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

Division of State Government Accountability

Disaster Recovery Planning

Office of Information Technology Services

Report 2016-S-97 December 2017

Executive Summary

Purpose

To determine whether the Office of Information Technology Services (ITS) has a complete, functional, and tested disaster recovery plan for its agency and the College of Nanoscale Science and Engineering (CNSE) data center. The audit covers the period January 2017 through June 2017.

Background

ITS was established in November 2012 as part of a New York State Information Technology (IT) Transformation to consolidate and merge State agencies' operations and streamline services. ITS is responsible for providing centralized IT services to 46 executive State agencies, as well as setting statewide technology policy for all executive branch State agencies and monitoring large technology expenditures in the State. ITS also operates a statewide data center at the CNSE.

To ensure continued operation of critical State systems, ITS should have a complete, functional, and tested disaster recovery plan that covers all aspects of its operations, including the CNSE data center and the centralized IT services it provides to the 46 executive agencies. That plan should comply with State laws and ITS policies and should also conform to guidance issued by the National Institute of Standards and Technology (NIST).

Key Findings

- ITS has made some efforts toward disaster recovery planning; however, there is not a complete, functional, and tested disaster recovery plan that covers all aspects of its operations, including the CNSE data center and the centralized IT services it provides to the 46 executive agencies.
- ITS is working on completing a disaster recovery plan for the CNSE data center and anticipates it will be done in late 2018.

Key Recommendations

- Finalize the NYS Disaster Recovery Project: Disaster Recovery Draft Plan in accordance with ITS policies, NIST, and other relevant guidance.
- Ensure the finalized NYS Disaster Recovery Project: Disaster Recovery Draft Plan covers ITS' own operations, including but not limited to the centralized IT services it provides to the 46 executive agencies.
- Review the disaster recovery plan regularly, documenting changes needed and when those changes were made.

Other Related Audits/Reports of Interest

Office of Information Technology Services: Security and Effectiveness of Division of Criminal Justice Services' Core Systems (2014-S-24)

Office of Information Technology Services: Effectiveness of the Information Technology Transformation (2015-S-2)

Office of Information Technology Services: Security and Effectiveness of Division of Criminal Justice Services' Core Systems (Follow-Up) (2016-F-28)

State of New York
Office of the State Comptroller

Division of State Government Accountability

December 6, 2017

Mr. Robert H. Samson
Chief Information Officer
Office of Information Technology Services
Empire State Plaza
P.O. Box 2062
Albany, NY 12220

Dear Mr. Samson,

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 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 *Disaster Recovery Planning*. 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 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: Brian Reilly
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 Information Technology (IT) Transformation to consolidate and merge State agencies' operations and streamline services. ITS is responsible for providing centralized IT services to 46 executive State agencies, with the awareness that citizens are reliant on those services. ITS sets statewide technology policy for all State agencies, and monitors all large technology expenditures in the State, seeking efficiencies, lower costs, and innovative solutions. ITS is organized into clusters, each of which supports a group of related State agencies. ITS also operates a statewide data center at the College of Nanoscale Science and Engineering (CNSE). As of June 2017, 27 separate data centers have been consolidated into the CNSE data center, and ITS anticipates another 20 will be moved there. ITS operates a single backup data center for the CSNE data center that is geographically distant from CNSE. According to ITS officials, the majority of applications and data in the CNSE data center are backed up at their designated site, and the data in critical applications can be fully restored from that location. Officials noted not all systems, applications, and data within CNSE are critical or backed up in their designated backup site. ITS is also responsible for another six smaller data centers that are not being moved into the CNSE data center and are not backed up to ITS' designated backup site.

Disaster recovery plans are intended to help an entity restore mission-critical operations after a natural or man-made disaster. ITS has issued New York State Information Technology Policy P03-002 (Information Security Policy), which includes guidance for State agencies in developing disaster recovery plans. In addition, the National Institute of Standards and Technology (NIST) has issued its Contingency Planning Guide for Federal Information Systems (NIST Special Publication 800-34, Revision 1) – another primary source of guidance for developing disaster recovery plans.

