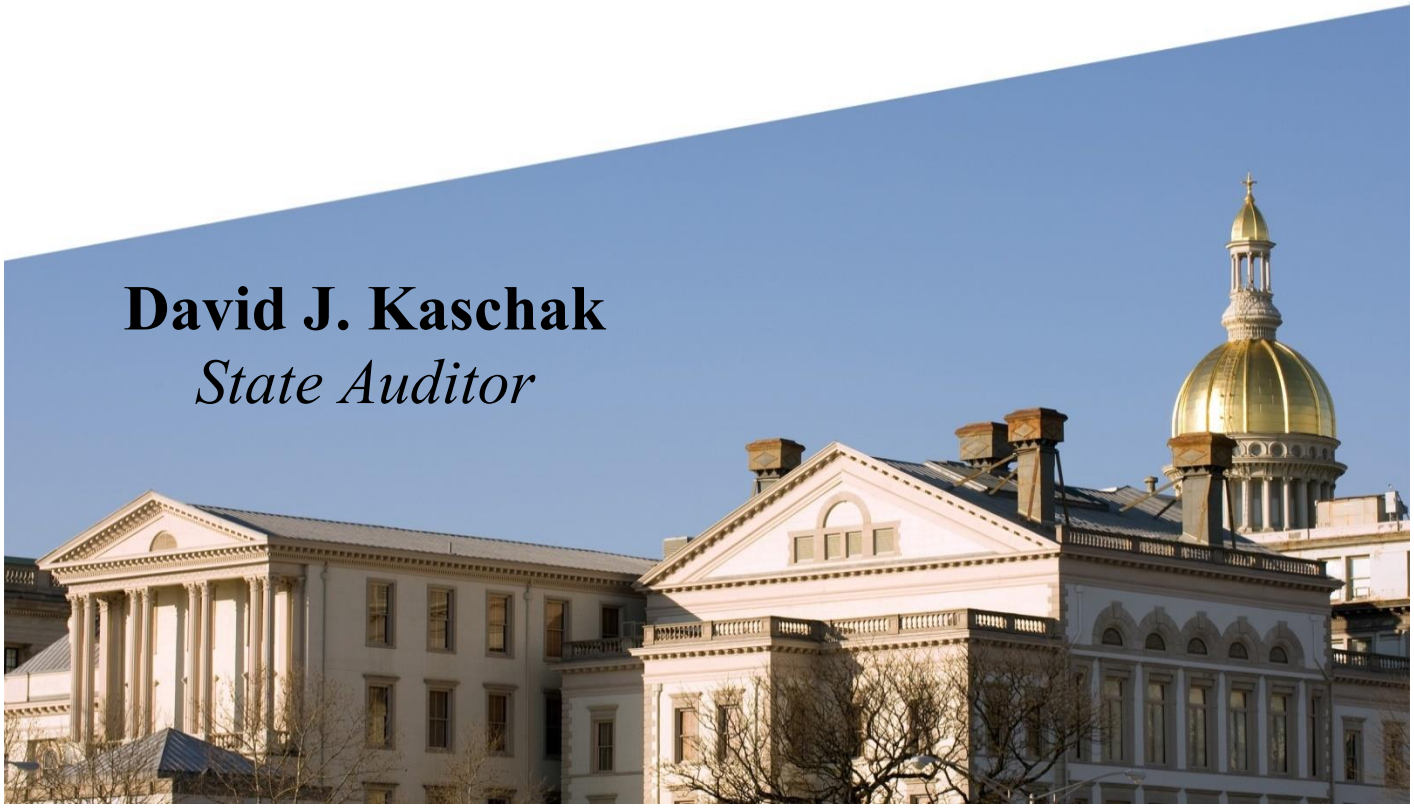
NEW JERSEY LEGISLATURE

OFFICE OF LEGISLATIVE SERVICES

OFFICE OF THE STATE AUDITOR

Office of Information Technology
Executive Branch Software-as-a-Service (SaaS)

February 1, 2024 to March 31, 2025



NEW JERSEY LEGISLATURE
OFFICE OF LEGISLATIVE SERVICES

125 SOUTH WARREN STREET • P.O. BOX 067 • TRENTON, NJ 08625-0067
www.njleg.gov

OFFICE OF THE STATE AUDITOR
609-847-3470

David J. Kaschak
State Auditor

Brian M. Klingele
Assistant State Auditor

Thomas Troutman
Assistant State Auditor

The Honorable Philip D. Murphy
Governor of New Jersey

The Honorable Nicholas P. Scutari
President of the Senate

The Honorable Craig J. Coughlin
Speaker of the General Assembly

Ms. Maureen McMahon
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Office of Information Technology, Executive Branch Software-as-a-Service for the period of February 1, 2024 to March 31, 2025. If you would like a personal briefing, please call me at (609) 847-3470.

