THOMAS P. DiNAPOLI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

April 7, 2017

Mr. Mahesh Nattanmai
Executive Deputy Chief information Officer
Office of Information Technology Services
Empire State Plaza
P.O. Box 2062
Albany, NY 12220

Re: Security and Effectiveness of Division of Criminal Justice Services' Core Systems
Report 2016-F-28

Dear Mr. Nattanmai:

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, we have followed up on the actions taken by officials of the Office of Information Technology Services to implement the recommendations contained in our audit report, *Security and Effectiveness of Division of Criminal Justice Services' Core Systems* (2014-S-24).

Background, Scope, and Objectives

The Office of Information Technology Services (ITS) was established in November 2012 as part of the New York State Information Technology Transformation to consolidate and merge State agencies and streamline information technology services. The consolidation of agency information technology employees was organized into clusters, based on the type of service the agency provides. ITS currently has eight clusters: Administration and General Services, Revenue and Transportation, Citizen Services, Disabilities and Aging, Health, Human Services, Public Safety, and Enterprise Business Solutions. The Division of Criminal Justice Services (Division) is one of seven agencies included in the Public Safety cluster (Cluster).

Our initial audit report, which was issued on February 24, 2015 covering the period of May 22, 2014 through October 22, 2014, determined whether the Division's core systems were secure, operating effectively, and available to continue critical processing in the event of a disaster or mishap that disabled normal processing. We found that ITS did not have established policies and procedures for backup of key Division systems. Also, ITS did not have an active regional backup site, and Division systems were at risk for total data loss in the event of a regional disaster. We also found ITS did not comply with certain State cybersecurity policies and did not establish adequate

processes to monitor and oversee user access to Division operating systems and software as well as the changes made to systems and software. The objective of our follow-up was to assess the extent of implementation, as of March 13, 2017, of the eight recommendations included in our initial audit report.

Summary Conclusions and Status of Audit Recommendations

ITS made some progress in implementing the recommendations identified in our prior audit report. However, we found that disaster recovery and business continuity planning continue to be deficient, and ITS had not entered into a cooperative agreement with the Division to delineate agency versus ITS responsibilities. Of the eight prior recommendations, four have been implemented, two have been partially implemented, and two have not been implemented.

Follow-Up Observations

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.

Status – Implemented

Agency Action – The Cluster now handles requests for granting, modifying, and cancelling access to critical systems directly in its IT service management tool, which documents approval and also allows tracking and monitoring of user access rights. Granting and modifying access now requires approval by both the Division and ITS, and the Cluster has updated its forms accordingly. Further, the Cluster follows detailed procedures to ensure that all access is revoked timely when a user leaves employment.

Effective September 2016, the Cluster requires a biannual review of database access to identify and remove users who no longer need access. The Cluster also developed the ability to track and monitor user access to critical applications along with a process whereby access will be reviewed on a quarterly basis. Division executive staff, managers, and supervisors and Cluster managers will receive a quarterly report on critical access information to review.

Recommendation 2

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

Status – Implemented

Agency Action – The Cluster has established a Cluster Change Advisory Board that includes a

permanent Change Manager. The Cluster has also developed a change management process that aligns with the ITS Enterprise-Wide Change Management policy issued in January 2016. As part of the process, the Cluster uses the IT Service Management tool to administer its change requests.

Also, although the Cluster implemented our recommendation, we noted in another follow-up report (2016-F-15, issued in December 2016) that the IT Service Management tool does not allow Cluster or Division officials to ensure all implemented system changes have gone through the approved management process and are recorded. To provide adequate controls, ITS is developing a separate configuration management database which will flag exceptions and create a report when changes are applied. Without established controls to ensure that all changes adhere to the established process, ITS cannot demonstrate that the process is working as intended.

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.

Status – Not Implemented

Agency Action – The Cluster has not developed a comprehensive process to inventory and monitor Division systems and software. We found unsupported systems and software that had not been removed or updated. Among the issues we found were:

- 22 (14 Linux, 7 Windows, and 1 SQL) servers no longer supported;
- 20 Oracle databases no longer supported; and
- 6 Oracle databases without the version numbers required to determine whether they are supported.