Audit Findings and Recommendations

ITS does not yet have a complete, functional, and tested disaster recovery plan that covers all aspects of its operations, including the CNSE data center and the centralized IT services it provides to the 46 executive agencies. ITS has created a centralized repository of information for its employees to use when restoring select IT systems in their Continuity of Operations Plan. We were provided the NYS Disaster Recovery Project: Disaster Recovery Draft Plan for the CNSE data center, which ITS officials anticipate being finalized in late 2018. As part of that effort, ITS is in the process of developing and testing application-specific disaster recovery plans for the 24 most critical applications located at the CNSE data center, and has completed two of those.

Disaster Recovery Planning by ITS

ITS officials have, on several occasions, acknowledged their responsibility for developing, implementing, and testing disaster recovery plans as the primary IT support for many State agencies. However, they have made inconsistent and conflicting statements about the need for and existence of disaster recovery plans. During previous audits of ITS, officials stated they had a disaster recovery plan, although they never provided one to our auditors. In November 2016, in response to our audit of the IT Transformation (Report 2015-S-2, issued August 2016), ITS officials stated they had a project underway that "supports the development of disaster recovery plans." In this current audit, officials have provided us with a draft disaster recovery plan for the CNSE data center, which they anticipate taking about 18 months to complete. However, officials also stated that disaster recovery is a "fluid concept" and "any plan to thwart and recover from a disaster must always be evolving to reflect the latest information, thinking, strategizing and planning."

The New York State Technology Law (Technology Law) Article I, Section 103 (12-a)(d) states that ITS shall develop formal disaster recovery plans for the State data center and statewide network, NY e-net; and such plans shall be confidential. In addition, ITS issued an Information Security Policy, last updated March 2017, which is intended primarily to ensure the confidentiality, integrity, and availability of State data, but also addresses contingency plans. These plans include business continuity plans and continuity of operations plans as well as disaster recovery plans. According to the Information Security Policy, disaster recovery plans must be established and tested regularly. Such plans must, at a minimum, have an evaluation of the criticality of each system, as well as the expected time frame and allowable age of backup data to be used for restoration. To that end, State information, software, and system images should be backed up regularly, and those backups tested in accordance with the parameters outlined in the respective disaster recovery plan.

The Information Security Policy does not specify who is responsible for developing disaster recovery plans for the systems ITS supports, although it does state that ITS is responsible for implementing any such plans. In January 2017, during our initial meeting with ITS officials on this audit, they informed us that State agencies would be responsible for developing their own disaster recovery plans while ITS would be responsible for implementing those plans. ITS officials did acknowledge their responsibility for developing disaster recovery plans for its own operations,

which includes the centralized IT services it provides to the 46 executive agencies.

As noted previously, the Technology Law requires ITS to develop a formal disaster recovery plan for the State data center. As such, ITS should have a disaster recovery plan in place to cover both its own operations as well as the CNSE data center.

In a previous audit (Report 2014-S-24, issued February 2015), we recommended that ITS establish cluster-level backup and recovery policies. However, in a recent follow-up to that audit (Report 2016-F-28, issued April 2017), we determined no such policies were in place, although ITS was working on a disaster recovery plan for one of its client agencies (the Division of Criminal Justice Services). According to ITS officials, a comprehensive disaster recovery plan for that cluster (and by extension all ITS clusters) is on hold, pending development of a statewide disaster recovery strategy, although they did not provide an estimate of when that would be finalized.

In March 2017, we were given the NYS Disaster Recovery Project: Disaster Recovery Draft Plan (Disaster Recovery Draft Plan) for the CNSE data center, which ITS officials estimated would take 18 months to finalize. Because this plan is still in draft, we did not determine whether it is in compliance with State laws, ITS policies, or the guidance in NIST Special Publication 800-34, Revision 1. As part of this effort, ITS has identified 24 critical applications housed at the CNSE data center that require their own disaster recovery plans. As of June 2017, ITS had developed and tested 2 of the 24 application-specific disaster recovery plans. We were also shown some documentation that ITS employees could use to restore systems, applications, or data lost due to a disaster. This information is stored on a secure electronic server with access restricted to those employees who would be responsible for responding to a disaster. In response to our preliminary findings, ITS officials stated that ITS has ensured the new data center and its associated backup site are prepared for and can withstand an array of the most likely threats and disasters. However, we did not test those efforts as they were not part of our audit scope.