David J. Kaschak

David J. Kaschak
State Auditor
September 10, 2025

Table of Contents

Scope

We have completed an audit of the Office of Information Technology, Executive Branch Software-as-a-Service (SaaS) provider and service management for the period of February 1, 2024 to March 31, 2025. Our audit focused on SaaS providers and products in use by executive branch departments and agencies during the audit period.

Objectives

The objectives of this audit were to evaluate the Office of Information Technology's (OIT) controls and processes in place related to SaaS providers and products in the executive branch and to determine state department and agency compliance with those controls and processes specifically related to the acquisition, performance and monitoring, and security of the SaaS provider and product.

This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section I, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted 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 objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Additional guidance for the conduct of the audit was taken from the New Jersey *Statewide Information Security Manual* (*SISM*), published by the New Jersey Office of Homeland Security and Preparedness (OHSP), and various industry best practices. These documents were used as the criteria against which internal controls were measured.

In preparation for our testing, we studied legislation, circulars promulgated by the Department of the Treasury and the Office of Information Technology (OIT), individual agency policies and procedures, and industry best practices. We also reviewed SaaS provider contracts, interviewed agency personnel, and surveyed state agencies in the executive branch. Provisions we considered significant were documented, and compliance was verified by interviews with key personnel and reviewing relevant documentation. To achieve our objectives, we performed various tests and analyses as we determined necessary. Additional details regarding our methodology and work performed can be found in the Appendix, as well as in the finding section when testing resulted in a reportable condition.

A non-statistical judgmental sampling approach was used. Our sample was designed to provide conclusions on our audit objectives, as well as internal controls and compliance. Because we used a nonstatistical sampling approach for our tests, we cannot project the results to the respective populations.

Data Reliability

We assessed the reliability of the data collected from our surveys through follow-up meetings with the agency personnel who provided the information. Those meetings included a more in-depth inquiry into the survey responses and a review of documentation referenced in the survey. We determined that the data was sufficiently reliable for the purposes of this report.

Conclusion

We found that, overall, the Office of Information Technology has adequate controls and processes in place related to Software-as-a-Service providers and products in the executive branch and that state departments and agencies are complying with those controls and processes. In making these determinations, we noted certain opportunities for improvement meriting management's attention regarding the system architecture review process, disaster recovery documentation, and the establishment of service-specific key performance indicators.

Background

Software-as-a-Service (SaaS) is a software delivery model in which the state department or agency accesses a provider's product through an internet-based connection. In this model, most aspects of the product are managed by the provider, with the individual department or agency retaining some responsibilities. Though individual SaaS configurations may vary slightly, the basic SaaS shared responsibility model is as follows:

SaaS Cloud Shared Responsibility Model

Responsibilty	On-Premise	SaaS Provider
Data	Customer	Customer
Identity and Access	Customer	Customer
Application	Customer	Both
Runtime and Performance	Customer	Provider
Operating Systems	Customer	Provider
Hardware and Network	Customer	Provider
Disaster Recovery	Customer	Provider
Physical Security	Customer	Provider

- Data – The information that is stored within the application and the confidentiality level given to that data by the data owner.

- Identity and Access – The method by which authentication to the application is handled, as well as the assignment of authorized privileges within the application.

- Application – Different aspects of the application can be managed by the customer and the provider. The customer would configure operational options of the application; however, application patching and maintenance may be handled by the provider.

- Runtime and Performance – The application's availability for use by the customer, including both the uptime of the application as well as the quality of the delivery.

- Operating Systems – This includes access to, and configuration and maintenance of, the environment in which the application is installed.

- Hardware and Network – The technology infrastructure, including servers and network devices, that the application uses to operate and provide services to the customer.

- Disaster Recovery – The backup and recovery of data and information systems in the event of a disruption of service.