The Cluster established a standard for the management of commercial off-the-shelf (COTS) products, effective April 2016. According to this standard, the Cluster COTS team is supposed to keep a central repository of all COTS applications, and review the repository at least once a year to ensure it is up to date and accurate. However, the Cluster is not in compliance with its own standard. At the time of our audit, the repository had 32 total COTS applications but only seven applications actually had a version listed, and only one of those was current. In addition, only ten COTS applications had license information, and six of those had expired.

The Cluster does not have accurate information regarding the status of Division infrastructure. We were given a status report from November 2016 showing that the Cluster remediated 32 unsupported Division servers. However, a second report from January 2017 of active Division servers included seven of these unsupported servers, indicating that they were still in use and therefore had not been remediated. ITS officials

subsequently stated that they have added staff to the COTS team, which has now identified 118 COTS products in inventory. However, ITS officials failed to provide an updated list with those 118 products and their version and license information.

Recommendation 4

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

Status – Partially Implemented

Agency Action – Since August 2014, the Cluster has been covered by the Enterprise ITS Backup and Recovery Services. These backup and recovery services cover six operating system types and two virtual environments that are tested three times per year. However, the Cluster currently does not have disaster recovery capability covering the core business systems used by the Division. It is working on a disaster recovery plan that will provide disaster recovery capability to restore critical Division systems. However, according to ITS officials, a final comprehensive disaster recovery plan for the Cluster is on hold pending development of a Statewide Disaster Recovery Strategy.

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.

Status – Partially Implemented

Agency Action – The Division provided the audit team with a Continuity of Operations Plan and Comprehensive Emergency Management Plan (Plan) dated October 2015. The Plan referenced a Division impact analysis that was conducted as well as a list of the Division's essential functions as supported by a separate document (dated April 2015) identifying the Division's mission-critical systems, and also contained responses to the Plan from all 13 units of the Division as an appendix. The Plan requires annual review by each office, which provides any changes to the Division's Emergency Manager so that the Plan can be updated by September 30 of each year. The Plan requires annual training for all employees of the Division, regardless of which unit they work for. According to Division officials, the training is done via an online system, and all employees completed the training in 2016.

However, the Plan does not have an alternate location for Division employees to report should the building remain closed for a significant period of time, though one unit did specify an alternate location for its employees in its response to the Plan. According to Division officials, they have identified an alternate location, and are now working with ITS and the Division of Homeland Security and Emergency Services to finalize the arrangements for that site.

Recommendation 6

Formalize and complete the process of classifying Division data.

Status – Implemented

Agency Action – The Division has developed an Information Asset Classification System Repository (Repository). As of January 2017, the Repository had 69 assets, with the following information about each: description, use, Department to which the asset belongs, source, business process supported, information owner and custodian, internal and external information users, activity status, format, means of storage, confidentiality, integrity, availability, classification date, and comments.

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.

Status – Not Implemented

Agency Action – During the aforementioned follow-up review (2016-F-15), we obtained a draft Customer Operating Agreement that documents IT service management and specific services, such as system availability, level of support, and the process to manage service interruptions/outages. However, the only agreement ITS officials provided us for this follow-up was an updated Management Control Agreement (MCA) between ITS and the three State agencies (one of which is the Division) in the Cluster that maintain criminal justice systems and data subject to Federal policies. The MCA covers security policy, guidelines, and standards for state and Federal criminal justice systems and agency-specific information systems under ITS control. However, this document does not define service level objectives for ITS, the Cluster, or the Division, and so does not address the recommendation. According to ITS officials, they aim to meet the same standards that were achieved by the agencies before the creation of ITS. However, they did not provide us with any evidence of what those standards would be or how they would be met.

Recommendation 8

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

Status – Implemented

Agency Action – The Cluster adheres to the Enterprise Secure System Development Life Cycle Standard in order to make systems less susceptible to security issues that might impact availability and performance. In addition, as a result of our original audit, the Cluster has implemented several tools to monitor the availability and performance of Division systems, as well as its own performance in diagnosing, troubleshooting, and resolving issues.

Major contributors to this report were Nadine Morrell, Jennifer Paperman, Jared Hoffman, Holly Thornton, and Christopher Bott.

We would appreciate your response to this report within 30 days, indicating any actions planned to address the unresolved issues discussed in this report. We also thank the management and staff of ITS for the courtesies and cooperation extended to our auditors during this review.

Very truly yours,

Brian Reilly, CFE, CGFM
Audit Director

cc: Rajni Chawla, ITS Director of Internal Audit
Division of the Budget