On several occasions, ITS officials informed us that a disaster recovery plan is a living document, one that needs to be constantly revised for changes in the IT environment. Advances in technology, changing needs of the client agencies supported by ITS, and even upgrades of and replacements for critical applications used by the agencies will all impact a disaster recovery plan. While we agree that a disaster recovery plan needs to be regularly updated, it is insufficient justification for ITS to go nearly five years since its creation without developing a formal disaster recovery plan for its own operations. This also does not justify ITS' failure to develop a formal disaster recovery plan for the CNSE data center, as required by State law.

Without a finalized disaster recovery plan in place, there is neither a place to record what changes are needed nor any way to ensure those changes are adequately addressed. Most critically, without a finalized disaster recovery plan in place, ITS officials cannot guarantee that they would be able to restore critical State systems, applications, or data timely in the event of a disaster.

Recommendations

1. Finalize the NYS Disaster Recovery Project: Disaster Recovery Draft Plan in accordance with ITS policies, NIST, and other relevant guidance.

2. Ensure the finalized NYS Disaster Recovery Project: Disaster Recovery Draft Plan covers ITS' own operations, including but not limited to, the centralized IT services it provides to the 46 executive agencies.

3. Review the disaster recovery plan regularly, documenting changes needed and when those changes were made.

Audit Scope, Objective, and Methodology

The objective of our audit was to determine whether ITS has a complete, functional, and tested disaster recovery plan for its agency and for the CNSE data center. The audit covers the period January 1, 2017 through June 21, 2017.

To accomplish our audit objective and evaluate the relevant internal controls, we reviewed on-site documentation that ITS is developing and using as support of its disaster recovery project and also reviewed the draft disaster recovery plan for the CNSE data center. In addition, we interviewed ITS officials to learn more about their disaster recovery plan. We conducted on-site visits of the CNSE data center as well as the backup site.

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 threats to 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

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.

Reporting Requirements

A draft copy of this report was provided to ITS officials for their review and comment. We considered their comments in preparing this final report, and they are attached in their entirety at the end. In their response, ITS officials disagree with the audit's recommendations. This concerns us, and in fact, we are disappointed with the response. As noted in the response, ITS and OSC staff met to discuss the draft report's findings and recommendations. As a result of the meeting, OSC made certain revisions to the draft report based on the appropriateness of the additional evidence offered. On March 30, 2017, OSC and ITS management met and ITS management provided a copy of the NYS Disaster Recovery Project: Disaster Recovery Draft Plan (Disaster Recovery Draft Plan). ITS officials estimated this plan to be completed in late 2018. In fact, they proposed that ITS and OSC staff meet regularly during those 18 months: an initial meeting to discuss what ITS plans to do and then quarterly until the plan is finalized. At the completion, OSC could issue a report stating whether ITS met its targets and whether the final plan is in compliance with NIST standards. We declined as this would impair our audit independence.

As part of this Disaster Recovery Draft Plan, ITS identified 24 critical applications housed at the CNSE data center that require their own disaster recovery plans. As of June 2017, ITS had developed and tested only 2 of the 24 application-specific disaster recovery plans. However, as they have done throughout this audit, ITS officials insist that they have a disaster recovery plan in place. Nowhere in the response does ITS reference this Disaster Recovery Draft Plan – they only state that ITS has "long had a formal plan and strategy for disaster recovery" and, further, that "this ITS plan and strategy has been finalized" but do not define what plan they are referring to. The response continues the pattern of avoidance and misdirection we have seen from ITS officials in this and other audits. As a result, it is difficult to discern what type of disaster recovery plan ITS has now finalized and what it actually encompasses.

Within 90 days after the final release of this report, as required by Section 170 of the Executive Law, the Chief Information Officer of the Office of Information Technology Services 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 where the recommendations were not implemented, the reasons why.

