for this opportunity to respond to this draft audit.

(Appendix A)

Backup and Recovery Services for Block Storage

1. Purpose

Backup and Recovery is a service component included within the ITS data center Block Storage service offering. Backup and recovery will be offered in the service catalog and will be available to ITS enterprise data center service subscribers that host business application solutions.

Note: Block storage is a type of data storage typically used in storage-area network (SAN) environments where data is stored in volumes, also referred to as blocks.

2. Service Objective

Backup and recovery is about operational recovery of a business system. The primary objective of backup and recovery is to recover a system as quickly as possible and as close to the last "good state" of the system as possible.

All systems, applications, and databases centrally hosted by ITS will be protected against data loss by the use of regularly scheduled backups following standard backup procedures.

This service should be used as part of a set of solutions and technologies to address stricter business requirements for application and data recovery (e.g. local and remote replication, high-availability systems, application level resiliency and recovery).

3. Service Features

a. The scope of this service is limited to distributed systems environments. It does not address mainframe platforms.

b. The service is built using industry standard, vendor provided solutions.

c. Backups are performed to centrally located storage media.

d. The backup service is automated, centrally scheduled, and policy based.

e. Recovery services include the full range of requirements from single files to complete server rebuilds.

f. The service leverages common ITS incident, change, problem, and request management processes.

4. Backup Retention

Retention refers to the amount of time backup copies are held before they are of no value for operational recovery needs.

a. For infrastructure components, such as, operating systems, applications, and all flat-file data structures, the retention is 30 days.

b. For platform components, such as, database, the retention policy is 30 days. The ITS platform delivery teams will work with the business data owners to address exceptions and provide alternate solutions.

5. Backup Schedules

a. For infrastructure components, such as, operating systems, applications, and all flat-file data structures backups are scheduled to run every 24 hours.

b. For platform components, such as, database, the schedules will be managed based on service classification standards. ITS Application Platform teams will work with the business data owners to address exceptions and provide alternate solutions.

6. Offsite Protection

a. Daily copies of backup data is electronically transferred offsite to an alternate data center facility.

b. For agencies that have consolidated to the common ITS Enterprise solution at CNSE the offsite backups are sent to the Utica DR site.

7. Data Archiving

a. Longer-term data retention and archiving requirements are addressed on a case by case basis

State Comptroller's Comments

1. Based on the ITS response, we revised our report to clarify the prior and planned roles of the EISO.
2. We do not agree with ITS. The audit team received an e-mail from an ITS staff member indicating that the document in question was, in fact, created in response to our preliminary findings.