- Physical Security – The operation and security of the physical facilities housing the hardware and network the application uses to operate.

N.J.S.A. 52:18A-224 through 52:18A-234, known as "The Office of Information Technology Reorganization Act", gives authority and responsibility to the OIT, under the direction of the Chief Technology Officer (CTO), to provide and maintain the information technology infrastructure of the executive branch of state government, including all ancillary departments and agencies. All executive branch departments and state agencies are directed to cooperate fully with the OIT and the CTO to implement the policies and procedures.

When reviewing SaaS providers and products in the executive branch, we categorized the process into three areas: acquisition, performance and monitoring, and security.

Acquisition

The acquisition process for SaaS products is a combination of OIT review and approval and the Division of Purchase and Property (DPP) procurement process governed by a joint circular for information technology procurement. Agencies procuring SaaS products should follow all applicable laws and procurement requirements, complete the required System Architecture Review process documents for the OIT, and ensure that SaaS providers complete the state's Third-Party Information Security Questionnaire. This questionnaire is used as a risk assessment tool for third parties with access to state information assets.

SaaS products can be purchased in multiple ways, including the standard competitive bidding process, delegated purchase authority, or through a waiver of advertising if the purchase meets certain requirements. However, the most common method for SaaS purchases is through an approved reseller that offers many SaaS products from multiple providers. If the SaaS product either stores or allows the provider to access state data, or the product manages a critical state

business function, the purchasing agency must create a custom agreement with the software provider. Custom agreements must include security language as well as technology-level performance expectations.

Performance and Monitoring

The performance of a SaaS product is the responsibility of the provider, while monitoring of that performance is the responsibility of the using state department or agency. SaaS contracts must include provider technical responsibilities, including an uptime guarantee, and provide advance notice of any upgrades or maintenance that may impact service availability and performance. The SaaS provider and the agency should determine any additional service-specific metrics that should be made available to assist in the monitoring process.

Security

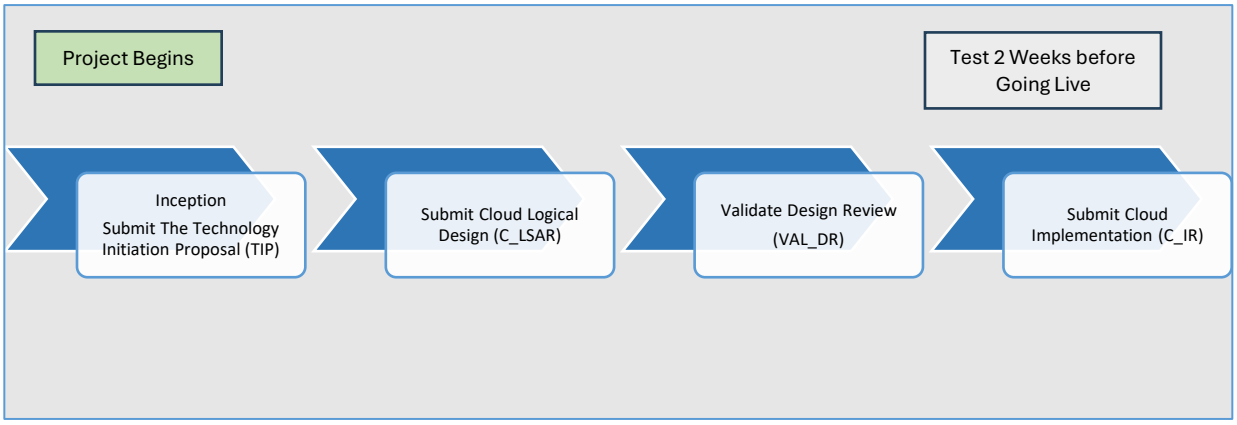
Cybersecurity risk identification and mitigation are a shared responsibility between the OIT, the OHSP, and state departments and agencies. The OIT and the OHSP are primarily responsible for policy setting and review, while state departments and agencies are responsible for implementation. SaaS providers that are seeking to do business with the state are required to complete a security questionnaire, which identifies the security frameworks they follow or controls they implement to protect sensitive data. Providers are required to maintain an incident reporting plan that includes preparation, detection, analysis, containment, recovery, and reporting activities. Providers may also be required to have third-party audits conducted addressing system and organizational controls to ensure continued security compliance.