Contributors to This Report

Brian Reilly, CFE, CGFM, Audit Director
Nadine Morrell, CIA, CISM, CGAP, Audit Manager
Jennifer Paperman, CPA, Audit Supervisor
Kathy Garceau, Examiner-in-Charge
Jared Hoffman, OSCP, GPEN, GWAPT, IT Specialist IV
Holly Thornton, CISA, CFE, Examiner-in-Charge
Patrick Lance, Senior Examiner
Lisa Whaley, Staff Examiner
Mary 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

Ken Shulman, Assistant Comptroller
518-473-0334, kshulman@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

Office of Information Technology Services

ANDREW M. CUOMO
Governor

ROBERT SAMSON
Chief Information Officer

September 27, 2017

By electronic and first class mail

Brian Reilly
Office of the State Comptroller
110 State Street, 11th Floor
Albany, New York 12236

Re: *ITS Response to Disaster Recovery Planning Draft Report 2016-S-097*

Dear Mr. Reilly:

The Office of Information Technology Services ("ITS") has received and reviewed "Disaster Recovery Planning Draft Report 2016-S-097," the draft report of the findings of the Office of the State Comptroller ("OSC") related to its audit of ITS disaster recovery planning (the "Draft Report"). ITS writes to provide the following feedback and information to ensure that OSC has a full and complete picture of the agency's disaster recovery planning efforts.[1] In addition, after a comprehensive review of the Draft Report, ITS contacted OSC to schedule a conference to discuss the report finding and recommendations. As a result of the meeting, OSC made certain modifications to the Draft Report based on the appropriateness of the additional evidence offered.

* Comment 1

Background

ITS was established in 2012. Over the past 4.5 years, ITS has focused on resiliency, security, business continuity and disaster prevention and recovery. Of relevance to the Draft Report, one of ITS's core initiatives is to enhance and stabilize the State's ability to prevent and, if needed, recover from, an interruption in its ability to provide critical information technology ("IT") related services to citizens. These considerations have been the consistent focus and common threads underlying ITS' multi-phase,

[1] To allow OSC to understand that full and complete picture, ITS shared material and documents with OSC certain details of which, for security reasons, ITS cannot disclose in this response; material disclosed in this response is therefore not necessarily reflective of the full scope of ITS' disaster recovery capabilities and planning.

P.O. Box 2062, Empire State Plaza, Albany, NY 12220 | (518) 408-2140 | https://its.ny.gov

*See State Comptroller's Comments, page 15.

multi-year effort to consolidate and transform IT assets, resources, infrastructure, and service delivery across more than forty-five executive agencies.

To achieve this level of resiliency and security, one of ITS' primary – and continuing – missions is to consolidate agencies' disparate data centers into a world-class data center to ensure high availability and benefit from the manifold protections that such a data center can offer. One of ITS's first accomplishments was an agreement with the State University of New York to move the State's IT infrastructure into a tier three plus data center at the College of Nanoscale Science and Engineering ("CNSE") in Albany. ITS then built a geographically diverse backup data center to ensure that critical data is highly available in the event of an interruption.

ITS will complete the consolidation of agencies' disparate data centers into its data center at the CNSE in 2017. The data of identified critical applications in the CNSE is replicated in the geographically diverse backup data center. These moves have reduced, and will continue to significantly reduce, the physical and environmental risks that the previous data centers posed to the state IT infrastructure. As a result, ITS has fundamentally modernized and rebuilt the State's overall IT security posture and resiliency, heightening its ability to avoid and recover from major interruptions.

Disaster Recovery Overview

An analysis of ITS's disaster recovery efforts must include an understanding that "disaster recovery" is a fluid concept; IT evolves, and threats to IT evolve with it. A robust and documented disaster recovery strategy, with associated processes for restoration and recovery of systems and data that are updated when appropriate, are essential. However, the dangers posed by a large-scale interruption or "disaster" are constantly evolving, and as ITS continues its many efforts to protect the integrity of the State's IT infrastructure, ITS must also evolve and progress. Accordingly, while ITS has finalized its disaster recovery planning and strategy, and consistently challenges and tests its planning and strategy, ITS' responsible efforts to thwart and recover from a disaster must always be evolving to reflect the latest information, thinking, strategizing and planning. This is ITS's mission, and ITS devotes significant resources to ensuring the protection of the State's critical information.

