



Office of Information Technology Services

ANDREW M. CUOMO
Governor

MARGARET MILLER
Chief Information Officer

The Honorable Andrew M. Cuomo
Governor
State of New York
State Capitol
Albany, New York 12224

The Honorable Carl E. Heastie
Speaker
New York State Assembly
Legislative Office Building, Room 932
Albany, New York 12248

The Honorable Kathleen C. Hochul
Lieutenant Governor
State of New York
State Capitol
Albany, New York 12224

The Honorable Joseph D. Morelle
Majority Leader
New York State Assembly
Legislative Office Building, Room 926
Albany, New York 12248

The Honorable Thomas P. DiNapoli
Comptroller
State of New York
110 State Street
Albany, New York 12236

The Honorable Brian M. Kolb
Minority Leader
New York State Assembly
Legislative Office Building, Room 933
Albany, New York 12248

The Honorable John J. Flanagan
Temporary President and Majority Leader
New York State Senate
State Capitol, Room 330
Albany, New York 12247

The Honorable John A. DeFrancisco
Chairman, Finance Committee
New York State Senate
State Capitol, Room 416
Albany, New York 12247

The Honorable Jeffrey D. Klein
Independent Democratic Conference Leader
New York State Senate
Legislative Office Building, Room 913
Albany, New York 12247

The Honorable Liz Krueger
Ranking Member, Finance Committee
New York State Senate
Legislative Office Building, Room 808,
Albany, New York 12247

The Honorable Andrea Stewart-Cousins
Democratic Conference Leader
New York State Senate
Legislative Office Building, Room 907
Albany, New York 12247

The Honorable Herman D. Farrell, Jr.
Chairman, Ways and Means Committee
New York State Assembly
Legislative Office Building, Room 923
Albany, New York 12248

The Honorable Robert C. Oaks
Ranking Member, Ways and Means Committee
New York State Assembly
State Capitol, Room 444
Albany, New York 12248

Dear Governor Cuomo, Lt. Governor Hochul, Comptroller DiNapoli, Leader Flanagan, Leader Klein, Leader Stewart-Cousins, Speaker Heastie, Leader Morelle, Leader Kolb, Senator DeFrancisco, Senator Krueger, Assemblyman Farrell and Assemblyman Oaks:

Enclosed is the ITS status report on the implementation of recommendations contained in the Office of the State Comptroller's audit report entitled: "Security and Effectiveness of the Division of Criminal Justice Services' Core Systems – Report 2014-S-24". ITS's responses do not contain specific details of its security efforts in order to better protect the integrity of the State's critical infrastructure and data.

Sincerely,

A handwritten signature in dark ink, appearing to read "Theresa Papa", is written over a faint, circular official seal.

Theresa Papa
Director of Administration

Enclosure

OFFICE OF INFORMATION TECHNOLOGY SERVICES
Status of the Office of the State Comptroller's
Recommendations Contained in the Final Audit Report on
"Security and Effectiveness of Division of Criminal Justice Services' Core Systems"
Report 2014-S-24

Recommendation	Status
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.	Access to Division systems by ITS (or Division) employees are authorized by the Division. A quarterly process to validate the applications and systems that individuals have access to has been implemented. The full adherence with the EISO Standard on Account/Management/Access control is expected to be completed between ITS and the Division in late 2015.
2. Appoint a permanent Change Manager and create a unified, Cluster-wide change management process.	A permanent Change Manager was appointed for the Public Safety Cluster (PSC) in January 2015. An enterprise-wide change management process is under development.
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.	<p>ITS Data Center Hosting (DCH) has a comprehensive process to inventory and monitor Operating Systems supported by ITS at CNSE. ITS has a process, compliant with the Patch Management Standard issued by EISO in January 2015, to continually patch all Operating Systems that are currently supported by the OS Vendor.</p> <p>ITS has an inventory of the entire enterprise's applications and software products. The focus is on maturing the business processes to keep the information current.</p> <p>While these tools and processes to identify opportunities to remove unsupported systems and software, these changes require funding that, in many cases, has not and continues not to exist. Additionally, removal of unsupported systems and software requires significant investments in, and commitment to, application modernization by and between the impacted business, technology and budget making entities.</p>
4. Establish Cluster-level backup and recovery policies. Coordinate with the Division to develop and regularly test a comprehensive disaster recovery plan.	<p>Since August 14, 2014, DCJS has subscribed to Backup and Recovery Services for Block Storage provided by ITS. This service was formally published as a Technical Standard on October 27, 2014. The backup team performs recovery testing of each OS platform twice per year.</p> <p>In addition, ITS is supporting the Division in its development of a disaster recovery (DR) solution for those applications that the Division identifies as being critical. This DR solution is intended to be based in the State's DR facility in Utica and would be invoked should a catastrophic event cause the primary infrastructure to become unavailable. We expect this proposal to go before the Public Safety IT Governance Board, which is comprised of public safety and not ITS staff, by the end of this calendar year.</p>
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 identification of an alternate facility.	The Division is primarily responsible for its Business Continuity plan, however, ITS is working with the Division to identify a suitable facility for Business Continuity and to identify an enterprise wide back-up location with high availability.

<p>6. Formalize and complete the process of classifying Division data.</p>	<p>According to the Information Classification IT Standard, NYS-S14-002, information owners are responsible for classifying information and data. The Division is the owner of its data and is responsible for classifying it. ITS provides consultation to the Division's business units about data classification and related issues.</p>
<p>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.</p>	<p>ITS continues to work with the Division towards documenting roles and responsibilities within each agency. As enterprise services, policies and processes are finalized, deployed, and adopted, these services, policies and processes will supersede legacy arrangements.</p>
<p>8. Implement a process to monitor the availability and performance of Division systems.</p>	<p>The Division has identified its highest priority systems. Performance of these high priority systems is monitored by daily and weekly response time reports, which were initiated in October 2014. Availability of these highest priority Division systems is monitored by a weekly Priority 1 Incident (i.e., system is unavailable) reports, which were initiated in March 2015.</p>