System Architecture Review Process

Agencies are not consistently completing the System Architecture Review process when implementing SaaS solutions.

According to OIT State of New Jersey Technology Circular No. 16-05-NJOIT, a System Architecture Review (SAR) is required to ensure that technology solutions for the state are conceived, designed, developed, and deployed to maximize the benefits and functionality of those solutions. The review also ensures compliance with cybersecurity and architecture standards and monitors the introduction of new technologies. The SAR process is required for new SaaS solutions, enhancements, or modifications, as well as migration of an on-premises product to a SaaS version of the same product.

There are four phases to the solution, each requiring a document submission:



SAR Phases within the System Development Lifecycle

Each of these submissions is reviewed by various areas of OIT and OHSP in conjunction with the agency:

System Architecture Review Process

Phase	Description
Technology Initiation Proposal Review (TIP)	This review is performed before any RFP is generated. It involves a high-level discussion between the agency and the OIT. Included in the review are the scope of the initiative, the asset classification, and the technological and infrastructure requirements of the initiative.
Cloud Logical System Architecture Review (C_LSAR)	This review is performed before any software is procured or installed. The review determines: the system information, data type, and interfaces; authentication and user access methods; bandwidth usage/business transaction volume; security and data privacy; and cybersecurity requirements.
Validate Design Review (VAL_DR)	The complete system design is presented and approved. Design consists of the system components and the data that is shared between SaaS provider and the state, including the method of data transport.
Cloud Implementation Review (C_IR)	This phase verifies that all open action items from previous SAR meetings have been addressed, and all essential steps have been completed. Also, ensures all cybersecurity requirements have been successfully tested.

Our test of 12 active SaaS products throughout the executive branch included determining what phase of the SAR process was completed before the solution was implemented. Below is a summary of the test:

SaaS Product Sample

Phase	1	2	3	4	5	6	7	8	9	10	11	12
TIP	■	■	■	■	■	■	■	■	■	■	■	
C_LSAR	■	■		■	■		■	■				
VAL_DR	■	■	■	■	■	■						
C_IR	■	■	■									

■ = **Phase Completed**

Our testing disclosed that agencies are not completing all the steps in the SAR process before implementing the SaaS product.

- Only two of the products we tested completed all four phases of the SAR process.
- An additional product did complete the C_IR; however, we could not find evidence of a C_LSAR taking place. Because the C_IR phase verifies that all open action items from previous SAR meetings have been addressed and all essential steps have been completed, this missing step should have been caught at the C_IR phase.
- One product had the VAL_DR phase, but not the preceding C_LSAR phase.
- Three products only completed the TIP phase.
- One did not complete any steps in the process.

As noted on the previous page, procurements should not be made until after the C_LSAR phase has been completed; however, at least four projects were implemented without going through that phase.

Departments and agencies are responsible for moving their technological solutions through the SAR process. Discussions with OIT management confirmed that agencies do not always complete all phases in the process despite the requirements in the Technology Circular. The OIT stated that once an agency obtains procurement approval, they decide not to complete the rest of the SAR process, and the OIT loses leverage to enforce completion of the process because the agency can start procuring the product.

The OIT can waive a project through one or more phases of the SAR process on a case-by-case basis; however, none of the SaaS solutions in our sample had any evidence that a phase had been waived. As more state agencies acquire SaaS products, skipping all or part of the SAR process increases the risk that compliance with cybersecurity and architecture standards will not be met.

Recommendation

We recommend the OIT enforce the SAR process with agencies, particularly the requirement of the C_LSAR completion before procurement approval is granted. In addition, the OIT should develop criteria for waiving a SaaS product through phases of the SAR process and document all such waivers.

Disaster Recovery Documentation

Contracts with SaaS providers do not require disaster recovery documents to be provided at defined intervals.

The purpose of contingency planning is to minimize the risk of system and service unavailability from a variety of disruptions by providing effective and efficient solutions to enhance system availability. Contingency planning consists of technical and operational aspects. The technical aspects (disaster recovery) are the processes connected to backing up and restoring an information technology system to a ready state with minimal loss of time, functionality, and data. The operational aspects (business continuity) are the processes and procedures that are used to put the agencies' employees and customers in a position to resume normal operations.