It is abundantly clear that ITS has made disaster recovery planning a priority – in fact such planning was the very reason for the creation of ITS. ITS has since made significant investments and taken critical steps toward disaster preparedness, mitigation and avoidance, and system resiliency, availability and recovery. In so doing, ITS has enhanced the ability of the State to maintain business continuity in the event of a disaster or major interruption. ITS' final plan and strategy, consistent since formation and in recognition of the above facts, is to: (i) avoid, (ii) mitigate, and (iii) recover from disasters and major interruptions. Virtually all of the actions ITS takes every day to build and remediate systems are designed to operationalize and advance this strategy.

ITS has demonstrated and documented its achievements in modernizing the State's resiliency and redundancy, and such measures should provide increased confidence in restoration of critical systems and in business continuity capabilities, particularly when compared to the pre-transformation status of systems, applications and data centers. As set forth below, it is against this backdrop of milestones and achievements, borne out by ITS' consistent, underlying focus on prevention and avoidance of disasters or major interruptions in the ability to provide IT services, that ITS must be evaluated.

Disaster Recovery Milestones

ITS has achieved the following major business continuity, resiliency and recovery milestones, all of which will be of critical importance during any major interruption or disaster event:

- Substantial and ongoing consolidation into tier three plus world-class data center at CNSE;
- A geographically diverse backup data center;
- Redundant recovery for essential statewide communications systems;
- Redundant recovery for the State's essential work papers;
- Redundant recovery for the State's employee identity stores; and
- Redundant recovery for the State's major IT infrastructure.

Of note, ITS was, and continues to be, completely focused on system integrity, availability, and disaster recovery when designing the entire data center migration and consolidation plan, which includes the geographically diverse backup site, as well as the many redundant services which have been integral to ITS service offerings for years. The tier three plus ITS data center located at the CNSE represents a significant investment in disaster avoidance and recovery – indeed, it is the most significant investment in disaster recover the State has made. ITS has built and consistently invested in a data center facility capable of maintaining the integrity of New York State IT infrastructure, and ensuring business continuity.

Moreover, in the event a disaster capable of taking the CNSE tier three plus data center off-line, ITS has redundancy built into the State's IT infrastructure through the geographically diverse backup site. At the backup site, ITS is capable of restoring full performance of such systems from that location. Indeed, recently ITS recovered from a total power shutdown in this facility and restored and recovered all functionality within one business day. This is a remarkable achievement, as prior to transformation no such geographically diverse recovery location existed for agencies now served by ITS. This will enable full communications internally within government and with citizens, even during a critical disaster completely taking out the CNSE data center.

* Comment 2

Not all disasters are total, however. The risk of a full data center loss is not nearly as great as the risk of losing individual legacy systems, applications, or environments. Recognizing this, ITS invested

its resources accordingly. ITS has mitigated a great deal of risk, implemented significant disaster planning, and achieved greater resiliency and business continuity through the successful migrations of agency systems on servers in fragile physical environments such as closets and hallways around the State, to the CNSE. Additionally, ITS realized the benefits of its successful strategic planning and investments when it successfully defended all State systems for which it has responsibility from a recent global ransomware event in the news; while several Fortune 50 corporations were impacted, ITS-supported systems were not. This is a testament to the State's disaster preparedness.

ITS Response to Audit Findings

ITS disputes the Key Finding in the Executive Summary section of the Draft Report, and the Audit Finding in the Draft Report. OSC states that "ITS does not yet have [a] complete, functional and tested disaster recovery plan" for ITS, the agencies it supports and the CNSE datacenter, and finds that "there are no formal procedures in place to ensure that [] systems are restored timely." OSC also finds that ITS has "failed to develop a formal disaster recovery plan" and has "go[ne] nearly five years . . . without developing [a] formal disaster recovery plan." This is incorrect and inconsistent with the documents and information ITS shared with OSC during the course of this audit. ITS has long had a formal plan and strategy for disaster recovery, including documented processes for implementing recovery and restoration of key systems; OSC auditors directly reviewed hundreds of pages of original documentary evidence provided by ITS that document ITS's disaster recovery plan, its continuity of operations plan, and its business continuity plan.[2]

* Comment 3

Of significance, ITS' strategy, plan and processes are working: as noted above, in a recent situation involving the total power shutdown of the State's backup datacenter, ITS restored to function all systems and applications in production there within one business day due to the standards and procedures ITS has in place to minimize disruption in just such an event. This ITS plan and strategy has been finalized, and ITS will review the plan as needed and will certify the plan annually, in accordance with best practices.