The *SISM* states that agencies are responsible for contingency planning and operations for their systems in coordination with the OIT. This includes initial review and approval of the plans by the agency and OIT management, as well as annual review of the plans. In addition, the *SISM* defines the required contents of the plan, including the requirement to test the plan at defined intervals to determine effectiveness and address any issues. In the case of SaaS products, agencies are still responsible for business continuity of their operations in the event of a disruption; however, disaster recovery planning for the product lies with the provider since they are managing the infrastructure.

The 12 SaaS contracts we reviewed do not explicitly have a requirement for providers to submit their disaster recovery plans and/or plan test results to the agencies at defined intervals. Our review found inconsistent SaaS contract language related to disaster recovery plans:

- Two contracts required the submission of an initial disaster recovery plan but did not require the submission of updates or test results.

- Nine contracts had language stating only that the disaster recovery plan is to be provided "upon request" from the agency.

- One contract did not require disaster recovery planning documents at all. During our testing, the agency was unable to provide us with the documents because the SaaS provider did not have them when asked.

The OIT should hold SaaS providers to the same standards as internal systems and require that they submit their initial disaster recovery planning documents to the agency for review and then provide either updated plans or plan test results and corrective action on a defined basis. The absence of a disaster recovery plan exposes providers and the state to various risks, including service disruptions to the public, financial losses, operational disruptions, security breaches, compliance violations, and decreased resilience. Without these plans in place, providers may struggle to recover from unforeseen events, leading to prolonged downtime, loss of critical data, and potential reputational damage.

Recommendation

We recommend the OIT modify the contract language regarding disaster recovery planning documents to require them at defined intervals, such as when a plan is updated or after a test is conducted.

Service-Specific Key Performance Indicators

Service-specific key performance indicators (KPIs) are not being defined for all SaaS products.

KPIs are a set of quantifiable, measurable benchmarks used to gauge a SaaS provider's overall performance of, and compliance with, contractual obligations. There are multiple categories of KPIs that can be developed, including financial, customer experience, process performance, sales, and information technology. Performance metrics help compare expected performance with actual performance. These metrics help to hold the provider accountable for the delivery of quality services.

All state SaaS product contracts include a supplement that defines provider terms and conditions. The supplement defines the components of a Service-Level Agreement (SLA), which include service-level performance promises (i.e., metrics for performance and intervals for measurement), description of service quality, identification of roles and responsibilities, security controls, dispute resolution, and remedies for performance failures. Although the supplement does cover data protection, security responsibilities, and uptime requirements, other performance measures specific to the service provided should also be defined in the SLA between the provider and the department or agency.

Our test of the twelve SaaS products found that four did not have an SLA for the product, and an additional four had SLAs that did not have service-specific KPIs included. Of those eight contracts, six of the agencies described performance monitoring activities that they perform. However, defining the KPIs in an SLA ensures that the expectations of both the provider and the state are aligned. Agencies are responsible for reviewing and approving the SLA to ensure that it includes everything necessary to address all their business needs. The OIT is required to review and approve the SLA; however, its review is currently limited to information technology-related items only.

The absence of an SLA or service-specific KPIs within an SLA could result in misaligned expectations between the provider and the state, operational inefficiencies, and accountability gaps. Further, without defined performance measures, the state may not be able to assess performance and identify issues.

Recommendation

We recommend the OIT reinforce with agencies the importance of having an SLA that defines necessary service-specific KPIs for SaaS products. In addition, the OIT should expand its review of the SLA to determine if service-specific KPIs are included in the SLA and, if not included, inquire with the agency to ensure the agency addressed the issue.

Appendix

Methodologies to Achieve Audit Objectives

We surveyed state departments and agencies to identify and obtain information about SaaS products in use. We developed criteria to assist the survey recipients in identifying SaaS products in their environment. In addition to the aspects of a SaaS product's acquisition, performance and monitoring, and security requirements, the survey asked for only SaaS products that hold state data or manage a critical state business function. The survey results identified a total of 228 SaaS products in use that met our criteria. From this total population, we judgmentally sampled 12 products from a cross-section of agencies based on total cost, contract age, sensitivity of data, and whether a known data breach against the provider existed.

In addition to the procedures outlined in the findings, we performed the following audit procedures to reach our conclusions:

Acquisition

To determine whether agencies implement effective acquisition practices over third-party SaaS providers, we documented and evaluated whether contracts were properly approved during the acquisition process and they included provisions for the right to audit, storage of data, roles and responsibilities, and required disclosures of conflict of interest.

Performance and Monitoring

To determine whether agencies implement effective performance and monitoring practices over third-party SaaS providers, we documented and evaluated whether contracts were properly monitored, determined whether providers advised state agencies regarding software updates, and verified whether there were any protests or complaints made about the provider.

Security

To determine whether agencies implement effective security measures over third-party SaaS solutions, we documented and evaluated whether those providers completed the third-party information security questionnaire and determined whether the agencies properly reviewed third-party security audits or reports, such as system and organization controls or international organization for standardization.

To determine whether agencies are being notified by the providers when there are cybersecurity incidents and data breaches that affect state data or operations, we documented and evaluated whether the providers adhered to the security incident and breach of security responsibilities provision in their contracts.

To determine whether providers are adhering to risk-mitigation requirements when the provider has access to state data or manages critical processes, we documented and evaluated whether contracts included provisions requiring providers to maintain a cyber breach insurance of $2 million or higher to mitigate financial risks associated with data breaches and data confidentiality requirements.

State of New Jersey

PHILIP D. MURPHY
Governor

TAHESHA WAY
Lt. Governor

Office of Information Technology
P.O. Box 212
Trenton, New Jersey 08625-0212

CHRISTOPHER J. REIN
Chief Technology Officer

September 3, 2025

Mr. David J. Kaschak
State Auditor
Office of Legislative Services
Office of the State Auditor
PO Box 067
Trenton, NJ 08625-0067

Re: Executive Branch Software-as-a-Service (SaaS) Audit

Dear Mr. Kaschak:

Regarding your audit of the Executive Branch Software-as-a-Service (SaaS) at the Office of Information Technology (OIT), we appreciate the Office of the State Auditor's (OSA) thorough review and are encouraged by the overall conclusion, particularly the confirmation that the OIT has adequate controls in place and that executive branch agencies are complying. These results reflect our ongoing commitment to governance and oversight of SaaS products across the state. We acknowledge the noted opportunities for improvement and will take them into consideration as part of our continuous improvement efforts. In that regard we would like to provide the following comments on the OSA's recommendations made via audit report dated August 28, 2025 covering the period February 1, 2024 to March 31, 2025:

System Architecture Review Process:

OIT acknowledges the importance of ensuring full adherence to the System Architecture Review (SAR) process and appreciates the recommendation. We recognize that consistent completion of all SAR phases is essential to maintaining architectural integrity and cybersecurity standards, particularly as the use of SaaS solutions continues to grow across state agencies. We will evaluate our current enforcement mechanisms and work with all involved agencies to develop a plan to strengthen compliance prior to procurement approval. Additionally, we will establish formal criteria and documentation procedures for SAR process waivers to enhance transparency and accountability.

Disaster Recovery Documentation:

OIT agrees with the importance of strengthening disaster recovery planning requirements for SaaS providers. We recognize that holding external providers to the same standards as internal systems is essential to safeguarding service continuity, data integrity, and public trust. In response to this recommendation, going forward we will work with the relevant agencies involved to review and update relevant contract language to require the submission of disaster recovery plans, test results, and any corrective actions on a defined and recurring basis. This will help ensure appropriate oversight and improve overall resilience.

Service-Specific Key Performance Indicators:

OIT agrees that clearly defined, service-specific Key Performance Indicators (KPIs) are valuable tools for setting expectations and measuring the effectiveness of SaaS solutions. We will reinforce with agencies the importance of including such KPIs in their Service Level Agreements (SLA) to promote alignment between business needs and provider responsibilities and enhance our online workflow to do so. While agency requirements and provider capabilities may vary, we will make a best effort to expand our SLA review process to include the presence of service-specific KPIs and, where they are not present, engage agencies in follow-up to ensure performance expectations are appropriately addressed.

Finally, we appreciate the cooperative way you and your staff conducted this audit. Your recommendations are well regarded as OIT is committed to continual improvement. If you have any further comments, please contact Stephen Foundos at 609-376-7056. Mr. Foundos will be available to expedite any communications throughout OIT.

Sincerely,

Christopher J. Rein
Chief Technology Officer

cc: Lisa Blauer, Chief of Staff
Stephen Foundos, Auditor