ITS also disputes OSC's statement in the Draft Report that ITS "informed [OSC] that State agencies would be responsible for developing their own disaster recovery plans while ITS would be responsible for implementing those plans." This is incorrect. ITS informed OSC that its partner agencies, as the business owners and those most knowledgeable about their systems and applications requiring continuity in a disaster, are responsible for developing their own continuity of operations and business continuity plans if those systems and applications are impacted by a service interruption. While those agency plans are a critical component of an overall statewide strategy for maintaining continuity of

* Comment 4

[2] OSC states that in a recent follow-up audit of IT systems at DCJS, it learned that disaster recovery at DCJS (and all "clusters") is "on hold, pending the development of a statewide disaster recovery strategy." This is a misunderstanding of the information provided and is not true. DCJS systems, and all critical systems ITS supports, are included in the ITS final disaster recovery plan.

operations through interruption, ITS' agency partners are not responsible for developing a disaster recovery plan for their IT applications and systems. Rather, ITS is responsible for IT disaster recovery planning, and accordingly has disaster recovery plan covering such systems and applications. Lastly, if the testimonial evidence provided by ITS was not sufficient or appropriate to reach a reasonable and accurate conclusion on this or any point, ITS would have provided, if asked, stronger evidence to support it.

ITS Response to Recommendations

OSC recommends that ITS finalize its disaster recovery plan. ITS disagrees with this recommendation, as it has already finalized its disaster recovery plan, protocols, and procedures, subject to review, change, and certification, as described herein.

OSC recommends that ITS develop and maintain a disaster recovery plan that covers the CNSE, ITS, and the services ITS provides to its client agencies. ITS disagrees with this recommendation, as ITS has already finalized its disaster recovery plan, subject to review, change, and certification as described herein. Further, ITS provided OSC with access to the ITS comprehensive continuity of operations and business continuity plans.

OSC recommends that ITS review the disaster recovery plan regularly and document changes. ITS partially agrees with this recommendation. This is already ITS' current practice and ITS will continue to review the plan as needed, and on an annual basis, consistent with best practices.

Please do not hesitate to contact the ITS Director of Internal Audit, Rajni Chawla, at (518) 457-5465, should you require anything further.

Very truly yours,

Robert Samson
NYS Chief Information Officer

RS/amd

P.O. Box 2062, Empire State Plaza, Albany, NY 12220 | (518) 408-2140 | https://its.ny.gov

State Comptroller's Comments

1. We made certain revisions to the draft report based on the appropriateness of the additional evidence offered.
2. As previously noted, according to ITS officials, the majority of applications and data in the CNSE data center are backed up at their designated site, and the data in critical applications can be fully restored from that location. However, officials did note that not all systems, applications, and data within CNSE are critical or backed up in their designated backup site. ITS is also responsible for another six smaller data centers that are not being moved into the CNSE data center and are not backed up to ITS' designated backup site.
3. On March 30, 2017, we met with the ITS executive management team. At that meeting, ITS executive management provided us with the NYS Disaster Recovery Project: Disaster Recovery Draft Plan, which they told us would take 18 months to finalize. Until it is finalized, ITS does not have a "complete, functional and tested disaster recovery plan," as we state in our report. In addition, ITS officials repeatedly state they have always had disaster recovery planning in place. Yet, in a meeting after our closing conference, an ITS official explicitly stated that the agency had done nothing in regard to developing a disaster recovery plan during the first two years after it was created.
4. Once again, ITS officials are presenting conflicting information. At our initial meeting with ITS on January 11, 2017, ITS executive management informed us that business continuity, continuity of operations, and disaster recovery would be developed by the agencies, and that ITS would execute disaster recovery. Further, ITS' own Information Security Policy (last updated in March 2017) explicitly states that IT management is responsible for "implementing business continuity and disaster recovery plans." Despite this, later in the audit, as noted previously, we received the NYS Disaster Recovery Project: Disaster Recovery Draft Plan in which ITS identified 24 critical applications housed at the CNSE data center that require their own disaster recovery plans.